UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORIA DE SEGURIDAD INFORMÁTICA A LA EMPRESA BANAGINA S.A, UBICADA EN LA PROVINCIA DEL ORO, PARROQUIA EL CAMBIO

GUAYAS BELDUMA BRIGITTE NICOLE
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORIA DE SEGURIDAD INFORMÁTICA A LA EMPRESA BANAGINA S.A, UBICADA EN LA PROVINCIA DEL ORO, PARROQUIA EL CAMBIO

GUAYAS BELDUMA BRIGITTE NICOLE
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2018

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

AUDITORIA DE SEGURIDAD INFORMÁTICA A LA EMPRESA BANAGINA S.A, UBICADA EN LA PROVINCIA DEL ORO, PARROQUIA EL CAMBIO

GUAYAS BELDUMA BRIGITTE NICOLE
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

ORDÓÑEZ BRICEÑO KARLA FERNANDA

MACHALA, 09 DE JULIO DE 2018

MACHALA
09 de julio de 2018

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Auditoria de Seguridad Informática a la Empresa BANAGINA S.A, ubicada en la Provincia del Oro, Parroquia El Cambio, hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

ORDÓÑEZ BRICEÑO KARLA FERNANDA
0705031003
TUTOR - ESPECIALISTA 1

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 2

PARRA OCHOA EUDORO BENITO
0701063406
ESPECIALISTA 3

Fecha de impresión: lunes 09 de julio de 2018 - 16:03

Urkund Analysis Result

Analysed Document:	CASO PRACTICO-EMPRESA BANAGINA- GUAYAS BRIGITTE.docx (D40252488)
Submitted:	6/19/2018 12:18:00 AM
Submitted By:	bguayas_est@utmachala.edu.ec
Significance:	0 %

Sources included in the report:

Instances where selected sources appear:

0

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, GUAYAS BELDUMA BRIGITTE NICOLE, en calidad de autora del siguiente trabajo escrito titulado Auditoria de Seguridad Informática a la Empresa BANAGINA S.A, ubicada en la Provincia del Oro, Parroquia El Cambio, otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 09 de julio de 2018

GUAYAS BELDUMA BRIGITTE NICOLE
0706762036

AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA EMPRESA BANAGINA S.A, UBICADA EN LA PROVINCIA DEL ORO, PARROQUIA EL CAMBIO.

RESUMEN

En el presente trabajo, la auditoria de la seguridad informática, se desarrolló con el propósito de hacer una evaluación, a los procesos informáticos más importantes de la Empresa BANAGINA S.A, para ello, se hizo uso de la metodología, para realizar auditorías a los sistemas computacionales (ASC), que se basa, en determinar las actividades a evaluarse, haciendo uso, de las herramientas o métodos (cuestionarios y fichas de observación), para obtener resultados sobre sus activos, sistemas informáticos y el desarrollo de sus actividades; cabe recalcar que cada una de sus fases, fue desarrollada, dependiendo de la situación en la que se encuentra la empresa. Esta auditoria tiene como objetivo realizar, una evaluación al rendimiento de cada uno de los empleados, detectar amenazas y vulnerabilidades en el hardware y software, con el fin de obtener una información confidencial y segura de sus activos informáticos y poder determinar, el cumplimiento de los objetivos establecidos por la empresa; ya que por ello, es muy importante aplicar los controles de seguridad informática, para estar a salvo ante cualquier amenaza.

Así mismo, se puede concluir que; con la redacción del informe, se muestra que los resultados obtenidos del desarrollo de la auditoria informática, se han detectado hallazgos y en base a esto, se han dado recomendaciones, con el fin de evaluar la eficacia y eficiencia de recursos informáticos, con propósito de obtener el desarrollo óptimo de las actividades, por parte de los usuarios y controlar a la seguridad física y lógica, para beneficio de la empresa.

PALABRAS CLAVES: Auditoria informática, Seguridad física y lógica, Recursos informáticos.

AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA EMPRESA BANAGINA S.A, UBICADA EN LA PROVINCIA DEL ORO, PARROQUIA EL CAMBIO.

ABSTRAC

In the present work, the computer security audit was developed with the purpose of making an evaluation of the most important IT processes of the BANAGINA S.A Company, for this, the methodology was used to perform systems audits computational (ASC), which is based on determining the activities to be evaluated, making use of the tools or methods (questionnaires and observation forms), to obtain results about their assets, information systems and the development of their activities; It should be noted that each of its phases was developed, depending on the situation in which the company is located. This audit aims to perform an evaluation of the performance of each employee, detecting threats and vulnerabilities in hardware and software, in order to obtain confidential and secure information about their computer assets and to determine compliance with the objectives established by the company; Because of this, it is very important to apply computer security controls, to be safe from any threat.

Likewise, it can be concluded that; with the writing of the report, it is shown that the results obtained from the development of the computer audit, findings have been detected and based on this, recommendations have been given, in order to evaluate the effectiveness and efficiency of computing resources, with the purpose of obtain the optimal development of the activities, by the users and control the physical and logical security, for the benefit of the company.

KEY WORDS: Computer audit, Physical and logical security, Computer resources.

INDICE

INTRODUCCIÓN

Actualmente, la tecnología es una clave muy importante para el desarrollo de una empresa, pero a través del tiempo, “las amenazas tecnológicas son parte de nuestra cotidianeidad y más aún de la vida organizacional, las cuales van desde diversas formas de virus, pasando por los recientes ataques de *ransomware* hasta amenazas sofisticadas como los ataques día cero” (Valencia & Orozco, 2017, pág. 74). Es decir, que ha provocado ciertas falencias, atacando a los sistemas informáticos y para poder controlar, cada actividad que se realice dentro la misma, se ha optado por desarrollar auditorías informáticas, con el fin de que nos permita, tomar una mejor decisión, logrando ubicar a la empresa dentro de un nivel competitivo.

