UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2017 – MARZO 2018

EXÁMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

INGENIERÍA EN SISTEMAS

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS.

TEMA:

AUDITORÍA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA FÁBRICA QUICORNAC DEL CANTÓN VINCES.

EGRESADA:

FÁTIMA DE LOURDES ANCHUNDIA BUSTAMANTE.

TUTOR:

MSC. JOFFRE LEÓN ACURIO.

AÑO 2018

INTRODUCCIÓN

La Empresa Quicornac S.A. es una empresa multinacional de origen suizo -ecuatoriano dedicada a la producción y comercialización de jugos y concentrados de frutas tropicales, esta empresa ha estado en permanente evolución ya que cuenta con más de 32 fábricas a nivel nacional y mercados internacionales, teniendo su principal fábrica en Vinces en las calles Sucre y Herbert Freire, su matriz en Guayaquil está ubicada en el edificio Conauto, su dirección es Avenida Juan Tanca Marengo en el km 1.8.

La empresa estableció su primera fábrica en el año de 1.989, siendo en el año 1.990 sus primeras funciones con 25 trabajadores, su punto específico de producción era el concentrado y jugo de maracuyá para la exportación, llegando a tener un buen prestigio en el año 1.991 por su buena calidad en la exportación llevó a la empresa a innovar sus maquinarias ahora ya contando con la tecnología adecuada.

La finalidad de este estudio es la auditoria de la infraestructura tecnológica de la fábrica Quicornac S.A. ya que en la actualidad busca el desarrollo de nuevos productos y sistemas de mayor calidad exigidas por los estándares de los organismos de control, para esto se necesita tener una buena seguridad en el sistema de red para que no exista fuga de información.

Se utilizará una metodología basada en la norma internacional que gestiona la seguridad de información en una empresa, la cual puede ser ejecutada en empresas con o sin fines de lucro ya sean éstas grandes o pequeñas, también las empresas pueden ser públicas o privadas, estamos hablando de la norma ISO 27001 y así también utilizaremos buenos estándares de calidad.

En el área de Auditoría se inicia evaluando la parte física de una red, condiciones del cableado estructurado, mantenimiento de la sala de servidores, gabinetes de comunicación, etiquetado de los cables, orden, limpieza.

En esta parte, también se consideran el mantenimiento de los equipos de comunicaciones, tener un inventario actualizado de los equipos de red.

En el área de Redes podemos decir que la clasificación de los diferentes ataques que permiten evitarlos es el modelo OSI (Open System Interconnection), la cual es un modelo de referencia para los protocolos de la red.

Luego se hace una evaluación para que dé como resultado el estado de la red, este resultado no es cualitativo sino cuantitativo utilizando la escala de Likert, la escala de Likert tiene el honor de ser uno de los ítems más populares y utilizados en las encuestas.

A diferencia de las preguntas dicotómicas con respuesta sí/no, la escala de Likert nos permite medir actitudes y conocer el grado de conformidad del encuestado con cualquier afirmación que le propongamos.

Cada día es mayor el número de situaciones irregulares que se presentan, como consecuencia del uso y aplicación de la Tecnología de Información (TI.), en las diferentes organizaciones, entidades, empresas y compañías en general.

Las empresas tienen riesgo de perder tanta información valiosa, esto podría detener su operatividad, deteniendo procesos de producción o administrativo, para esto se necesita proteger el funcionamiento de toda la información existente.

Existen diferentes maneras de proteger un sistema de información, todas las partes del sistema de seguridad deben de trabajar en conjunto para asegurar la información que la empresa posee.

En lo que es seguridad, debemos saber que las redes permiten la comunicación entre dispositivos llamados inteligentes, pero también sabemos que es el medio principal por los que los dispositivos son infectados con virus para robar información confidencial, las necesidades de tener entornos seguros en la red cada vez son más necesarias.

La línea de investigación de la Facultad de Administración Finanzas e Informática F.A.F.I., para realizar el caso de estudio se enmarca en el Desarrollo de Sistemas de comunicación e información y emprendimiento empresariales y tecnológicos.

La sub línea de investigación de éste estudio de caso se basa en el Proceso de Transmisión de Datos y Telecomunicaciones.

DESARROLLO

La Fábrica Quicornac en el año 1995, incursiona en el mercado nacional con su marca Sunny convirtiéndose en uno de los líderes en el mercado de los néctares de fruta natural, empezando con néctar de durazno para después así ir agregando poco a poco los demás sabores que se encuentran en el mercado.

El tiempo para detectar las vulnerabilidades será a corto plazo, haciendo la respectiva investigación de campo para sacar el resultado necesario y así poder brindar el respetivo control según la necesidad del caso.

En todo objeto de estudio se necesita estabilidad y protección de información o bienes, en el ámbito informático sabemos que la herramienta principal que ayuda la propagación en el mundo son las computadoras, y éstas necesitan estar protegidas.

Es por esto que es importante saber los factores de protección informática, mostrando los métodos, conociendo los tipos y medios a nuestro sistema de información en una red de datos.

Con todos los conocimientos adquiridos se puede informar a los usuarios lo que deben saber para no caer en los famosos ataques en línea o virus informáticos.

Las empresas tienen riesgo de perder tanta información valiosa, esto podría detener su operatividad, deteniendo procesos de producción o administrativo, para esto se necesita proteger el funcionamiento de toda la información existente.

En este trabajo de investigación identificaremos las realidades acerca de la seguridad informática y describiremos errores comunes y amenazas para la seguridad informática.

¿Cuál es la incidencia de realizar una auditoría en la infraestructura tecnológica de la fábrica QUICORNAC S.A. del cantón Vinces?

