



UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

ENERO – JUNIO 2017

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

Ingeniería en Sistemas

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS

TEMA:

Estudio de las vulnerabilidades del sistema contable Mónica implementado en la librería Don Arturo de la ciudad de Vines

EGRESADO (A):

Karina Alexandra Bobadilla Pionce

TUTOR:

Ing. Raúl Ramos Morocho, MIA

AÑO 2017

Tema:

ESTUDIO DE LAS VULNERABILIDADES DEL SISTEMA CONTABLE MÓNICA
IMPLEMENTADO EN LA LIBRERÍA DON ARTURO DE LA CIUDAD DE VINCES

I. INTRODUCCIÓN

En la actualidad la inclusión de las TIC (Tecnologías de la Información y la Comunicación) está creciendo a pasos agigantados, esto ha permitido que las empresas crezcan en su productividad enormemente. La utilización de sistemas informáticos empresariales conlleva situaciones de peligro ya que existen potenciales programas dañinos (software maliciosos) que intentan dañar o apoderarse de la información delicada de dichas entidades ante lo cual los directivos y personal informático deben estar alerta y en constante capacitación.

Los departamentos de las TIC de las diferentes empresas tienen la obligación de actualizar la información con respecto al sistema contable Mónica, mediante documentación y capacitación a los empleados, para así aumentar la productividad y seguridad del software.

Este trabajo tiene como título “Estudio de las Vulnerabilidades del Sistema Contable Mónica implementado en la librería Don Arturo de la ciudad de Vinces”, la información ha sido recopilada por medio de la observación a los empleados, el objetivo de este estudio de caso es identificar las vulnerabilidades del sistema contable Mónica.

Desarrollo

La librería Don Arturo es una micro – empresa dedicada a ventas de útiles escolares y materiales de oficina, desde el año 2000, ubicada en la ciudad de Vinces, provincia de Los Ríos. El sistema que utiliza la librería se llama Mónica versión 8.5, es un sistema informático contable que gestiona funciones de contabilidad, facturas, control de inventario, facturación, y muchas más utilidades que hacen de una forma más sencilla, que el negocio o actividad puedan ser controlados de una manera eficaz.

El presente trabajo está enmarcado en las líneas de investigación Desarrollo de Software y Trasmisión de Datos y Redes de computador.

En la presente investigación se utiliza el método inductivo – deductivo para la obtención de la información necesaria.

Inicialmente se realizo una entrevista al Sr. Walter Carriel Salazar, dueños de la empresa en la cual se pudo obtener los lineamientos a seguir en el proceso investigativo.

Se realizo una investigación de campo y aplicada en la cual se pudo observar las principales deficiencias de la investigación del sistema contable Mónica 8.5., por lo que el instrumento utilizado para la recopilación de información fue la observación directa, se procedió a realizar una encuesta a los diferentes usuarios del sistema Mónica (20 personas), como también al dueño de la empresa.

A mediados del mes de enero del presente año, librería Don Arturo implementó el sistema contable Mónica versión 8.5 ya que es una micro – empresa dedicada a la venta de útiles escolares y materiales de oficina por la cual se vió en la necesidad de ajustar y personificar ciertas exigencias, por lo que el proceso para desarrollar en un tiempo determinado de tres (03) meses, en vista que hasta el mes

de marzo se estaban completando detalles, adicionando funciones y capacitando a los empleados; pese a seguir con el proceso de implementación librería Don Arturo ya que estaba trabajando con normalidad, haciendo uso del sistema Mónica versión 8.5.

Durante el mes de abril el sistema no funcionó varios días debido al mal manejo de unos de los empleados de la librería.

En el mismo mes se suscitó otro problema por la misma causa; con la diferencia que esta vez fue por sacar el inventario, el empleado se equivocó de módulo y provocó que el sistema se colapsara y dejara de funcionar por varias horas.

En el mes de mayo se registraron algunas irregularidades como se muestra en el siguiente gráfico (ver anexo 1)

Durante todo el mes hubo diferentes irregularidades como pérdida de información, facturas borradas, datos erróneos en el sistema, etc.

En el mes de junio, un día lunes, los empleados de librería Don Arturo, notaron que no podían acceder a los ordenadores que utilizaban como: ingresar nuevos productos, generar reportes, facturación, es decir, todos los servicios del sistema que manejaban se encontraban dados de baja, por tal situación no permitía el acceso a la documentación guardada, misma que estaba ubicada en el dispositivo de cómputo con (Windows Xp).