Por tal motivo, la auditoría informática es fundamental para obtener un mejor desempeño de actividades, en cuanto al uso de redes informáticas y control de información, garantizando el funcionamiento de equipos de cómputo y software con un rendimiento máximo; es por ello que la Empresa BANAGINA S.A, realiza una auditoria a la seguridad física y lógica, la misma que se dedica al cultivo, venta al por mayor y menor de banano, solicitando que se evalúe el rendimiento óptimo, por parte de los empleados y poder detectar posibles fallas, vulnerabilidades en el software, con el fin, de que avale la confidencialidad, integridad de los procesos realizados dentro de cada área dando como resultado el cumplimiento de los objetivos.

Durante el desarrollo de la auditoria a la empresa, se procede a determinar las siguientes fases; cabe recalcar que la metodología a aplicarse, es la metodología para realizar auditorías de sistemas computacionales (ASC), ya que se han establecido ciertos puntos relacionados, con el problema determinado por la empresa; en la primera parte se realiza la planeación, en donde se visitará las instalaciones de la empresa, para poder proceder a recolectar la información pertinente en base a la red de datos y computadoras del departamento a auditarse; en la segunda parte se da la ejecución, en donde vamos a detectar las vulnerabilidades, dentro del área a auditar mediante, la aplicación de métodos e instrumentos, de tal manera que permita identificar los hallazgos, para los respectivos análisis sobre el rendimiento de las actividades, que impiden el desarrollo optima de la misma; dando por terminado con el dictamen de auditoría.

DESARROLLO

Auditoría Informática

La auditoría informática, se ha convertido en un factor importante, para las empresas ya que hoy en día, debido a "los diferentes ataques a los activos informáticos pueden provocar la pérdida de la disponibilidad, confidencialidad o integridad de la información; lo cual generalmente implica graves consecuencias para las empresas y en muchas ocasiones se ocasionan daños irreparables" (Montesino, Baluja, & Porvén, 2013, pág. 40). Todo esto, con el fin de salvaguardar, proteger la información, los recursos de las empresas y controlar las actividades desarrolladas.

Tomando en cuenta, todos estos factores en la evaluación de los sistemas computacionales dentro de la empresa, se puede definir que:

La auditoría informática, es un conjunto de técnicas, que permiten realizar una evaluación a los sistemas informáticos, teniendo como objetivo, proteger los activos informáticos y comprobar que las actividades se desarrollen eficiente y eficazmente, dentro de cada entidad.

Seguridad Informática

Esta seguridad informática está, "dirigida fundamentalmente a prevenir, detectar y contrarrestar las acciones que pongan en peligro" (Díaz, Pérez, & Proenza, 2014, pág. 3). La misma que previene, detecta y contrarresta la información y además, trata de asegurar que los recursos, sean utilizados de manera correcta y puedan ser manipulados por aquellas personas, que únicamente tengan la autorización, para acceder a dicha información; ya que si no se dan estos controles de seguridad existe, "la vulnerabilidad de los sistemas de computadoras hacia la pérdida de recursos, el impacto del fracaso de la seguridad en datos confiables, la posibilidad de faltar a los cumplimientos con los requisitos legales" (Azán, y otros, 2014, pág. 55). Lo que provoca, que se sufran daños y tengan pérdidas, provocadas por la falta de estos controles de seguridad, por ello es muy importante la confidencialidad y la aplicación de los mecanismos de seguridad, ya que está garantiza la protección de sistemas y así poder evitar o minimizar, ciertas amenazas que se presenten, y poder lograr que esta seguridad informática, dentro de la empresa, pueda tener éxito.

Seguridad Física y Lógica

Seguridad física.- es importante, para poder prevenir cualquier falencia en equipos informáticos, incluso para poder evitar algún desastre natural. Entonces podemos definir que la seguridad física, hace "referencia a las barreras físicas y mecanismos de control en el entorno de un sistema informático, para proteger el hardware de amenazas físicas" (Martelo, Tobar, & Maza, 2018, pág. 4). Mediante este control, se puede disminuir algún contratiempo de fuerza mayor, incumplimiento de actividades o pérdida de información confidencial; cabe recalcar que la seguridad física, no solo se refiere a los equipos, sino también lo que pueda ocurrir alrededor de la empresa.

Seguridad lógica.- a diferencia de la física, se presentan daños internos con el almacenamiento o procesamiento de información, ya que el activo primordial o más importante, que puede haber en una empresa es la información, por ello se dice que, la seguridad lógica, "hace referencia a la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático" (Martelo, Tobar, & Maza, 2018, pág. 4). Esto quiere decir, que la información debe ser salvaguardada y únicamente, utilizada por personas, que estén autorizadas.

Fases de la Auditoría

1. Planeación.- esta fase nos indica, cómo vamos a desarrollar o que pasos se deben seguir para hacer la auditoria, para ello se deberá tener en claro los "objetivos, la colaboración y responsabilidad de todo el personal involucrado para garantizar el desarrollo de las actividades y el cumplimiento de las funciones de cada uno de ellos" (Escobar, Moreno, & Cuevas, 2016, pág. 6). Es decir, que será necesario de la colaboración y de las visitas preliminares para así, poder establecer las herramientas o técnicas, a utilizarse para la recolección de información.
2. Ejecución.- en base a los objetivos establecidos de la auditoria, se procede a desarrollarla en base a la información o documentación recolectada, y se aplica los métodos o técnicas.
3. Informe.- en esta última fase, se procede a realizar un borrador de todos los hallazgos presentados en la empresa y luego, la presentación del informe

final de forma clara y concisa, expresando los resultados y dando un dictamen para el mejoramiento de sus operaciones.