Determinar la situación actual, vulnerabilidad y fortaleza de una red de datos, ya que una empresa necesita saber cómo está la situación de sus redes para así tomar la decisión de mejorarlas o cambiarlas, a su vez determinar los estándares a ser utilizado de acuerdo al análisis realizado por el profesional, con lo que se podría determinar un plan de mejoras que nos permita darle una mejor seguridad a las redes de la empresa.

Una auditoría de la infraestructura tecnológica, es indiscutiblemente un control de una red en una institución, con la finalidad de examinar dentro de un determinado tiempo toda operación que este sistema lleve a cabo con la base de prestar un buen servicio con los más altos niveles de acreditación para dicha institución.

La parte importante en la auditoría en la infraestructura tecnológica, es la comprobación y evaluación de cómo se están manejando por parte del personal de sistemas, las políticas y procedimientos dados por la directiva de la empresa, para así llevar un control y evitar posibles fallas que pueden ser perjudicial para el procedimiento de auditoría y así obtener el mayor beneficio económico y cumplir con todos los objetivos propuestos por la institución.

La existencia de una auditoría en la infraestructura tecnológica, con su implementación puede ser una parte muy decisiva para optimizar recursos y así poder lograr todas las Metas, Objetivos, Misión y Visión de la Fábrica QUICORNAC S.A.

Para tal efecto se realizará un manual que será quien permita un buen funcionamiento de dicha auditoría, y garantizar la validez de los resultados obtenidos para ser comparados en un nuevo periodo de auditoría posteriormente.

La empresa cuenta con certificación nacional ISO 9001 2000*, BASC*, HACCP*.

Según (iso9001calidad, 2013) la norma ISO 9001 2000 es una norma internacional aceptada por innumerables organizaciones y empresas que define los requisitos mínimos que debe cumplir un sistema de gestión de calidad para ser certificado.

La certificación BASC, los elementos que cubren esta norma son todos esenciales para un sistema eficaz de Gestión de Control y Seguridad en el Comercio Internacional. Los factores humanos, incluyendo la cultura, políticas, etc., dentro de las organizaciones, pueden crear o destruir la eficacia de cualquier sistema de administración y se deben considerar cuidadosamente al implementar esta norma. (Organization, 2015-2016)

Dentro de la certificación HACCP (Corporativa, 2014) nos explica que es el Análisis de Peligros y Puntos Críticos de Control, es un proceso sistemático preventivo para garantizar la inocuidad alimentaria, de forma lógica y objetiva. Desarrollado en los años 50 por compañías alimentarias de Estados Unidos como Pillsbury y potenciado en los años 80 por instituciones que a nivel mundial impulsaron su aplicación tales como la Organización Mundial de la Salud, continúa siendo una herramienta insustituible de prevención de los riesgos en la producción de alimentos.

Esta empresa está dándole a la ciudadanía un gran cambio, porque así genera trabajo a personas que son de muchos sectores del cantón.

El fin es hacer una auditoría rigurosa y un análisis de sus redes actuales, con toda precisión, asuntos clave relacionados con la red, cómo el lugar en el que las nuevas aplicaciones empresariales generarán nuevas demandas de red, etc. Es con el afán de crear una base sólida para el posterior diseño de red y para proyectos de despliegue.

Para el informático y para el auditor informático, el entramado conceptual que constituyen las redes nodales, líneas, concentradores, multiplexores, redes locales, etc. no son sino el soporte físico-lógico del tiempo real.

Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.

La decisión de abordar una auditoria Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Se elaboran "matrices de riesgo", en donde se consideran los factores de las "Amenazas" a las que está sometida una instalación y los "Impactos" que aquellas puedan causar cuando se presentan. Las matrices de riesgo se representan en cuadros de doble entrada "Amenaza-Impacto", en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz.

En lo que vamos a auditar será:

Tabla 1: TABLA DE DETALLES DE LO AUDITADO.

DETALLE	EXISTENCIAS
Computadoras de escritorio.	3
Computadoras personales.	4
Software crítico.	1
Licencias en uso.	6

Fuente: Fátima Anchundia Bustamante.

Tabla 2: DETALLES DE LO AUDITADO.

Equipos	Ficha Técnica
Computadora de escritorio (1, 2, 3)	Pentium IV, Disco duro 250 Gb, RAM 500, S.O. Windows XP Professional
Computadoras personales.	Intel Core i3, disco duro 500 Gb, RAM 4gb, S.O. Windows 8
Software crítico.	Software contable de la empresa, Latinium
Licencias en uso.	Licencias para software S.O. en portátiles, ninguna para computadoras de escritorio.

Fuente: Fátima Anchundia Bustamante.

.

Tabla 3: MATRIZ DE RIESGO.

MATRIZ DE RIESGO

Elaborado Por: Fátima Anchundia Bustamante.

Realizado Por: Fátima Anchundia Bustamante.

Fecha: 11 de enero del 2018

RIESGO	AMENAZA	IMPACTO	TOTAL
1.- Cortes De Energía.	3	3	9
2.- Incendios dentro o fuera de la empresa.	3	2	6
3.- Perdida de máquinas	3	2	6
4.-. Virus.	3	2	6
5.- Terremotos.	2	2	4
6.- Suspensión del internet.	2	2	4
7.- Fallas por hardware	1	3	3
8.- Fallas por software	3	1	3
9.- Digitar incorrectamente los datos de la empresa.	2	1	2
10.- Violación al sistema.	1	1	1

Fuente: Fátima Anchundia Bustamante.

Después de realizarse la observación al sistema, podemos acotar que los riesgos más probables según la tabla realizada se mostraría en orden descendente como se muestra en la matriz, todo esto según datos dados por el personal del área de sistemas de la fábrica.

