ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

CARRERA DE INGENIERÍA CONTABILIDAD Y AUDITORÍA

AUDITORÍA INFORMÁTICA A LA EMPRESA MASTER TECHNOLOGY, CANTÓN QUITO, PROVINCIA DE PICHINCHA

Trabajo de titulación

Tipo: Proyecto de investigación

Presentado para optar al grado académico de:

INGENIERA EN CONTABILIDAD Y AUDITORÍA C.P.A

AUTORA:

DIDIMA JOHANNA UCLES ROMO

Riobamba – Ecuador

2020

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

CARRERA DE INGENIERÍA CONTABILIDAD Y AUDITORÍA

AUDITORÍA INFORMÁTICA A LA EMPRESA MASTER TECHNOLOGY, CANTÓN QUITO, PROVINCIA DE PICHINCHA

Trabajo de titulación

Tipo: Proyecto de investigación

Presentado para optar al grado académico de:

INGENIERA EN CONTABILIDAD Y AUDITORÍA C.P.A

AUTORA: DIDIMA JOHANNA UCLES ROMO

DIRECTOR: ING. WILLIAN GEOVANNY YANZA CHÁVEZ

Riobamba – Ecuador

2020

Yo, Didima Johanna Ucles Romo, declaro que el presente trabajo de titulación es de mi autoría, y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes, están debidamente citados y referenciados.

Como autora, asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación. El patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo

Riobamba, 24 de agosto del 2020

Didima Johanna Ucles Romo
C.C.: 210082815-7

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

CARRERA DE INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

El tribunal del trabajo de titulación certifica que: El trabajo de titulación: Tipo: Proyecto de Investigación, **AUDITORÍA INFORMÁTICA A LA EMPRESA MASTER TECHNOLOGY, CANTÓN QUITO, PROVINCIA DE PICHINCHA**, realizado por la señorita: **DIDIMA JOHANNA UCLES ROMO**, ha sido minuciosamente revisado por los Miembros del Tribunal del trabajo de titulación. El mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	**FECHA**
Ing. Marco Antonio Gavilanes Sagñay **PRESIDENTE DEL TRIBUNAL**	MARCO ANTONIO GAVILANES SAGNAY Firmado digitalmente por MARCO ANTONIO GAVILANES SAGNAY Fecha: 2021.01.04 11:21:02 -05'00'	**2020-01-12**
Ing. Willian Geovanny Yanza Chávez **DIRECTOR DEL TRABAJO DE TITULACIÓN**	WILLIAN GEOVANNY YANZA CHAVEZ WILLIAN GEOVANNY YANZA CHAVEZ c=EC, l=RIOBAMBA, serialNumber=0602356214, cn=WILLIAN GEOVANNY YANZA CHAVEZ	**2020-01-12**
Dr. Carlos Volter Buenaño Pesántez **MIEMBRO DEL TRIBUNAL**	CARLOS VOLTER BUENANO PESANTEZ Firmado digitalmente por CARLOS VOLTER BUENANO PESANTEZ Fecha: 2021.01.06 10:02:06 -05'00'	**2020-01-12**

DEDICATORIA

El presente trabajo va dedicado en primer lugar a Dios, por dármela vida, salud, haberme guiado por el buen camino y ayudado a superar los obstáculos que se presentaron a lo largo de este proceso, permitiéndome de esta manera culminar con mis estudios. A mis padres Vicente Ucles y Dirima Romo quienes siempre me apoyaron de manera incondicional por todo el transcurso de mi vida estudiantil, estuvieron para mí a pesar de las dificultades a ellos les dedico este triunfo, esta meta que logre alcanzar gracias al apoyo de ellos a su paciencia, a sus consejos. Por ellos logre ser una profesional y por ellos estoy donde me encuentro ahora. A todos mis amigos que supieron proporcionarme su apoyo de diferentes maneras hasta conseguir cumplir mis metas.

Didima

AGRADECIMIENTO

Agradecimiento eternamente a Dios, que me supo brindar su sabiduría para completar unos de mis objetivos como es la culminación de mis estudios, cuidándome en todo lugar y momento de los peligros que se presentan día con día y encaminándome hacia el éxito.

A mis padres por saber guiarme e inculcarme valores, por su apoyo incondicional, por su paciencia y esfuerzo para culminar mis estudios y convertirme en una profesional. Les agradezco infinitamente por estar conmigo en mis altas y bajas, por nunca permitir que a pesar dificultades no logre cumplir mi sueño. A Dios por permitir que estén conmigo en esta etapa de mi vida y observen el fruto de sus esfuerzos por ser quien soy ahora.

También agradezco infinitamente a mis mentores. El Dr. Carlos Buenaño y al Ing. Willian Yanza, por hacer posible este sueño, quienes con su paciencia, experiencia, enseñanza, consejos y conocimientos en cada etapa del presente proyecto de investigación.