Control Interno

El control interno de la empresa, es aplicado con el fin de poder disminuir los riesgos suscitados, salvaguardando los activos y controlando que se cumplan con los procedimientos, los mismos que estén "acorde con los objetivos y metas de la organización" (González, de Zayas, & López, 2015, pág. 36). Además, cabe recalcar que así como existe el control interno; también existe el control interno informático y este hace referencia al control de las operaciones desarrolladas de los "sistema de información se debe monitorear y evaluar de manera constante, con métricas establecidas que permitan medir con objetividad y tomar las decisiones oportunas respecto a los riesgos que se enfrentan" (Miranda, Valdéz, Pérez, Portelles, & Sánchez, 2016, pág. 17). De tal manera que el auditor aplique los controles a los sistemas de información, para poder prevenir corregir y prevenir eventualidades no deseadas.

Metodología De La Investigación

El presente proyecto, hace referencia a un enfoque cualitativo del desarrollo de una auditoria informática, el cual se sujetará de la "responsabilidad de cada auditor, documentos que deben entregar al jefe de equipo, forma y periodicidad de entrega de informes de avance de trabajo, resultados de la terminación de cada fase" (Martínez, Blanco, & Loy, 2013, pág. 8). Con el propósito, de lograr obtener un resultado que, me "Garanticen la confidencialidad, la integridad y la disponibilidad de la información" (Parada, Flóres, & Gómez, 2018, pág. 28). Es por ello, que la metodología a implementarse para el desarrollo de la auditoria a la Empresa BANAGINA S.A, es la METODOLOGÍA PARA REALIZAR AUDITORÍAS A LOS SISTEMAS COMPUTACIONALES (ASC); la misma que determinará: las fases, las actividades que se requieren para su desarrollo, que está ejecutada conforme a las necesidades propuestas por la empresa.

Caso Práctico

En la empresa ‘ABC’ se ha detectado que los empleados han bajado considerablemente su rendimiento, debido a que constantemente se encuentran conectados a las Redes Sociales, y las computadoras tienden a colgarse con mucha frecuencia, lo cual impide el desarrollo óptimo de las actividades que aquí se desarrollan.

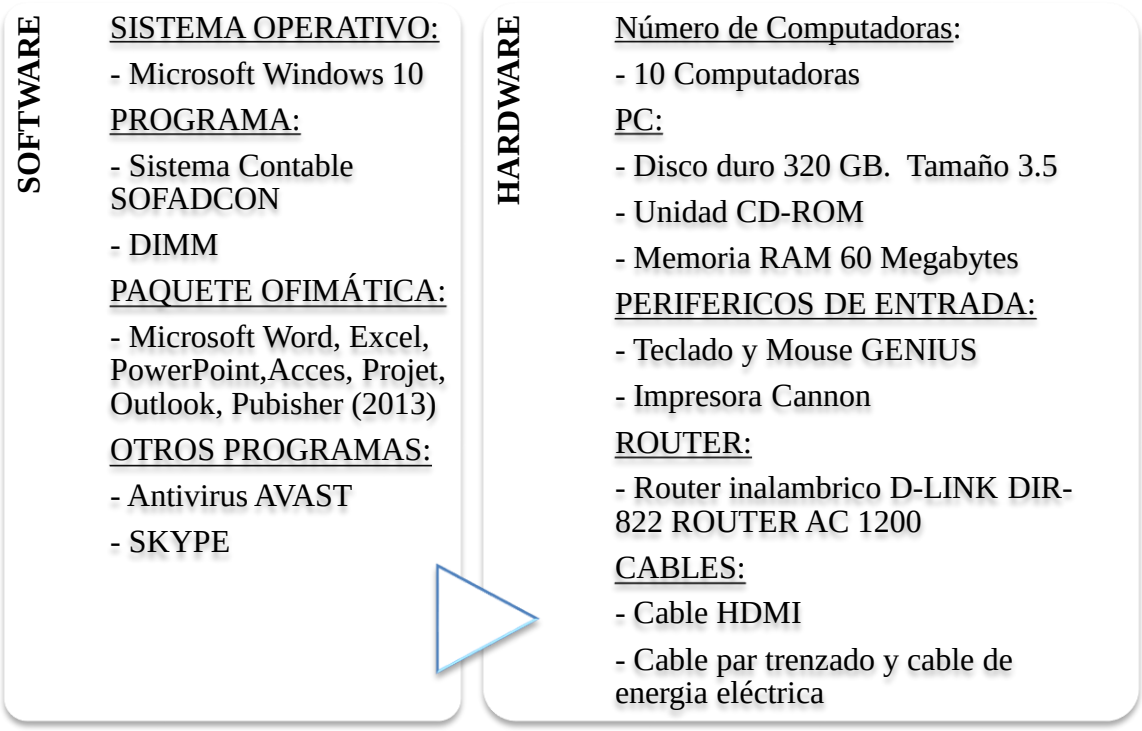
¿Cómo Auditor Informático Interno que solución propone?

PLANEACIÓN DE LA AUDITORÍA

EMPRESA BANAGINA S.A, en el año 2009, inicia su actividad económica, la misma que se dedica al cultivo de banano, venta al por mayor y menor de banano, Ubicada en La Provincia El Oro, Parroquia El Cambio, en la AV. Panamericana y AV. Ferroviaria S/N; está representada legalmente, por la Sra. Gina Alvear Bohórquez, y además cuenta con profesionales especializados en cada una de sus áreas, logrando dar como resultado un servicio eficiente antes las exigencias de nuestros clientes, con la debida confidencialidad y responsabilidad en cada una de sus operaciones**.(VER ANEXO N°1. ORGANIGRAMA ESTRUCTURAL).**

Visita Preliminar Al Área Auditada.