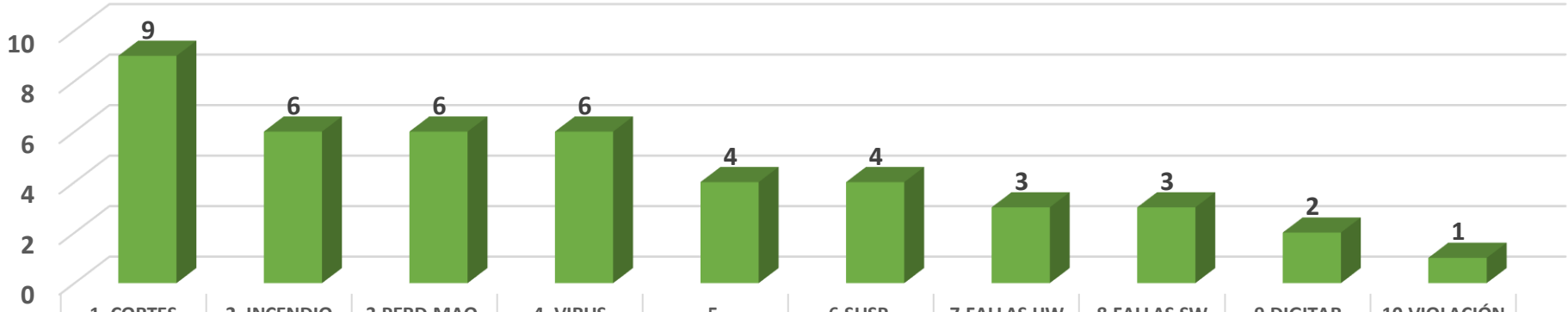
Los identificaron así dentro de la tabla de rangos, ubicando el riesgo de mayor probabilidad de riesgo, a menor:

Tabla 4: RANGOS DE RIESGOS

RANGO	RIESGO	PROBABILIDAD
10 – 8	▪ Corte de energía.	**ALTO**
7 – 4	▪ Incendios dentro o fuera de la fábrica. ▪ Pérdida de máquinas. ▪ Virus. ▪ Terremotos. ▪ Suspensión del internet.	**MEDIO**
3 – 0	▪ Fallas de Hardware. ▪ Fallas de Software. ▪ Digitar incorrectamente los datos de la empresa. ▪ Violación al sistema.	**BAJO**

Fuente: Fátima Anchundia Bustamante.

MATRIZ DE RIESGO



	1. CORTES	2. INCENDIO	3.PERD.MAQ.	4. VIRUS	5. TERREMOTOS	6.SUSP. INTER.	7.FALLAS HW	8.FALLAS SW	9.DIGITAR	10.VIOLACIÓN
MATRIZ DE RIESGO	9	6	6	6	4	4	3	3	2	1

Fuente: Fátima Anchundia Bustamante.

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos.

El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando la cumplimentación de cuestionarios pre impresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Se requieren varios pasos para realizar una auditoría. El auditor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de auditoría que consta de objetivos de control y procedimientos de auditoría que deben satisfacer esos objetivos.

El proceso de auditoría exige que el auditor de sistemas reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de auditoría que presente esos temas en forma objetiva a la gerencia. Asimismo, la gerencia de auditoría debe garantizar una disponibilidad y asignación adecuada de recursos para realizar el trabajo de auditoría además de las revisiones de seguimiento sobre las acciones correctivas emprendidas por la gerencia.

Tabla 5: MATRIZ DE RIESGO Y DE CONTROL

MATRIZ DE RIESGO Y DE CONTROL.

Área: Entorno lógico y físico.
Fecha: 11 de enero del 2018
Elaborado por: Fátima Anchundia Bustamante.

RIESGOS ENCONTRADOS	CONTROL 1	CONTROL 2	CONTROL 3	TOTAL CONTROL EXISTENTES EN LA FÁBRICA
1.- Cortes de Energía	• Conexiones ininterrumpidas.	• Existen regletas con sobrecarga de conexiones.		1
2.- Incendios dentro o fuera de la empresa.	• Alarmas contra incendio. • Contratar servicios especializados.	• Mantener los extinguidores recargados y en buen estado.	• Capacitar a todo el personal sobre un plan de evacuación.	3
3.- Perdida de máquinas	• Sobre la seguridad física • Control al área de equipos sólo a personas autorizadas. • Crear respaldos y mantenerlos en lugares estratégicos.	• Hacer inventarios de cada equipo que llegue al área. • Instalaciones de cámaras de vigilancia, alarmas, rejas, sensores de movimientos, caja fuerte.	• Poner clausulas o anexos en los contratos del personal que se integre al manejo de la información confidencial de la empresa.	2
4.- Virus.	• Instalar programas que detecten virus o ataques en la red.	• Lectura de puertos USB automática, desactivada.	• Permisos solo para archivos de lectura.	2
TOTAL DE RIESGOS				8

Fuente: Fátima Anchundia B.

INFORME DEL CONTROL INTERNO

Fecha: 18 de enero del 2018
Fábrica Quicornac
Planta Vinces.

Auditoría:

Evaluación del entorno lógico y físico, a los equipos utilizados por el personal del área de sistemas.

Objetivos:

Evaluar los riegos, las causas y los efectos que pueden ser peligrosos para los datos en todos los equipos.

Alcance:

Ésta auditoría está diseñada para realizar la evaluación del control de la infraestructura tecnológica de la empresa Quicornac de Vinces, reconocer los riesgos que existen en el entorno lógico y físico.

Importancia del área auditada:

Es importante realizar dicha auditoria en el área de la fábrica para determinar en qué grado de operatividad se encuentran los equipos y así poder tomar una decisión final en mejorarlos o desecharlos.