Inclusive en ese mismo día todos estaban desconcertados, creían que se debía a problemas con el programa contable "Mónica", igualmente las otras funciones también dejaron de funcionar.

Al día siguiente todavía continuaban con el problema por lo que se comunicaron con el proveedor que el sistema no les permitía realizar ninguna función, entonces él mediante acceso remoto a través de Internet ingreso a la maquina central, para

analizar cuál era el inconveniente, después de revisar escrupulosamente se pudo esclarecer que el servicio de la base de datos no estaba funcionando correctamente, por lo que se había detenido el funcionamiento del sistema.

Después se dieron cuenta que toda la información de archivos tales como: documentaciones, carpetas, subcarpetas comprimidas y netamente todo la información que se encontraba y todo lo que estaba almacenado en el computador, y eso se daba en las particiones que tenía el disco duro, se presentaban con diferentes extensiones de aplicaciones, como podría indicar, un registro autoejecutable; si bien conocemos, como muestra: un archivo de Microsoft Excel, tiene una extensión “.xlsx” de un documento, de igual manera un audio, video, tienen su extensión, los cuales no son de aplicaciones, por lo que fue necesario que el encargado del departamento de soporte técnico logre evidenciar que los problemas presentados se dieron por algún tipo de software malicioso (virus) como:

Trojanos, changeup, ramnit, stuxnet w32/dorkbot, spyware; hoy en día mientras las tecnologías de la información y comunicaciones avanzan, así mismo van apareciendo un sin número de códigos maliciosos, malwares en red de datos, con el único fin de causar vulnerabilidades en los sistemas informáticos.

Gran parte de esta anomalías infecciosas se han producido por los llamados pendrive (memoria USB) extraíbles, aunque algunos de códigos maliciosos, en cantidad menor no causan infecciones, algunos de estos virus lo que hacen es ocultar los archivos originales y luego creando otros con el mismo nombre pero con diferentes extensiones, que habitualmente los crean con extensiones de aplicaciones o crean un acceso directo, lo cual es fácilmente resolver con una simple combinación de línea de códigos en la consola (DOS) de comandos de

Windows, de esta forma podemos eliminar los virus y queda resuelto el problema de este tipo de malwares.

A inicios del mes de julio, también no se podía acceder al sistema, pero esta vez fue causa de un bajón de energía la cual averió la máquina central.

En el mismo mes, un día sábado uno de los ordenadores no facturaba por motivo de que el disco duro de dicho ordenador no tenía espacio para seguir guardando información; se llamó al técnico de planta para que resolviera dicho problema.

Durante los dos años que tiene instalado el sistema contable Mónica en la librería Don Arturo el índice de vulnerabilidades se muestra en el siguiente gráfico (ver anexo 2).

Los diferentes sistemas informáticos presentan vulnerabilidades, riesgos y amenazas, que atentan contra la confidencialidad de los datos; como los virus informáticos, errores humanos, software mal configurado, software desactualizado u obsoleto, ausencia de copias de seguridad, cuentas de usuarios mal configuradas, la accesibilidad sin autorización al sistema informático, pérdidas de datos, información errónea, etc.

(Ludwing, 1995) Afirma: “Que los virus informáticos se unen a otro programa para facilitar su reproducción sin que el operador se dé cuenta, de esta forma van infectando el ordenador y producen pérdidas de información”.

Los virus informáticos se alojan en la matriz del sistema operativo, los cuales día a día se almacenan como si fueran parte del sistema y presentan conflictos como pérdida de información.

“Los virus informáticos son pequeños programas maliciosos escritos de forma intencional para instalarse en los ordenadores de un usuario sin la aprobación de este. Se menciona que se trata de un software dedicado a la vulnerabilidad ya que ejecuta sus ataques de manera primaria a los archivos y se expande a sí mismo con el fin de para vincularse y desarrollar su esparcimiento”.(Hernández, 2007, pág. 3)

Estos virus se almacenan en un computador con el único fin de causar vulnerabilidades creando archivos autoejecutables, accesos directos, ocultando archivos, etc.

Los ataques maliciosos son frecuentes en la creación de software se acrecientan de manera rápida, esto representa inconsistencias constantes a las compañías, ya que éstas son el blanco primordial de los cibercriminales, el progreso del malware en los últimos años ha sido angustiosa.