Se realizó la visita a las instalaciones de la empresa para poder observar el comportamiento de los empleados, determinar las funciones realizadas, poder verificar seguridad de dispositivos y el acceso a la información. Además se revisó las características de los computadores se utilizó el programa WinAudit Freeware v3.1, el mismo que nos detalla el software, programas instalados, configuración de red, seguridad entre otros y el hardware. Se detalla a continuación:



Objetivos de la Auditoría

OBJETIVO GENERAL

Desarrollar una auditoría de los sistemas informáticos a la EMPRESA BANAGINA S.A, mediante la utilización de métodos y herramientas con el fin de lograr que los objetivos establecidos sean cumplidos.

OBJETIVOS ESPECÍFICOS

- Verificar el acceso a usuarios a los sistemas de información de la Empresa BANAGINA S.A
- Comprobar mediante documentación la existencia de políticas en cuanto al uso de páginas web.
- Verificar que los empleados cumplan con las políticas y responsabilidades a desarrollar dentro de la empresa.
- Revisar el hardware y software de los computadores, para que permitan el desarrollo óptimo de las actividades.
- Aplicar métodos y técnicas con el fin de disminuir riesgos en los sistemas informáticos.

Puntos a evaluarse de la Empresa BANAGINA S.A

Seguridad Física	• Inventario de equipos de hadware y software • Control para instalar dispositivos • Adquisicion de equipos.
Seguridad Lógica	• Acceso de usuarios a las paginas Web • Existencia de Antivirus • Acceso de los usuarios a programas o informacion.
Empleados	• Cumplimiento por parte de los empleados de politicas y de las responsabilidades.

Identificación y Selección de Métodos

En este punto se procedió a realizar la guía de auditoría, la misma que determinará los procedimientos a ejecutarse en cada actividad que se va a evaluar, haciendo referencia a cada una de las herramientas que serán utilizadas en cada área **(VER ANEXO N°2. GUÍA DE AUDITORÍA)**

EJECUCIÓN DE LA AUDITORÍA

Aplicar las Herramientas y Técnicas para el desarrollo de la Auditoría

Las herramientas y técnicas utilizadas para la aplicación a la auditoría informática de la Empresa BANAGINA S.A Son:

- Cuestionario de control interno. **(VER ANEXO N°3. C.C.I. Y TABULACIÓN)**
- Guías de observación **(VER ANEXO N°4. FICHAS DE OBSERVACIÓN)**

TABULACIÓN DEL CUESTIONARIO DE CONTROL INTERNO

EL cuestionario ha sido realizado a 5 personas de las diferentes áreas que laboran en la empresa; a continuación se presenta la tabulación de los encuestados de cada punto a evaluarse

- SEGURIDAD FÍSICA

Inventario de equipos de hardware y software.- Según la primera pregunta de la encuesta realizada a 5 personas, 3 de ellas nos dicen que la empresa, cuenta con un inventario de hardware y software; por lo tanto en la segunda pregunta 3 de ellas, también determinan que este inventario no es actualizado constantemente.

Control para instalar dispositivos.- en la tercera pregunta, 2 de los encuestados manifestaron que, si se realizan mantenimientos frecuentes a los equipos de cómputo; mientras que en la cuarta pregunta, 3 de ellos instalan portadores USB para pasar información en los computadores.

Adquisición de equipos.- en la quinta pregunta, según todos los encuestados dijeron que al momento de realizar adquisiciones, se piden las correspondientes facturas.

- SEGURIDAD LÓGICA

Acceso de usuarios a las páginas web.- en la sexta y séptima pregunta, los 5 encuestados manifestaron, que todos tienen acceso a páginas web y hacen uso de las redes sociales en horas de trabajo.

Existencia de antivirus.- en la octava y novena pregunta, los encuestados afirman que los antivirus no cuentan con licencias y que no son actualizados en el periodo establecido que se requiere.

Acceso de los usuarios a programas o información.- en la décima pregunta, 3 de los 5 encuestados manifestaron, que sí cuentan con respaldos de información en caso de pérdidas; mientras que en la onceava pregunta, los 5 encuestados cuentan con claves para el acceso al computador.

· EMPLEADOS

Cumplimiento de responsabilidades y de políticas.- en la doceava pregunta, realizada a las 5 personas manifestaron la existencia de políticas para el acceso a redes sociales; mientras que en la treceava pregunta todos los encuestados dijeron que el uso del equipo lo realiza el personal dentro de cada área.

Con la información recolectada, luego de haber realizado los cuestionarios al personal y fichas de observación, se procede a realizar la matriz de resultados (**VER ANEXO N°5**), en el cual se dará una calificación de cada actividad que ha sido evaluada.

DICTAMEN DE LA AUDITORÍA

Situaciones Detectadas

Con los resultados de la ejecución de la auditoría realizada a la Empresa BANAGINA S.A, se dará a conocer los principales problemas que afectan al rendimiento de la misma.

Como se ha podido evidenciar se detectó que en la seguridad física el inventario existente en la empresa está totalmente desactualizado y existen falta de controles a las instalaciones de portadores USB; en la seguridad lógica, no existe un control para el acceso al sistema ya que las contraseñas son de fácil acceso poniendo en riesgo la información proporcionada por la empresa, además no se cuenta con actualizaciones de antivirus, así mismo los empleados no tienen los controles ya que tienen el fácil acceso a las páginas web, es decir hacen uso de la redes sociales incumpliendo con el desarrollo óptimo de sus actividades y de las políticas establecidas por la empresa.