Conclusión general:

Dentro del estudio realizado se detectó riesgos que no han sido solucionados por los directivos ni por los trabajadores de la fábrica, dando como resultado que se puede perder información en el momento menos indicado, sin poder recuperarla debido a una falla o a un mal uso de parte del encargado de manejar dicha información.

Dentro de lo que es el entorno se puede expresar que no se encuentran en un lugar seguro, ya que están expuestos a varios factores climatológicos, robo, incendios, sobrecarga de energía, que son agentes para que se pueda perder información y la máquina en sí.

Recomendaciones y observaciones:

Observación 1: Lo que podemos añadir como observación es que los trabajadores no cuentan con una buena capacitación sobre la seguridad de los equipos.

Observación 2: Se conoció que los trabajadores no cumplen con un plan de contingencia porque los directivos no se los han propuesto.

Observación 3: No cuentan con la táctica para poder recuperar información perdida.

Recomendación 1: Proponiendo que se les haga extensivo un manual de usuario donde conste cada parte especificada para así ellos puedan trabajar mejor conociendo cada parte de su equipo de trabajo.

Recomendación 2: Buscar estrategias para cumplir o dar ideas para hacer un plan de contingencia que sea analizado y darle seguimiento continuamente.

Recomendación 3: Capacitar a los empleados para que aprendan a realizar copias de seguridad en caso de algún error humano involuntario, contratar a especialistas para que los capacite y así poder salvar la información que es vulnerable perder.

Auditora:

Fátima Anchundia Bustamante.

Realización de auditorías según procedimiento y plan definidos. Es conveniente que el personal que va a ser auditado conozca con antelación tal hecho, y lo mejor desde el punto de vista práctico es que la realización de auditorías sea sistemática, y el propio director o responsable del área a auditar transmita a sus subordinados afectados las fechas concretas en las que estas auditorías sistemáticas van a realizarse para que presten su mayor colaboración.

Posiblemente si se sigue este sistema, al recibir los responsables esta comunicación, tratarán de inculcar en sus subordinados la necesidad de que todo esté "en perfecto estado de revista" como se decía antiguamente, lo que inicialmente podría alterar los resultados, pero si las auditorias son periódicas, esto dejará de producirse, y sin embargo el que el responsable comunique a sus subordinados las fechas de realización.

Se trata de auditar la efectividad del sistema, tanto a través del propio sistema y su grado de cumplimiento, como a través de la calidad del producto obtenido, por lo que es necesario, para poder establecer las acciones correctoras, determinar el grado de cumplimiento del sistema, y su relación con la calidad del producto final.

Herramientas y Técnicas para la Auditoria.

Cuestionarios:

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor.

Entrevistas:

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

- Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.

- Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
- Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

Checklist:

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber, y por qué. Sus cuestionarios son vitales para el trabajo de análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para la cumplimentación sistemática de sus Cuestionarios, de sus Checklists.

Hay opiniones que descalifican el uso de las Checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero esto no es usar Checklists, es una evidente falta de profesionalismo. El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes. El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula. Esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer.

Los cuestionarios o Checklists responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

Finalmente, nos expresa (Ortíz, 2013) que ha de indicarse la conveniencia de que el auditor confeccione personalmente determinadas partes del Informe. Para ello, resulta casi imprescindible una cierta soltura en el manejo de Procesadores de Texto, paquetes de Gráficos, Hojas de Cálculo, etc.

AUDITORÍAS DE SEGURIDAD EN LA RED CORPORATIVA

Las auditorías juegan un papel relevante ya que permiten mostrar el estado en el que se encuentra la protección de la información y de los activos dentro de las organizaciones. Además, involucra la identificación, análisis y evaluación de debilidades en las medidas de seguridad que han sido aplicadas, así como de los componentes tecnológicos de la empresa.

En el caso específico de las redes, la auditoría está relacionada con un método o un conjunto de ellos para verificar el cumplimiento de los requisitos de seguridad, necesarios dentro de una colección de dispositivos interconectados -como pueden ser routers, switches, hubs, computadoras y dispositivos móviles, entre otros.

Revisiones técnicas o de cumplimiento

Según lo que explica (Mendoza, 2015) Las revisiones de cumplimiento o gestión permiten conocer el estado de apego en las prácticas que se llevan a cabo en las organizaciones relacionadas con la protección de las redes, en comparación con lo que establecen documentos especializados, como pueden ser estándares de seguridad, marcos de referencia o requisitos que deban ser cumplidos.

AUDITORÍA DE LA CALIDAD

Las auditorías de calidad son aquellas en las que se evalúa la eficacia del sistema de gestión de calidad de la organización. Normalmente, se auditan sistemas de gestión de la calidad conformes a la norma UNE-EN-ISO 9001:2008 puesto que esta es la norma mundial que

describe los requisitos de un sistema de gestión de la calidad, no obstante, también existen otros estándares propios de sectores particulares (por ejemplo, ISO/TS 16949:2009 para el sector de la automoción) o de determinadas actividades (por ejemplo, UNE 13816 de calidad en el transporte público de pasajeros).

La norma UNE-EN ISO 19011 proporciona orientación sobre los principios de auditoría, la gestión de programas de auditoría, la realización de auditorías de sistemas de gestión de la calidad y ambiental, así como sobre la competencia de los auditores.

Lo que se explica en (AEC, 2017) es que las auditorías de calidad ofrecen a las organizaciones confianza sobre la eficacia de su sistema de gestión de la calidad y su capacidad para cumplir los requisitos del cliente. Igualmente, las organizaciones pueden acceder a la obtención de certificados de gestión de la calidad a través de un proceso de auditoría de calidad que lleva a cabo una entidad certificadora.