Los expertos de G DATA Security Labs descubrieron 1.84 millones de nuevas amenazas informáticas en la primera mitad de 2014, lo que significa que el cibercriminal alumbró un nuevo malware para entornos Windows cada 8.6 segundos, es decir, más de 10,200 nuevos tipos de programas maliciosos cada día.(Computerworld, 2014, pág. 26)

Por otro lado, el programa mal intencionado no tiene sentido sino manipulan medios de propagación y formas para implantarse en los dispositivos para comprometer la información de los usuarios y sacar provecho de cualquier forma; y gran parte de esas infecciones se producen en nuestro país.

Al día hay 10.5 millones de ataques cibernéticos en el mundo, el 1.8% es en Ecuador; cada 34 segundos un malware desconocido es descargado, cada 5

minutos una aplicación de alto riesgo es utilizada. A nivel regional, Ecuador es el segundo país más atacado por cibercriminales. (Checkpoint, 2015, pág. 59)

Hoy en día como avanza la era tecnológica así mismo van evolucionando un sin número de códigos maliciosos destinados a causar daños desde el más sencillo al más severo.

Hay que tener en cuenta que los códigos declarados intrusos o maliciosos como bitcoinsminers, botnets y ransomware, estos nuevos códigos malintencionados se basan en establecer un beneficio económico para los individuos atacantes, en lugar de establecer un daño como lo creaban los virus antiguos maliciosos. Hoy en la actualidad emprenden nuevos objetivos principales de estas amenazas como son: la sustracción de información para recibir dividendos al trasladar dicha información a la competencia, la apropiación ilícita de los datos para solicitar una compensación económica como parte de la liberación y uso de ataques, rechazos de servicios para aplacar la producción de determinada compañía. (Pérez, 2016)

Los riesgos que tienen las bases de datos significan una parte trascendental de toda empresa, ya que manejan datos confidenciales y almacenan registros de clientes, por lo que están sujetas a sufrir riesgos, según el artículo presentado por la Universidad de Santiago de Compostela (Ticpymes, 2013) tales como:

Inyección por SQL. Un ataque de este tipo puede dar paso a alguien y sin ningún tipo de limitación a una base de datos completa e incluso reproducir o alterar la información.

Auditorías débiles. No compilar registros de auditoría detallados puede llegar a significar una amenaza muy seria para la corporación en muchos niveles.

Exposición de los medios de almacenamiento para backup. Éstos están con frecuencia desprotegidos, por lo que numerosas vulnerabilidades de seguridad se han sobrellevado al robo de discos y de cintas. Además, al no auditar y monitorear las actividades de ingreso de bajo nivel por parte del personal encargado de la administración sobre la información de carácter confidencial puede poner en peligro los datos.

Explotación de vulnerabilidades y bases de datos mal configuradas. Los atacantes saben cómo explotar estas debilidades para lanzar ataques contra las compañías.

Las vulnerabilidades de las bases de datos se dan por varios factores como:

Los privilegios excesivos e inutilizados. -Es cuando a un individuo le asignan privilegios de base de datos que exceden los requerimientos de su sección de trabajo, se crea cierta vulnerabilidad reiterada. Lo cual se da cuando los punto de unión de control de libertades de los roles de trabajo no han sido correctamente precisadas o conservados, no destinados a la aspirada apertura de privilegios mínimos. (Quintero, 2016)

A la seguridad informática, conocida también como “Ciber-seguridad” o seguridad de las TIC, en el área de la informática la cual se ubica notoriamente en salvaguardar la infraestructura de las Tecnologías de las Información y Comunicación y todo lo que concierne en relación con dicha seguridad, y fundamentalmente la información retenida o circulante. Es por esta situación que constan una inmensidad de políticas, protocolos, estándares de calidad, métodos, materiales y leyes creadas para concluir las posibles eventualidades de inseguridad a la infraestructura tecnológica y a la información.

La seguridad informática está precisada tanto de software como: metadatos, archivos, base de datos y hardware, todo lo que la asociación estime y figure una amenaza si esta información de carácter confidencial llegue a manos de otras personas se convierte, por ejemplo, en información predilecta. (Sharshh, 2016)

La seguridad informática se enfoca esencialmente en la seguridad de la información, en los cuales se pueden utilizar una serie de estándares de calidad, para brindar la seguridad necesaria de la información.

“La definición de seguridad de la información jamás debe ser mezclada con la Seguridad Informática, ya que esta última netamente se enfoca en la seguridad en contorno del sistema informático, pero en cambio la información la podemos encontrar en innumerables medios o formas, y no solamente en medios del sistema informático”(Lemus&Rodolfo, 2014, pág. 162).