Cabe recalcar que en cada punto a evaluar a la seguridad física, a la seguridad lógica, y a los empleados, se ha dado sugerencias para la solución a cada falencia, para poder ayudar a mejorar la situación en la que se encuentra y así pueda lograr el desarrollo óptimo de sus operaciones para poder tener éxito en su empresa. (**VER ANEXO N°6. SITUACIONES RELEVANTES)**

CONCLUSIONES

Con los problemas ya presentados por la gerente general de la empresa BANAGINA S.A, se procedió a elaborar las actividades o puntos a auditarse, los mismos que se basan en la seguridad física, seguridad lógica y evaluación a los empleados.

Es muy importante que la empresa cuente con actualizaciones en el software y debe implementar más controles a la seguridad informática el respectivo mantenimiento a los equipos, ya estos puntos son muy esenciales para el buen manejo y funcionamiento de los equipos y así poder cumplir con los objetivos establecidos por la empresa.

Cada empleado, deberá ser responsable con las contraseñas en cuanto a la información, ya que solo ellos podrán acceder únicamente para mantener confidencial y segura la información proporcionada. Se debe prohibir o restringir el acceso al internet en especial bloquear redes sociales para que no existieran distracciones.

En cada uno de los puntos a evaluarse de las situaciones relevantes, contienen las respectivas soluciones; así mismo se debe tener en cuenta que solo se usen programas útiles para el desarrollo de actividades y se debe vigilar las áreas por parte de algún responsable, para el mejoramiento de sus operaciones y tenga un buen funcionamiento la empresa.

BIBLIOGRAFÍA

Azán, Bravo, Rosales, Trujillo, García, & Pimentel. (2014). Solución basada en el razonamiento basado en casos para el apoyo a las auditorías informáticas a bases de datos. *Revista Cubana de Ciencias Informáticas, 8*(2), 52-68. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992014000200004&lang=pt

Díaz, Pérez, & Proenza. (2014). Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. *Ciencias Holguín, XX*(2), 1-14. Obtenido de http://www.redalyc.org/pdf/1815/181531232002.pdf

Escobar, Moreno, & Cuevas. (2016). La calidad de la auditoría en Sistemas de Gestión. Software AUDIT_INTEGRATED. *Ciencias Holguín, 22*(2), 1-18. Obtenido de http://www.redalyc.org/pdf/1815/181545579007.pdf

González, de Zayas, & López. (2015). Auditoría de información y auditoría de conocimiento: acercamiento a su visualización como dominios científicos. *Revista Cubana de Información en Ciencias de la Salud, 26*(1), 34-52. Obtenido de http://www.redalyc.org/pdf/3776/377645760005.pdf

Martelo, Tobar, & Maza. (2018). Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia. *Información Tecnológica, 29*(1), 3-10. Obtenido de https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000100003&lang=pt

Martínez, Blanco, & Loy. (2013). Propuesta del Sistema de Acciones para la implementación de la Auditoría con Informática. *Revista de Arquitectura e Ingeniería, 7*(2), 1-13. Obtenido de http://www.redalyc.org/pdf/1939/193929227003.pdf

Miranda, Valdéz, Pérez, Portelles, & Sánchez. (2016). Metodología para la implementación de la gestión automatizada de controles de seguridad informática. *Revista Cubana de Ciencias Informáticas, 10*(2), 14-26. Obtenido de http://www.redalyc.org/articulo.oa?id=378345292002

Montesino, Baluja, & Porvén. (2013). Gestión automatizada e integrada de controles de seguridad informática. *Ingeniería electrónica, Automática y Comunicaciones, 34*(1), 40-58. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59282013000100004&lang=pt

Muñoz, C. (2002). *Auditoría en Sistemas Computacionales.* México: Pearson Educación de México, S.A de C.V. Obtenido de https://cdryst.files.wordpress.com/2009/10/aussist.pdf

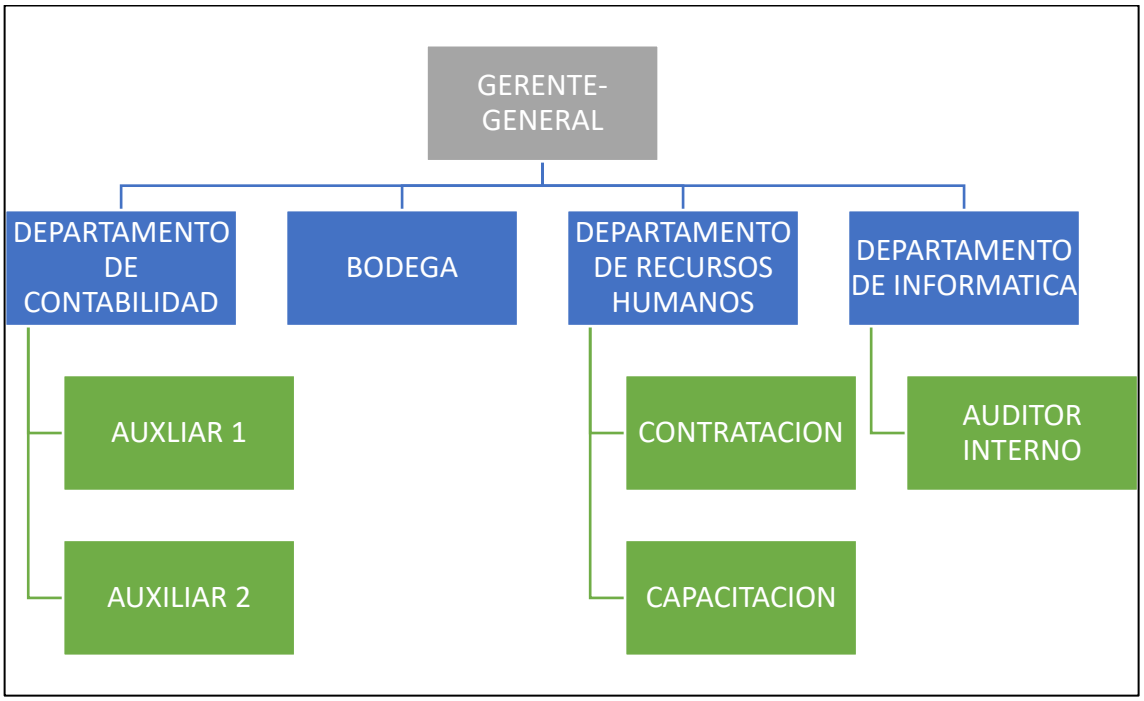
Parada, Flóres, & Gómez. (2018). Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas. *Información Tecnológica, 29*(1), 27-38. Obtenido de https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000100027&lang=pt