El término calidad se ha convertido en una de las palabras clave de nuestra sociedad, alcanzando tal grado de relevancia que iguala e incluso supera en ocasiones al factor precio, en cuanto a la importancia otorgada por el posible comprador de un producto o servicio.

Las redes de la fábrica se encuentran en un estado medio, ni bueno ni malo según nuestro estudio de campo. El propósito y la actividad de la auditoría es recoger, examinar y analizar la información necesaria para tomar las decisiones de aprobación. La auditoría debe tener capacidad para investigar la pericia técnica, el desarrollo del software o la calidad del departamento de desarrollo, el esfuerzo disponible, el soporte del mantenimiento o la efectividad de la gestión.

INFRAESTRUCTURA TECNOLÓGICA

Y si se habla de lo que se trata una infraestructura tecnológica, se puede decir como una breve introducción que es un conjunto de hardware y software, donde están varios servicios que una empresa necesita para que toda actividad sea realizada con éxito.

Dentro de lo que se refiere a hardware se encuentra lo que son las cámaras de seguridad, servidores, aires acondicionados, sensores, entre los elementos de red se puede hablar de lo que es un firewall o cortafuegos, que es quien nos bloquea o nos da el acceso de tráfico entre los puntos, computadoras, impresoras, estabilizadores de corriente, teléfonos, etc.

De lo que es software, se mencionan a los sistemas operativos y software de sistema, que son aplicaciones generales necesarias.

Como nos explica (Morales, 2013) en su capítulo 4, de la sección Diseño de la infraestructura, que se comenzará inicialmente generando el diagnóstico de la infraestructura actual, donde se realiza el levantamiento de la información de todos los elementos tecnológicos de la empresa, después se exhibe en un diagrama la interacción entre ellos a fin de conocer de forma general la arquitectura física de la infraestructura contenida con los elementos tecnológicos. Luego se reconoce cual es la arquitectura de la información, es decir, la forma en que los datos son utilizados y así poder identificar los elementos tecnológicos mínimos y políticas necesarias.

TIPO DE INVESTIGACIÓN

Se ha realizado la investigación de campo en las que se ha podido analizar la situación en las que se trabajan en la empresa.

Encuesta al personal del área de sistemas y trabajadores de distintas áreas en sus respectivas oficinas.

Entrevista con los superiores de la institución para saber cuál sería el método o la seguridad con la que respaldan su información.

La más adecuada en este tipo de investigación sería Checklist por ser la de mayor utilización y menos compleja, no se necesita tener mucho conocimiento informático para hacer una auditoria mediante esta técnica, solo tener en claro que es lo que se va a realizar sin tantos conceptos sin comprender.

Como dice (Jarrín Ortiz, 2013) que los conocimientos fundamentales que debemos tener para manejar mejor una auditoria son:

- Minicomputador
- Red local
- Periféricos
- Software de base
- Seguridad lógica y física

Y en lo investigado se encontró con lo que (Parra, 2014) explica, el informe final deberá presentarse por escrito, acompañado de una exposición verbal para asegurar que la interpretación del informe sea adecuada, tanto en los resultados como en las recomendaciones. En este informe se dará información clara y concisa, sobre los resultados obtenidos después de la auditoria, se darán recomendaciones para mejorar el área auditada.

CONCLUSIONES

- Con la determinación de la situación actual de las redes se ha podido comprobar que la vulnerabilidad en la empresa QUICORNAC SA es un factor muy alto, por lo tanto, se puede acceder muy fácilmente por personas ajenas a dicha institución y deben ser cambiadas a la brevedad posible, para así poder combatir posibles robos de información, virus, etc.
- Se determinarán los estándares a ser utilizado de acuerdo al análisis realizado por el profesional.
- Se elaborará un plan de mejoras para darle una mejor seguridad a las redes de la empresa, que sería un reto profesional al momento de ser creativos en la elaboración del plan, ya que nos puede permitir incorporar nuevos puntos de redes, al sumarse más producción.

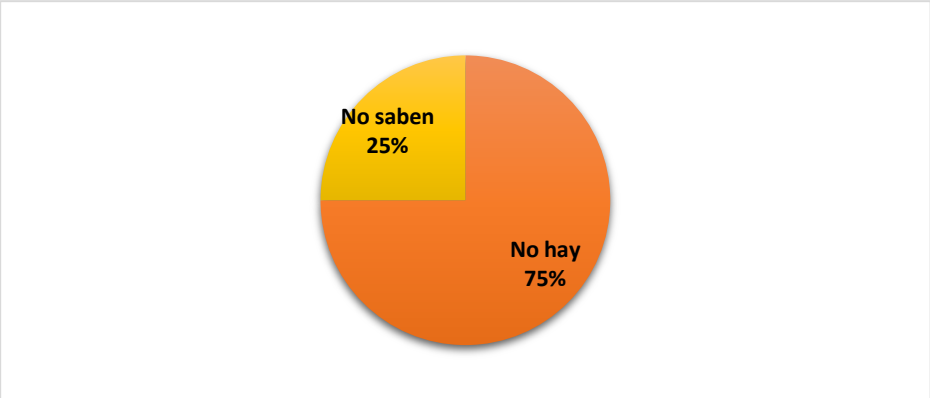
ANEXOS

Dentro de una encuesta que se realizó 8 preguntas a 30 personas dentro de la fábrica, obteniendo los siguientes resultados.

1.- Existe una implementación de evaluación a Hardware y Software para detectar fallos en el sistema.

R: El 75% manifestó que no lo hay, el otro 25% no tiene idea de aquello.

Grafico 1: Implementación de evaluación a Hardware y Software.