La seguridad informática es un procedimiento netamente designado a delinear las reglas, métodos, categorizaciones y técnicas seleccionados a obtener un sistema de información íntegro e innegable.

Puesto simple, la seguridad en una manifestación de la red como la destreza de identificar y excluir inconsistencias. Como definición muy general de seguridad se debe poner cuidado a la necesidad de resguardar la ventaja organizacional, dominando información y equipos físicos, tales como los equipos de computación. Nadie a cargo de seguridad debe implantar quién y cuándo puede tomar las tareas adecuadas sobre un ítem en específico. Cuando discutimos de la seguridad de una corporación, lo que más apropiado varía de organización en organización. Libremente cualquier compañía con una red debe adecuar políticas de seguridad que se dirija a la conveniencia y la coordinación.(Sharshh, 2016)

Aunque también existe una inmensidad de amenazas de forma que un ataque también pretende lograr adoptar más de una codificación. Como por modelo, un contenido de phishing puede conseguir substraer el password de un usuario de una red social y con esta consigue transformar un subrogación de identidad para un acoso de forma poderosa y oportuno, la malversación de la password para poder operar para algo tan sencillo como incurrir en cambios de las fotos de perfil y dejar todo en una inmediata burla, sin que este deje de ser una contravención en uno y otro proceso, con excepción de naciones con mantienen elegibilidad para el caso, como lo es el país europeo como España).(Sbajansmx2013, 2015)

De acuerdo a la publicación en su sitio web la empresa (Plastimetsa, 2014) menciona que las amenazas también pueden originar con la situación de vincular una red de datos a un contexto externo que nos da la apariencia de que algún sujeto dedicado a cometer ataques pueda inmiscuirse en la red y substraer la información o derogar el trabajo correcto de dicha red. Sin embargo, por lo habitual de que la red no se halle articulada al entorno externo como Internet, esto no prueba la seguridad de la red de datos.

Con el compromiso del (CSI) Computer Security Institute de San Francisco, cerca del 60 % y 80 % de los acontecimientos de red de datos son originados desde el interior de las redes. Estas se apoyan en el inicio de los ataques de las cuales logramos indicar que militan dos tipos de amenazas:

(Lombardo, 2012) Afirma que:

Las amenazas internas. Estas vulnerabilidades con frecuencia consiguen ser más rigurosas que las externas, por rehusar a situaciones como:

- ✓ Si es por usuarios o personal que brinda servicio técnico, estos individuos están al tanto absolutamente de la red y saben el método de trabajo de la misma, el lugar exacto de la información, identificaciones de mayor categoría, etc. Así mismo conservan algún nivel de salida a la red por la inmersa necesidad de su trabajo, lo que les determina crear mínimos movimientos.

- ✓ Los (Intrusion Prevention System) IPS, y firewallson aparatos que no tienen la mayor efectividad en las amenazas internas por no estar netamente, colocados en el tráfico interno. Estos ataques se desarrollen de forma interna no tiene que ser obligatoriamente por personas ajenas a la red de datos, igualmente pueden darse por la facilidad proporcionada al acceso a la red de datos de manera directa: tales como rosetas de fácil acceso, redes (Wifi) inalámbricas que se encuentran desprotegidas, equipos que carecen de vigilancia y control, etc.

De acuerdo a la prevención de delitos informáticos (Ávila&Caicedo&Carvajal&Delgado&Lodroño, 2015) afirman:

Que las amenazas externas: Son aquellas inseguridades causadas externamente de la red de datos. Al no ostentar información privilegiada de la red de datos, un individuo dedicado al crimen de datos implementa ciertas habilidades para poder realizar la comprobación de qué es lo que se encuentra en la red y ver la forma de introducirse y realizar ataques. La mayor ventaja que se goza en este asunto es que el personal que administra la red logra realizar la prevención de una gran parte de los ataques externos.

El tipo de amenazas según las consecuencias que ocasionan a quien recepta los ataques se clasifican de la siguiente forma:

- ✓ Hurto de la información.
- ✓ Devastación de la información.
- ✓ Neutralización de la actividad del sistema o consecuencias que se amplíena ello.
- ✓ Reemplazo de la identidad, propagación de datos expedidos como confidencial o personal, venta de información esencialmente personal y cambio de información, , etc.
- ✓ Robo de dinero, hurtos.