Valencia, & Orozco. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*(22), 73-88. Obtenido de http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952017000200006

ANEXOS

ANEXO N°1. ORGANIGRAMA ESTRUCTURAL DE LA EMPRESA

BANAGINA S.A



ELABORADO POR: Brigitte Guayas Belduma

FUENTE: EMPRESA BANAGINA S.A

ANEXO N°2. GUÍA DE AUDITORIA

 BANAGINA S.A. R.U.C.: 0992636459001 PRODUCTORES DE BANANO				**FECHA**: 21/22/05/2018 **HORA**:9H00AM
REFERENCIA	**ACTIVIDAD A EVALUAR**	**PROCEDIMIENTOS DE AUDITORIA**	**HERRAMIENTAS UTILIZADAS**	**OBERVACIONES**
AUD 01	Evaluar la seguridad física de la Empresa BANAGINA S.A	-Determinar si existe un inventario actualizado de equipos de hardware y software. -Verificar si existe un control para instalar dispositivos USB. -Verificar la adquisición de equipos mediante facturas.	• Cuestionario	
AUD 02	Evaluar la seguridad lógica de la empresa.	-Determinar si existe un control para el uso de páginas web. -Verificar la existencia de antivirus actualizados. -Verificar si cuentan con contraseñas para acceder a la información almacenada en equipos.	• Cuestionario • Ficha de observación	
AUD 03	Evaluar las políticas y el rendimiento del personal en cuanto al cumplimiento de responsabilidades	-Determinar si el personal cumple con las políticas establecidas. -Verificar si cumple con las funciones a desarrollarse en su área.	• Cuestionario	

ANEXO N°3. CUESTIONARIO DE CONTROL INTERNO A LA EMPRESA

BANAGINA S.A

BANAGINA S.A.
R.U.C.: 0992636459001
PRODUCTORES DE BANANO

DIRIGIDO AL PERSONAL DE CADA ÁREA (5 PERSONAS)

- SEGURIDAD FISICA

Inventario de equipos de hardware y software

1. ¿La asesoría cuenta con un inventario de hardware y software?
   SI ☐ NO ☐
2. ¿El inventario de hardware y software es constantemente actualizado?
   SI ☐ NO ☐

Control para instalar dispositivos

3. ¿Se realizan mantenimientos frecuentes a los equipos de cómputo?
   SI ☐ NO ☐
4. ¿Se instalan portadores USB para pasar información en los computadores?
   SI ☐ NO ☐

Adquisición de equipos

5. ¿Se pide facturas al momento de realizar una compra de equipos?
   SI ☐ NO ☐

- SEGURIDAD LÓGICA

Acceso de usuarios a las páginas web

6. ¿Es restringido el acceso a páginas web?
   SI ☐ NO ☐
7. ¿Tienen acceso a las redes sociales?
   SI ☐ NO ☐

Existencia de antivirus

8. ¿Los antivirus instalados cuentas con alguna licencia?
   SI ☐ NO ☐

9. ¿Los antivirus son actualizados cada cierto periodo de tiempo?

SI ☐ NO ☐

Acceso de los usuarios a programas o información

10. ¿La asesoría cuenta con respaldos de información en caso de perdidas?

SI ☐ NO ☐

11. ¿Para el acceso al computador se cuenta con claves para cada usuario?

SI ☐ NO ☐

- EMPLEADOS

Cumplimiento de responsabilidades y de políticas

12. ¿Existen políticas sobre el acceso o uso de redes sociales?

SI ☐ NO ☐

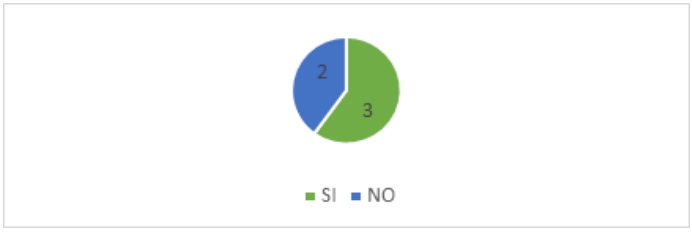
13. ¿El uso de los equipos solo lo realiza el personal de cada departamento?