Didima

TABLA DE CONTENIDO

ÍNDICE DE TABLAS.....ix
ÍNDICE DE GRÁFICOS.....x
ÍNDICE DE ANEXOS.....xi
RESUMEN.....xii
ABSTRACT.....xiii
INTRODUCCIÓN.....1

CAPITULO I

1. **MARCO TEÓRICO REFERENCIAL**.....2
1.1. **Planteamiento del Problema**.....2
1.2. **Formulación del Problema**.....5
1.2.1. ***Delimitación del Problema***.....5
1.3. **Sistematización del Problema**.....5
1.4. **Objetivos**.....6
1.4.1. ***General***.....6
1.4.2. ***Específicos***.....6
1.5. **Justificación**.....6
1.5.1. ***Justificación Teórica***.....7
1.5.2. ***Justificación Metodológica***.....7
1.5.3. ***Justificación Académica***.....7
1.5.4. ***Justificación Práctica***.....8
1.6. **Antecedentes de Investigación**.....8
1.7. **Marco Teórico**.....10
1.7.1. ***Auditoría***.....10
1.7.1.1. *Definición*.....10
1.7.1.2. *Objetivo*.....11
1.7.1.3. *Tipos de auditoría*.....12
1.7.1.4. *Riesgos*.....13
1.7.1.5. *Tipos de Riesgos*.....13
1.7.1.6. *Análisis del Riesgo*.....13
1.7.1.7. *Evaluación del Riesgo*.....14
1.7.1.8. *Gestión del Riesgo*.....15
1.7.1.9. *Control Interno Informático*.....15
1.7.2. ***Auditoría Informática***.....17
1.7.2.1. *Definición*.....17

1.7.2.2. *Objetivos*.....17
1.7.2.3. *Importancia* 17
1.7.2.4. *Seguridad*.....18
1.7.2.5. *Seguridad Física* 18
1.7.2.6. *Seguridad Lógica*.....21
1.7.2.7. *Norma ISO 27000 sistema de gestión de seguridad de la información.* 27
1.7.2.8. *Norma ISO 27001 Requisitos Para Implementar Un SGI* 27
1.7.2.9. *Norma ISO 27002 Buenas Prácticas Para El SGSI* 28
1.7.2.10. *Norma 410 Tecnología De La Información* 29
1.7.2.11. *Norma EIA/TIA 568 A*.....31
1.7.2.12. *Tipos De Seguridades En Las Redes Informáticas*.....33
1.7.2.13. *Protocolo De Red Segura* 33
1.7.2.14. *Análisis DAFO*.....34
1.7.2.15. *Coso II 35*
1.7.2.16. *Ataques Informáticos* 36
1.7.2.17. *Tipos De Ataques Informáticos*.....36
1.7.3. ***Etapas de una Auditoria*** 37
1.7.3.1. *Planificación*.....37
1.7.3.2. *Ejecución* 38
1.7.3.3. *Informe* 39
1.7.4. ***Fase de una Auditoría Informática*** 39
1.8. **Marco Conceptual**.....40

CAPÍTULO II

2. **MARCO METODOLÓGICO**.....42
2.1. **Enfoque de Investigación**.....42
2.2. **Nivel de Investigación**.....42
2.3. **Diseño de Investigación** 42
2.4. **Tipo de Estudio** 43
2.5. **Población y Muestra** 43
2.6. **Métodos, Técnicas E Instrumentos De Investigación** 44
2.7. **Análisis e Interpretación de Resultados** 45
2.8. **Idea A Defender** 54

CAPITULO III

3. **MARCO DE RESULTADOS, DISCUSIÓN Y ANÁLISIS DE RESULTADOS** .55
3.1. **Auditoría Informática A La Empresa Master Technology, Cantón Quito, Provincia De Pichincha, Período 2019.** 55

3.2. **Contenido De La Propuesta** 55
3.2.1. ***Archivo Permanente*** 56
3.2.1.1. *Reseña Histórica* 58
3.2.1.2. *Misión* 59
3.2.1.3. *Visión* 59
3.2.1.4. *Valores* 59
3.2.2. ***Archivo Corriente*** 68
3.2.3. ***Plan De Auditoría Informática*** 71
3.2.3.1. *Fase I: Planificación* 73
3.2.3.2. *Fase Ii: Ejecucición* 86
3.2.3.3. *Comunicación de Resultados* 131
CONCLUSIONES 137
RECOMENDACIÓNES 138
GLOSARIO
BIBLIOGRAFÍA
ANEXOS