(Monica - ecuador, 2017) Afirma:

El sistema Mónica 8.5 es un programa ideal para cualquier negocio, dedicado a la comercialización de productos. Es fácil de trabajar no necesita tener conocimientos en contabilidad en la cual permite controlar inventarios, ingresar mercadería, reportes, facturas, y muchas más actividades que pueden ser manipulados; ya que el sistema "MONICA" es un conjunto de programas que le permitirá realizar lo siguiente: facturas, inventarios, cuentas por cobrar, cuentas por pagar, cuentas corrientes, contabilidad.

Facturas: En la facturación nos admite efectuar las facturas, cambiar, excluir; así mismo se consigue subrayar con sus propias cifras (números) de facturas por obvias situaciones. De manera que podemos cambiar por cualquier dato incorrecto que haya ingresado; eliminarlas por si hubo algún cruce de factura, o con eventualidad existen devoluciones de mercadería.

Así mismo se logra desarrollar facturas en lotes, ideal por ejemplo al instante de tener que realizar la facturación a una similar agrupación de personal beneficiario al concluir el mes que sea por un mismo concepto.

De tal forma lograr alcanzar sus totales de ventas por plazos determinados, reporte de impuestos, compradores, etc. Inventarios, controla la mercancía en el establecimiento: crear, modificar y elimina productos (el código de mercadería puede ser hasta de 14 caracteres), se puede desarrollar un listado de valores, tarifas-valores, para un determinado grupo de productos, intercambio de costos de uno o varias mercancías al mismo tiempo, lograr almacenar más de diez (10) millones de ítems en los registros (archivos).

Así como puede emitir cotizaciones a sus proveedores (si lo desea puede realizar impresión en inglés) y luego puede transformarlos en órdenes de compras la cual se encuentra asociado con los módulos de cuentas por pagar.

Otra característica fundamental es la tarjeta de registro (kárdex) que puede llevar su inventario, es fácil realizar la actualización y maniobrar. Por otra parte "MONICA", brinda la eventualidad de manipular las imágenes (fotografías o esquemas) de sus productos.

Como por ejemplo usted logra poseer un inventario de todas sus mercancías en su computador.

En cuentas por cobrar. -Un claro concepto es cuando la mercadería se realiza la venta a cómodas cuotas (crédito), el sistema "MONICA 8.5" nos brinda la forma más sencilla de realizar el control de pagos recurrentes, las facturas vencidas, abiertas, etc. En el cual se puede poseer una lista de todos los clientes que se encuentran en

mora, de facturas que ya fueron canceladas, facturas próximas a vencer fecha de pago. De esta forma podremos obtener el estado de cuenta de un cliente de manera fácil y en cualquier momento.

Cuentas por pagar: Como toda empresa necesita mantener un registro de las compras adquiridas a sus proveedores, de tal forma que en este campo le beneficia a la empresa, ya que por medio de esta le facilita tener la información necesaria acerca de los proveedores que tiene cuentas pendientes, así mismo las fechas de vencimiento de facturas, etc. Control de calendarios de cancelación a sus proveedores y estos de pagos para cada uno de ellos.

Cuentas corrientes: Las empresas pueden mantener como una o más de 1000 cuentas de estas; ya que es muy sencillo realizar un cheque nuevo en la cuenta corriente de la compañía, realizar depósitos, consulta de saldo, clasificación de cheques, etc. Así mismo realizar un cheque, es como si estuviera en su chequera realizando, lo único que tiene que ingresar los datos en los espacios en blanco.

Contabilidad: Esta sección esta implementada esencialmente para la persona profesional encargada del de llevar la contabilidad, el registro de asientos por partida doble, así mismo admite delimitar su tabla contable o hacer uso la que viene diseñada especialmente para para cada país, el cual puede ser manejado en agrupación de cuentas. Con el sistema "MONICA 8.5" puede poseer el libro Diario, Mayor, y los reportes financieros prioritarios; también puede tener los balances de la compañía, estado de pérdidas y ganancias y los balances tributarios.

Módulo de anexos transaccionales del Sistema de Rentas Internas, el sistema "Mónica 8.5" contiene un módulo que le admite obtener sin ninguna complicación el formulario electrónico de declaración de Impuestos al Sistema de Rentas Internas,

le admitirá desplegar de una forma fácil y sencilla las declaraciones concernientes, el método trabaja de la subsiguiente forma:

El sistema "MONICA" también puede trabajar en red: Windows y Novell y. Es indicar que usted puede lograr crear una factura en continuación de la red, mientras que la otra periodicidad como por ejemplo se consigue continuar operando el catálogo o inventario.