SI ☐ NO ☐

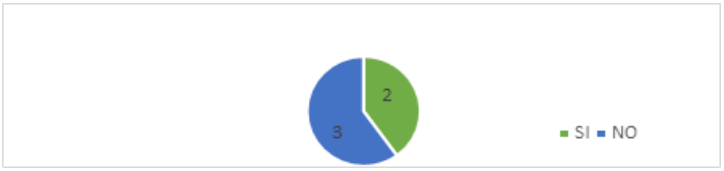
TABULACIÓN DEL CUESTIONARIO

SEGURIDAD FÍSICA

Inventario de equipos de hardware y software

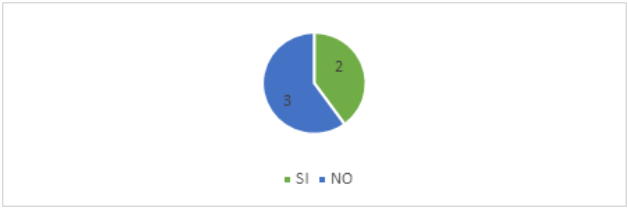


De las 5 personas encuestadas, 3 de ellas dijeron que la empresa SÍ cuenta con un inventario de hardware y software; mientras que 2 dijeron que NO.

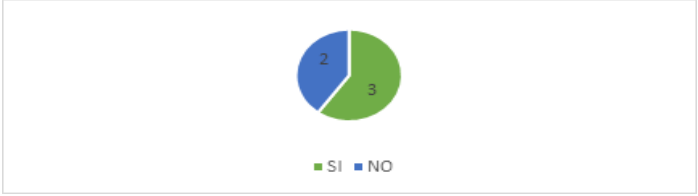


De las 5 personas encuestadas, 2 de ellas dijeron que el inventario SÍ es actualizado; mientras que 3 dijeron que NO.

Control para instalar dispositivos

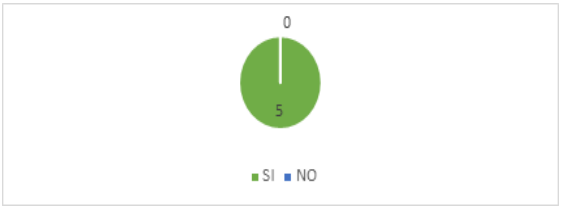


De las 5 personas encuestadas, 2 de ellas dijeron que SÍ se realizan mantenimientos frecuentes a los equipos; mientras que 3 dijeron que NO.



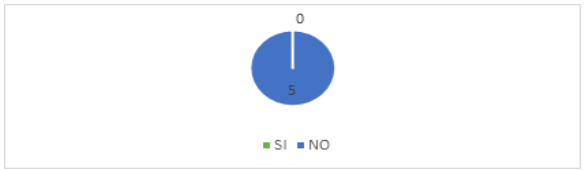
De las 5 personas encuestadas, 3 de ellas dijeron que SÍ se instalan portadores USB; mientras que 2 dijeron que NO.

Adquisición de equipos

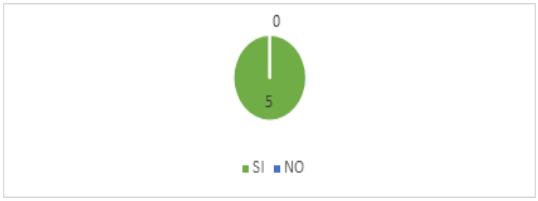


De las 5 personas encuestadas, todos dijeron que si se recibe factura al momento de hacer una adquisición.

SEGURIDAD LÓGICA

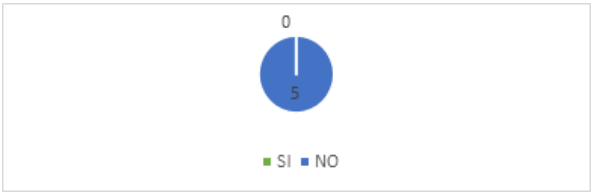


De las 5 personas encuestadas, todos dijeron que NO es restringido el acceso a internet

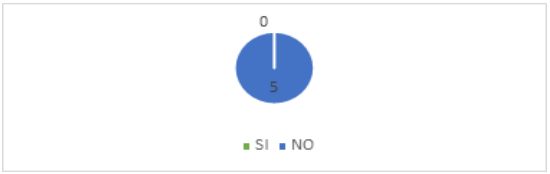


De las 5 personas encuestadas, todos dijeron que SI tiene acceso a las redes sociales.

Existencia de antivirus

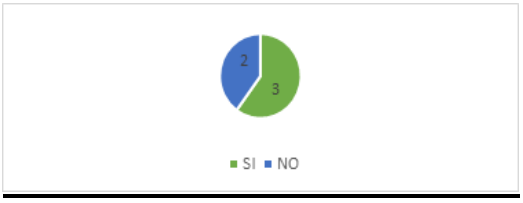


De las 5 personas encuestadas, todos dijeron que NO cuentan con licencias los antivirus.

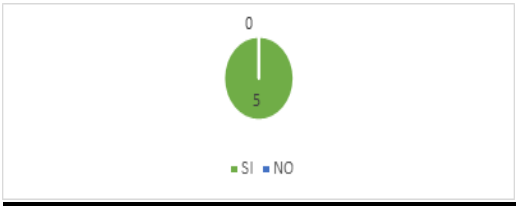


De las 5 personas encuestadas, todos dijeron que NO son actualizados cada cierto periodo.

Acceso de los usuarios a programas o información



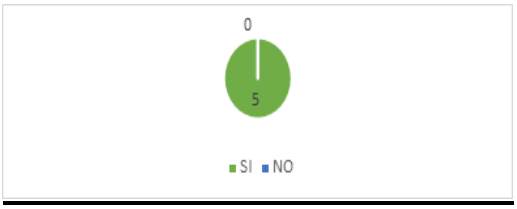
De las 5 personas encuestadas, 3 de ellos dijeron que Si cuentan con respaldos de información en caso de pérdidas.