Fuente: Fátima Anchundia Bustamante.

NO HAY	**22 personas**	**75%**
NO SABEN	**8 personas**	**25%**
TOTAL	**30 personas**	**100%**

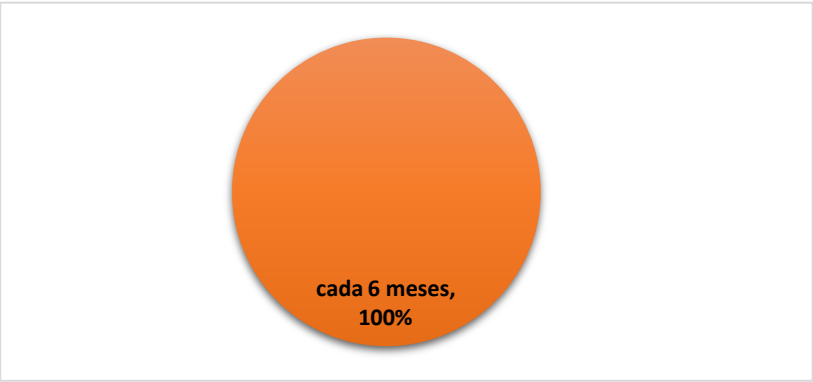
Tabla 1: Implementación de evaluación a Hardware y Software.

Fuente: Fátima Anchundia Bustamante.

2.- ¿Se hace mantenimiento de rutina para contrarrestar fallos en el hardware?

R: Si, Cada 6 meses, mediante contratación de personal especializado. El 100% estuvieron de acuerdo.

Gráfico 2: Se hace mantenimiento de rutina



Fuente: Fátima Anchundia Bustamante.

SI	30 personas	100%
NO	0 personas	0%
TOTAL	30 personas	100%

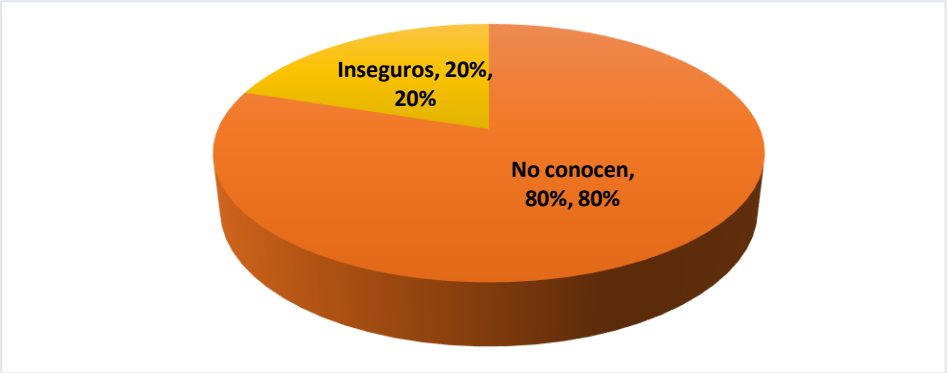
Tabla 2: SE HACE MANTENIMIENTO DE RUTINA

Fuente: Fátima Anchundia Bustamante.

3.- ¿Hay una protección de software dentro de lo que es configuración y mantenimiento, teniendo parámetros establecidos?

R: No tienen conocimiento el 80%, el 20% restante está inseguro.

Gráfico 3: Hay protección de Software



Fuente: Fátima Anchundia Bustamante.

NO	24 personas	80%
INSEGUROS	6 personas	20%
TOTAL	30 personas	100%

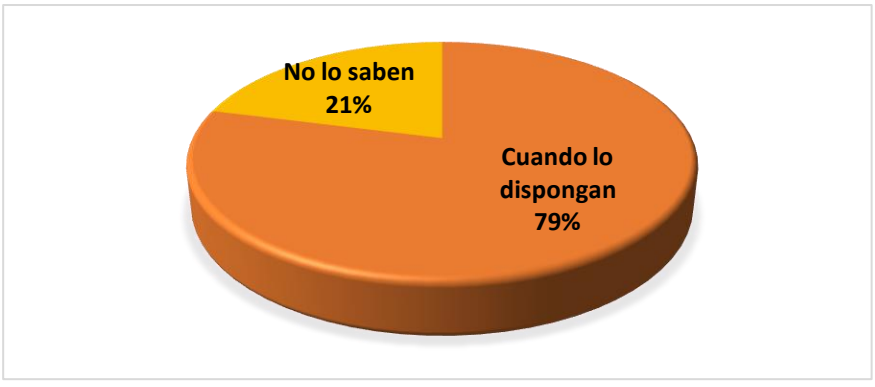
Tabla 3: Hay protección de Software

Fuente: Fátima Anchundia Bustamante.

4.- ¿El mantenimiento lo hacen basado a fechas específicas, siguiendo un itinerario?

R: El 79% dicen que es cuando los directivos dispongan, no tienen una fecha específica ni siguiendo un régimen, el 21% no lo saben.

Gráfico 4: Mantenimiento en fechas específicas.



Fuente: Fátima Anchundia Bustamante.