El sistema "MONICA" acepta el símbolo de su moneda y ha sido perfilada para concordar a los reglamentos de su país (por ejemplo, el RUT en Chile, RUC en Perú, NIT en Colombia, coma decimal en Sto. Domingo, Facturas reglamentadas en Venezuela, etc.)

"MONICA" posee entrada de seguridad, hasta cuatro (04) niveles de usuarios alcancen integrar a realizar las diferentes funciones de "MONICA", como por ejemplo personal de empleados que ingresa recientemente puede ser establecido un nivel básico el cual solamente le permite crear una factura, restringiendo la posibilidad de poder eliminarla o cambiarla y no puede consultar costos.

De acuerdo a (Sistemamonica, 2009) menciona los requerimientos para utilizar el sistema "MONICA" en la versión de Windows son los siguientes:

- ✓ Computadora en la cual se logre cargar Windows 9X o versiones consiguientes como (ejemplo la Pentium (r). se recomienda un computador Pentium(r) con un disco duro de alta velocidad (con 20 MB libres al menos), con memoria RAM de 256 MB en adelante y sistema operativo Windows 2000, Xp y Vista.
- ✓ Monitor VGA color o monocromático.

- ✓ Impresora de ochenta (80) columnas (Recomendable utilizar una impresora láser o de inyección 'Deskjet').
- ✓ En modo de "Punto de Venta" puede utilizar una impresora solo de recibos.

Las nuevas características que tiene el sistema contable MONICA para Windows traen más de treinta (30) adiciones, entre las cuales podemos mencionar las siguientes:

- ✓ El cálculo de la comisión para personal de mercantes.
- ✓ Actualmente es viable establecer hasta tres (03) diferentes características de facturas, como por ejemplo usted puede detallar un crédito fiscal, recibo y facturas.
- ✓ El módulo contable actualmente se encuentra combinado de una representación más eficaz que los demás módulos.
- ✓ Realización de Copias automáticas de respaldos.
- ✓ Etiquetas para los artículos de catálogos.
- ✓ Productos actualmente pueden ser detallados como servicios, físicos, esporádicos.
- ✓ La contabilidad ha sido mejorada de forma que se obtiene mayores cifras de reportes financieros.
- ✓ Cuentas por cobrar hoy permite el pago por cifra de Facturas y clientes. Puede remitir datos a otros paquetes: Listado de precios, clientes en formato Lotus, ASCII y Excel.
- ✓ Mayor ventaja de trabajar en redes Novell y Microsoft.
- ✓ Lugar de venta ahora accede mayor importe de impresoras de recibos, estantes de fortuna.

- ✓ Se ha abarcado mayores montos de reportes, y una excelente factibilidad de función para utilizar el software, más de veinte (20) explicaciones suministradas por nuestros usuarios que lo harán muy útil en su país.

II. Conclusiones

En el caso de las vulnerabilidades del sistema contable Mónica tuvo varias situaciones tales como: colapso del sistema, pérdida de información, facturas eliminadas, errores en el sistema contable Mónica 8.5, aplicaciones con extensiones ejecutables debido a la infección por códigos maliciosos, así mismo colapso del sistema por manejo indebido de parte de los empleados lo cual se da por falta de conocimientos del uso del sistema Mónica.

Por medio de este estudio se ha concluido que las diferentes vulnerabilidades del sistema contable Mónica en particular, fue por falta de seguridad en el sistema y es necesario tomar las medidas preventivas y correctivas para hacer frente a las diferentes anomalías que se presenten a futuro y así disminuir considerablemente los riesgos.

Por medio de esta experiencia, Librería Don Arturo de la ciudad de Vinces, ha tomado las medidas exhortadas para impedir e increpar este tipo de asuntos en los empleados, por tal situación se encuentra desarrollando capacitaciones y tomando todas las precauciones como: seguridad del sistema y respaldos de forma automática todos los días en una carpeta que luego serán subidos en un servidor FTP (File Transfer Protocol) en otro dispositivo y en otra ubicación geográfica. Si bien este es un caso de invariable investigación y progreso, este trabajo dará la iniciativa que va a admitir considerar la seguridad de la información verdaderamente importante en la productividad de dicha empresa.