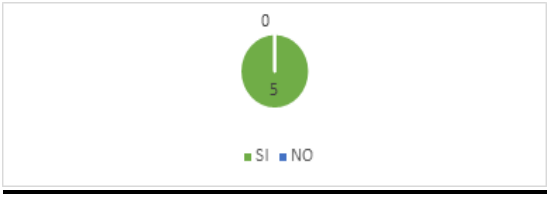
De las 5 personas encuestadas, todos dijeron que SI se cuentan con claves para el acceso a computadores.

EMPLEADOS

Cumplimiento de responsabilidades y de políticas

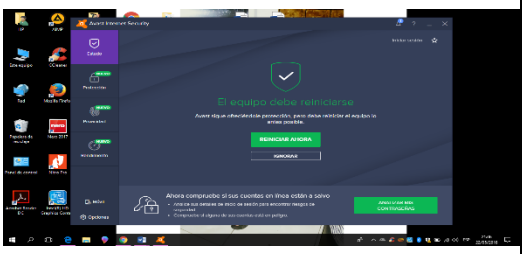


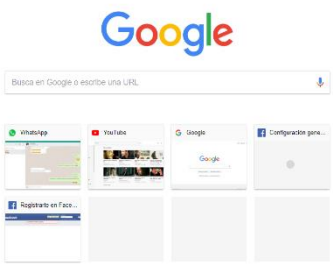
De las 5 personas encuestadas, todos dijeron que existen políticas sobre el acceso a redes sociales



De las 5 personas encuestadas, todos dijeron que el uso de los equipos lo realizan solo el personal de cada departamento.

ANEXO N°4. FICHA DE OBSERVACIÓN

FICHA DE OBSERVACION			
FICHA N°	1		
LUGAR	EMPRESA BANAGINA S.A		
ELABORADO POR:	BRIGITTE GUAYAS		
TIPO DE OBSERVACION	**OBSERVACION**	**COMENTARIO**	**ANEXO**
SEGURIDAD LOGICA	En la fase de la ejecución se ha detectado que las computadoras no cuentan con licencias de antivirus.	Los antivirus no cuentan con licencias lo que permite que fácilmente sea contaminado por virus frecuentemente ocasionando daños a la memoria RAM del computador.	

FICHA DE OBSERVACION			
FICHA N°	2		
LUGAR	EMPRESA BANAGINA S.A		
ELABORADO POR:	BRIGITTE GUAYAS		
TIPO DE OBSERVACION	**OBSERVACION**	**COMENTARIO**	**ANEXO**
SEGURIDAD LOGICA	En la fase de la ejecución se ha detectado que los usuarios hacen uso de las redes sociales en horas laborales.	En los computadores tienen facilidad de acceso a redes sociales por lo que es una distracción para la realización optima de sus actividades.	

ANEXO N° 5. MATRIZ DE RESULTADOS

PUNTOS A EVALUARSE	5: EXCELENTE	4: BUENO	3: SUFICIENTE	2: REGULAR	1: DEFICIENTE
Seguridad Física					
Inventario de hardware y software				X	
Control para instalar dispositivos				X	
Adquisición de equipos			X		
Seguridad lógica					
Acceso de usuarios a las páginas web					x
Existencia de antivirus					x
Acceso de los usuarios a programas o información				x	
Empleados					
Cumplimiento de las políticas y de responsabilidades					x

ANEXO N°6. SITUACIONES RELEVANTES

EMPRESA	ÁREA AUDITADA	SITUACIONES	CAUSA	SOLUCIÓN	FECHA
EMPRESA BANAGINA S.A.	Seguridad física	Existencia de Inventario desactualizado de hardware y software	Existe un inventario manual el cual no está de manera detallada	Elaborar un inventario de manera detallada sobre lo que la empresa cuenta, y lo que debe de adquirir en caso de alguna falencia en el computador.	22/05/2018
	Seguridad física	No existe un Control para instalar dispositivos	No existe un control que prohíba la instalación de USB	Determinar una política de restricción de uso de portadores USB para evitar robos de información, fraudes o instalaciones de programas.	22/05/2018
	Seguridad física	Adquisición de equipos	No existe un control de adquisición de equipos	Verificar de manera detallada la adquisición de equipos mediante las facturas.	22/05/2018
	Seguridad lógica	No existe un control de Acceso de usuarios a las páginas web	No existe un control de que el personal en horas laborables haga uso de las	Establecer políticas que determinen que únicamente se puede hacer uso de los programas contables, Excel, Dimm o cualquier otro que sea	22/05/2018

			redes sociales	necesario para su trabajo y se utilice únicamente el correo electrónico.	
	Seguridad lógica	Desactualización de antivirus	Ciertas computadoras cuentan con licencias para un año y otras cuenta con un antivirus desactualizado	Instalar un antivirus actualizado de manera que el software proteja la información digitalizada de la empresa.	22/05/2018
	Seguridad lógica	No existe un control de Acceso de los usuarios a programas o información	No existe un control de acceso a la información ya que cuentan con la contraseñas para el fácil acceso	Aplicar controles de acceso a los sistemas ya que la empresa pueda mantener la información integra y segura	22/05/2018
	Empleados	No existe un control de políticas y de cumplimiento de funciones	Incumplimiento de políticas y responsabilidades establecidas por la empresa.	Verificar que los empleados cumplan con sus responsabilidades y establecer sanciones en caso de incumplimientos.	22/05/2018
ELABORA: N. B.				APRUEBA: Brigitte Guayas	