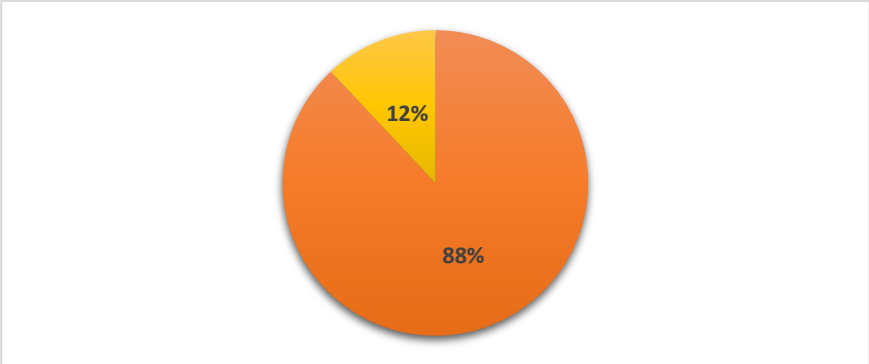
DIRECTIVOS	**24 personas**	**79%**
NO SABEN	**6 personas**	**21%**
TOTAL	**30 personas**	**100%**

Tabla 4: Mantenimiento en fechas específicas.
Fuente: Fátima Anchundia Bustamante.

5.- ¿El software es instalado de acuerdo a las bases de mantenimiento y adquisición?

R: 88% dicen que sí es instalado mediante las bases, mientras tanto el 12% no saben cómo se instala.

Gráfico 5: Sw instalado a las bases de mantenimiento.



Fuente: Fátima Anchundia Bustamante.

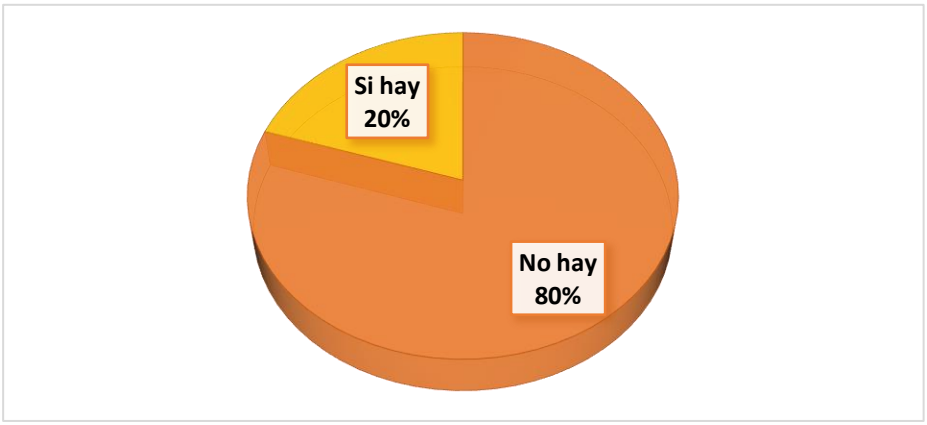
SI	**26 personas**	**88%**
NO	**4 personas**	**12%**
TOTAL	**30 personas**	**100%**

Tabla 5: Sw instalado a las bases de mantenimiento
Fuente: Fátima Anchundia Bustamante.

6.- ¿Se han agregado opciones para modificar, agregar o eliminar datos que garanticen el control del acceso?

R: Dentro de lo encuestado, el 80% aseguran que no hay y el 20% dicen que si hay opciones.

Gráfico 6: Agregar opciones para garantizar el control Del acceso



Fuente: Fátima Anchundia Bustamante.

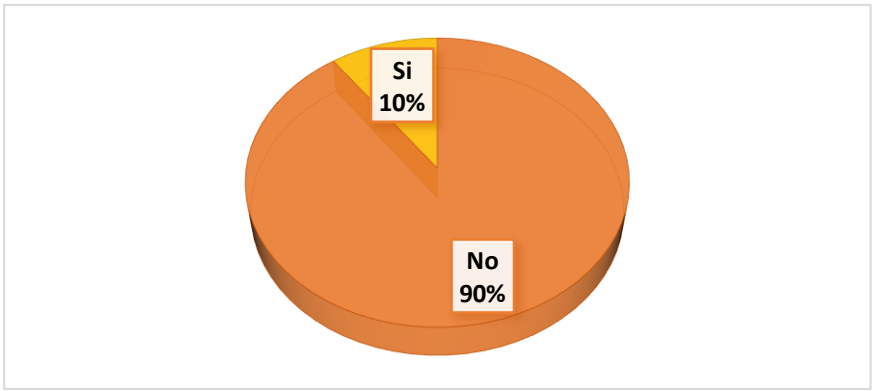
NO	**24 personas**	**80%**
SI	**6 personas**	**20%**
TOTAL	**30 personas**	**100%**

Tabla 6: Agregar opciones para garantizar el control Del acceso.
Fuente: Fátima Anchundia Bustamante.

7.- Las políticas de la fábrica, aseguran el envío de documentación confidencial dentro de una red segura.

R: No aseguran tener buena red aseguran un 90%, mientras que el 10% dicen que sí lo hay.

Gráfico 7: Aseguran el envío de documentación segura



Fuente: Fátima Anchundia Bustamante.

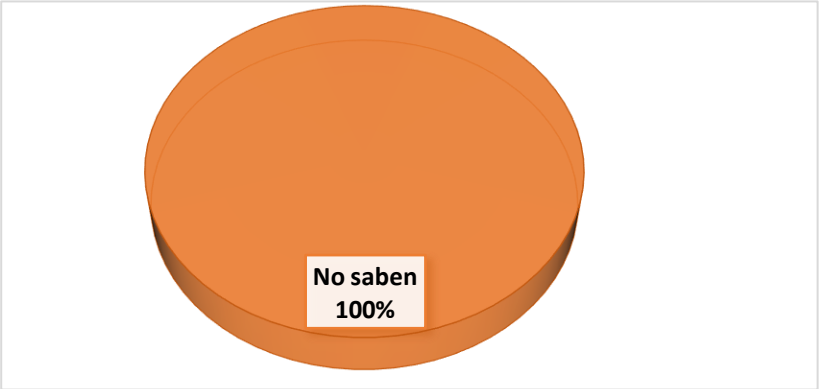
NO	**27 personas**	**90%**
SI	**3 personas**	**10%**
TOTAL	**30 personas**	**100%**

Tabla 7: Aseguran el envío de documentación segura.
Fuente: Fátima Anchundia Bustamante.