ANEXOS

Entrevista

- 1. ¿La utilización del sistema contable Mónica le ha dado algún tipo de problemas?**

Si

- 2. ¿Cuáles han sido los principales errores que se han producido?**

Perdida de información, niega el acceso de entrada al sistema, se cierra en ocasiones.

- 3. ¿Ud., piensa que los problemas suscitados han sido provocados por los sistemas informáticos o por el mal manejo de los empleados?**

Mal manejo de los empleados

- 4. ¿Ud., ha capacitado al personal en los últimos meses?**

No, nunca

- 5. ¿Cuáles son las horas picos de la utilización del sistema?**

En época escolar

Encuestas

1. ¿Está conforme con el Sistema Informático que utiliza en la actualidad en la empresa?

Si

No

2. ¿El trabajo ha sido retardado debido a un fallo en el sistema informático?

Si

No

3. ¿Ha habido pérdida de información por culpa del sistema informático?

Si

No

4. ¿Se realiza copias de seguridad periódicas de la información relevante de la empresa?

Si

No

5. ¿Se utilizan mecanismo de control de seguridad de la información (políticas de seguridad)?

Si

No

6. ¿Cree Ud., que un nuevo sistema informático ayudaría en el trabajo?

Si

No

7. ¿La empresa cuenta con seguridad física de la protección de los equipos?

Si

No

8. ¿El cableado de red cumple con certificaciones internacionales?

Si

No

9. ¿Se realiza mantenimientos periódicos en los equipos para garantizar el buen funcionamiento de los mismos?

Si

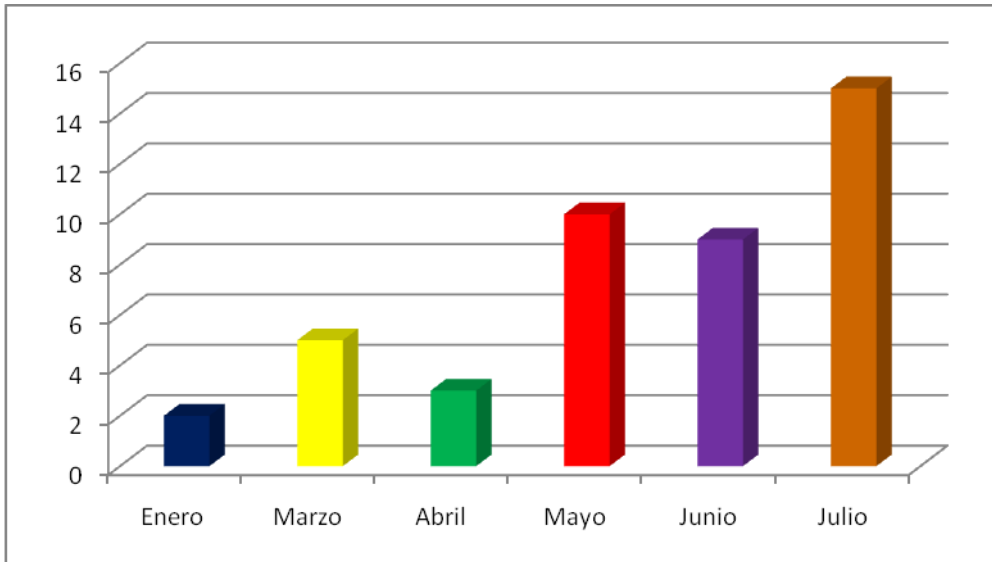
No

10. ¿La adquisición de nuevos computadores favorecería la realización adecuada de los trabajo?

Si

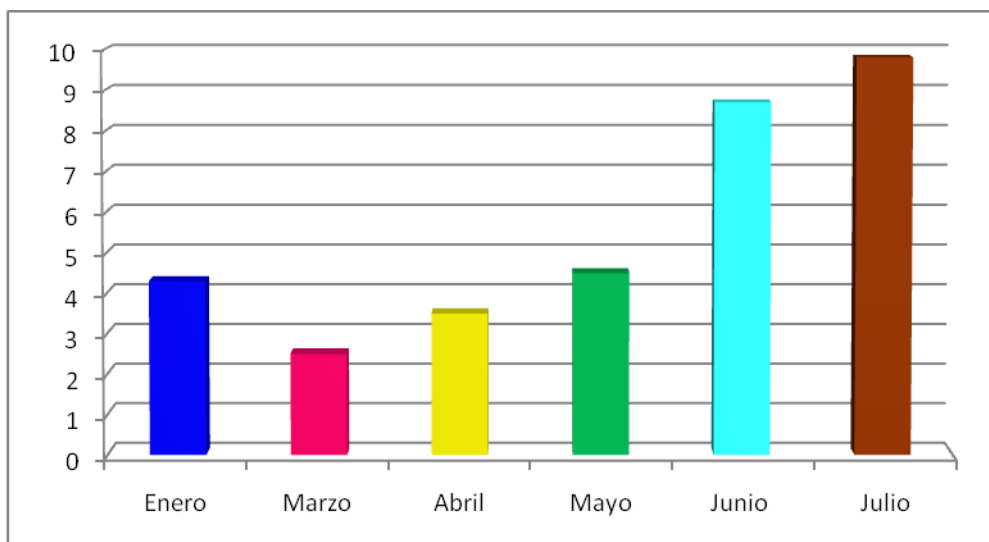
No

IRREGULARIDADES AÑO 2017



Anexo N° 1. Fuente: Elaboración propia.

ÍNDICE DE VULNERABILIDADES



Anexo N° 2. Fuente: Elaboración propia.

SISTEMA MONICA



Anexo N° 3. Pantalla principal del Sistema Contable Mónica.



Anexo N° 4. Pantalla de los recursos del Sistema Contable Mónica.

Bibliografía

- Ávila&Caicedo&Carvajal&Delgado&Lodroño. (2015). *Wixsite*. Obtenido de Proyectoutn.wixsite.com:
<http://proyectoutn.wixsite.com/delitos/tipos-de-amenazas>
- Checkpoint. (2015). Checkpoint. *Checkpoint*, 59.
- Computerworld. (2014). 26.
- Hernandez. (2007). *www.cyta.com.ar*. Obtenido de cyta:
<http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/virus/virus.pdf>
- Lemus&Rodolfo. (DICIEMBRE de 2014). SEGURIDAD DE LA INFORMACIÓN. (2. P. EDICIÓN, Ed.)
REVISTA DE LA SEGUNDA COHORTE DEL DOCTORADO EN SEGURIDAD ESTRATÉGICA, 162.
- Lombardo. (28 de NOVIEMBRE de 2012). *aytbjknjrplk*. Obtenido de Prezi.com:
<https://prezi.com/aytbjknjrplk/amenazas-internas-y-externas-a-la-informacion/>
- Ludwing. (1995). *EL LIBRO NEGRO GIGANTE DE LOS VIRUS INFORMÁTICOS*. ARIZONA: American Eagle Publications, Inc.
- Monicaecuador. (2017). *monicaecuador*. Obtenido de monicaecuador.com:
<http://www.monicaecuador.com/descripcion-monica/descripcion-monica-v8-5/>
- Pérez. (2016). Obtenido de computerworld.com.ec:
<http://computerworld.com.ec/actualidad/tendencias/30-el-malware-%20empresarial-crece-en-el-mundo.html>
- Plastimetsa. (DICIEMBRE de 2014). *Plastimetsa*. Obtenido de Plastimetsa.com:
http://www.plastimetsa.com/site/wpress/?page_id=157
- Quintero. (23 de Marzo de 2016). *blogspot.com*. Obtenido de blogspot:
<http://gabrielquintero.blogspot.com/2016/03/amenazas-las-bases-de-datos.html>
- Sbajansmx2013. (06 de Febrero de 2015). *servermnt*. Obtenido de servermnt.wordpress.com:
<https://servermnt.wordpress.com/2015/02/06/2-tipos-de-amenazas/>
- Sharshh. (01 de Agosto de 2016). *seguridadinformatica300*. Obtenido de seguridadinformatica300.wordpress.com:
<https://seguridadinformatica300.wordpress.com/author/shorshh/>
- Sharshh. (01 de Agosto de 2016). *seguridadinformatica300.wordpress.com*. Obtenido de seguridadinformatica300.:
<https://seguridadinformatica300.wordpress.com/author/shorshh/>
- SISTEMAMONICA. (2009).
- Sistemamonica. (2009). *monica*. Obtenido de monica.com.do:
http://www.monica.com.do/index.php?option=com_content&view=article&id=48&Itemid=59

Ticpymes. (2013). Las 10 grandes amenazas de seguridad en las bases de datos. *Las 10 grandes amenazas de seguridad en las bases de datos*, 2-3. Obtenido de Las 10 grandes amenazas de seguridad en las bases de datos.