8.- El hardware y software se encuentran protegidos para poder hacer la difusión de claves secretas

R: No saben del tema, coincidieron todos, 100%

Gráfico 8: Hardware y software se encuentra protegidos



Fuente: Fátima Anchundia Bustamante.

SI	**0 personas**	**0%**
NO SABEN	**30 personas**	**100%**
TOTAL	**30 personas**	**100%**

Tabla8: Hardware y software se encuentra protegidos.
Fuente: Fátima Anchundia Bustamante.

Imágenes de las plantas en Vinces, Guayaquil y Perú

Matriz En Guayaquil

Planta En Vinces

Planta En Olmos – Perú

Un trabajador cumpliendo su jornada.

Productos que son elaborados en la Fábrica Quicornac.

Ecuador.

Perú.

BIBLIOGRAFÍA

Acosta, D.; González, A. y Díaz, O. 2011. Proceso de auditoría de la calidad para la actividad productiva.

Universidad de las ciencias informáticas (UCI). La Habana, Cuba. Vol. 32. Nº 2. p 97.

AUDISA (Auditoría Informática S.A). 2009. Qué es un Checklist- para qué sirve. (En línea). ES.

Consultado el 22 de dic. 2014. Formato HTML. Disponible en: https://audisa.wordpress.com/2007/11/02/checklist-%C2%BFque-es%C2%BFpara-que-sirve/

Castells, M. 2010. La Sociedad red: una Visión Global. Edición Especial. Madrid.

Revista Venezolana de Información, Tecnología y Conocimiento. p 139 ESPE (Escuela Superior Politécnica del Ejército). 2010. Planificación de Auditoría. (En línea). EC.

Consultado el 20 de oct. 2014. Formato PDF. Disponible en: http://ai.espe.edu.ec/wp-content/uploads/2012/07/Manualde-Auditoría-Gubernamental-Cap-V.pdf

Govindan, M. 2007. Control Interno, Auditoría y Seguridad Informática. Tomo II – IV. España.

Loor, A y Espinoza, V. 2014. Auditoría de seguridad física y lógica a los recursos de tecnología de información en la carrera informática de la ESPAM MFL. Tesis. Ing. Informática. ESPAM MFL. Calceta-Manabí, EC. p 34

Martínez, A; Blanco, B; Loy M. 2012. Auditoría con Informática a Sistemas Contables. Revista de Arquitectura e Ingeniería, Vol. 6, Nº 2. p 1-14. Mira, J. s.f. Informes de Auditoría. (En línea). EC.

Consultado el 4 de Sept. 2014. Formato PDF. Disponible en: http://www.miramegias.com/auditoria/files/present/ut05s.pdf

Nava, J. s.f. Apuntes de Auditoría Informática. (En línea) EC. Consultado el 14 mayo 2014. Formato PDF.

Disponible en: http://www.escet.urjc.es/~ai/T1Apuntes.pdf

Ramírez, J y Álvarez, E. 2009. Auditoría a la Gestión de las Tecnologías y Sistemas de Información. Perú.

Universidad Nacional Mayor de San Marcos. Vol. 6. p. 99-102.

UOC (Universat Oberta de Catalunya). 2013. Infraestructura Tecnológica. (En línea) ES.

Consultado el 10 de mayo 2014. Formato HTML. Disponible en: http://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/index.html

Vásquez, R. s.f. Gestión Integral de Riesgos de Tecnologías de Información. (En línea).

Consultado el 22 de mayo 2014. Formato PDF.

Disponible en: http://www.share-pdf.com/ae5edbbca89945a7bfef43d893ad5fa6/6%20

Gestion%20Integral%20de%20Riesgos%20TI.pdf Villardefrancos, M y Rivera, Z. 2006.

La auditoría como proceso de control: concepto y tipología. Cuba. Ciencias de la Información. Vol.37. p. 53-59.

Yáñez, C. 2011. Enfoque Metodológico de la Auditoria a las Tecnologías de Información y Comunicación. Seudónimo 6. Chile. Pág. 17-26.

Disponible en:

http://www.olacefs.com/Olacefs/ShowProperty/BEA%20/Repository/Olacefs/uploaded/content/article/20120829_1.pdf 112

Whitten, J. 2008. Análisis y Diseño de Sistemas de Información. 2 ed. Editorial McGraw Hill Interamericana. Argentina. Buenos Aires. _____ 2010.

La auditoría, concepto, clases y evolución. 12 ed. Editorial McGraw Hill Interamericana. Colombia.

http://www.quicornac.com

http://ri.ufg.edu.sv/jspui/bitstream/11592/7106/3/657.458-A385m-Capitulo%20II.pdf

http://tecnicasdeauditoriainvest.blogspot.com/

http://www.aprendaredes.com/blog/como-hacer-auditoria-de-redes/

http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4638/0058M733.pdf?sequence=1

http://dspace.udla.edu.ec/bitstream/33000/3497/1/UDLA-EC-TTRT-2013-01%28S%29.pdf

http://www.lsqa.com/certificacion

http://iso9001calidad.com/iso-9001-2000-sistemas-gestion-calidad-requisitos-21.html

http://www.wbasco.org/espanol/normas.htm

https://www.aec.es/web/guest/centro-conocimiento/auditoria-de-calidad

https://itestrada.files.wordpress.com/2011/10/tesis-seguridad-informc3a1tica.pdf

http://biblioteca.usac.edu.gt/tesis/08/08_0249_CS.pdf