ÍNDICE DE TABLAS

Tabla 1-1: Nivel de Riesgo/Confianza 14
Tabla 2-1: Estructura ISO 27001.....28
Tabla 3-1: Tipos de Ataques Informáticos 36
Tabla 4-1: Fases de la auditoria informática.....39
Tabla 5-2: Personal Master Technology.....43
Tabla 6-2: Restricción del Personal no Autorizado 45
Tabla 7-2: Cámaras de Seguridad.....46
Tabla 8-2: Medidas de Seguridad y Respaldo 46
Tabla 9-2: Regulación de Temperatura 47
Tabla 10-2: Programas de Protección.....48
Tabla 11-2: Salida de Emergencia.....48
Tabla 12-2: Señalética.....49
Tabla 13-2: Capacitaciones Institucionales 50
Tabla 14-2: Perfiles de Usuario.....50
Tabla 15-2: Recursos Informáticos 51
Tabla 16-2: Actualización Lógica 52
Tabla 17-2: Actualización Física.....52
Tabla 18-2: Recursos Necesarios por Área 53
Tabla 19-2: Período de Tiempo.....53
Tabla 20-2: Póliza de Seguros.....54

ÍNDICE DE GRÁFICOS

Gráfico 1-1: Tipos de Auditoria 12
Gráfico 3-1: Elementos del Control Interno Informático 16
Gráfico 4-1: Fases De La Auditoría Informática 37
Gráfico 5-2: Restricción del Personal No Autorizado 45
Gráfico 6-2: Seguridad Interna y Externa 46
Gráfico 7-2: Medidas de Seguridad y Respaldo 47
Gráfico 8-2: Regulación de Temperatura 47
Gráfico 9-2: Programas de Protección 48
Gráfico 10-2: Salida de Emergencia 49
Gráfico 11-2: Señalética 49
Gráfico 12-2: Capacitaciones Institucionales 50
Gráfico 13-2: Claves de Acceso 51
Gráfico 14-2: Recursos Informáticos 51
Gráfico 15-2: Actualización de Software 52
Gráfico 16-2: Actualización Física 52
Gráfico 17-2: Recursos Necesarios Por Área 53
Gráfico 18-2: Período de Tiempo 53
Gráfico 19-2: Póliza de Seguros 54

ÍNDICE DE ANEXOS

ANEXO A: ENCUESTA APLICADA AL PERSONAL TÉCNICO DE LA EMPRESA MASTER TECHNOLOGY

ANEXO B: ENCUESTA APLICADA AL PERSONAL ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

ANEXO C: ENCUESTA APLICADA AL GERENTE ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

RESUMEN

El presente trabajo de investigación aplicado a la Empresa Master Technology, del Cantón Quito, Provincia de Pichincha, Período 2019, tuvo como objetivo, valorar la integridad, confidencialidad y disponibilidad de los recursos, equipos informáticos y su información mediante el uso de métodos, técnicas, estándares y herramientas de auditoria informática para la empresa. La ejecución de este trabajo se llevó a cabo con las 3 etapas de la auditoria: Planificación, Ejecución y Comunicación de Resultados mediante la metodología del cuestionario de control interno COSO II, el cual está establecido por 8 componentes que son: ambiente de control, establecimiento de objetivos, identificación de acontecimientos, evaluación de riesgos, respuesta al riesgo, actividades de control, comunicación y supervisión, que permitieron detectar los hallazgos para determinar el nivel de riesgo y de confianza, se definió en la hoja de hallazgos la condición, criterio, causa, efecto, conclusión y recomendación por cada anomalía encontrada en el COSO II. A través de estos componentes se encontraron aspectos relevantes como: la ausencia de respaldos de información, falta de pólizas de seguro, software informático que no cumple con lo que necesita la empresa, inexistencia de normas y reglamentos que ayuden al manejo y control de los recursos informáticos. Todos los hallazgos encontrados fueron expuestos en la etapa 2 de la auditoría que es la ejecución. Para finalizar el trabajo de investigación se emitió un informe en el cual se muestra de manera clara y concreta las opiniones y recomendaciones como, la implementación de una Unidad de Tecnologías de la Información y Comunicación, para erradicar los problemas detectados durante el proceso de auditoría a fin de tomar decisiones oportunas y eficientes para el buen desarrollo de la entidad.

Palabras claves: <CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS> <AUDITORÍA INFORMÁTICA> <COSO II> <RECURSOS INFORMÁTICOS>.

ABSTRACT

The present research work applied to the Master Technology Company, located in Quito, Province of Pichincha, term 2019, was aimed to value the integrity, confidentiality and availability of resources, computer equipment and its information through the use of methods, techniques, standards and computer auditing tools for the company. The execution of this study was carried out in 3 stages: planning, execution and communication of results through the methodology of the internal control questionnaire COSO II, established by 8 components: controlling environment, setting goals, identifying events, risk assessment, response risk, control, communication and supervision activities, which allowed the detection of findings to determine the level of risk and confidence, the condition, criterion, cause, effect, conclusion and recommendation for each anomaly found in the COSO II. Through these components, relevant aspects were found such as: the absence of information backups, lack of insurance policies, computer software that fails to what the company needs, the absence of rules and regulations to help the operation and control of the computing resources. All of the findings were presented in stage 2 of the audit process which is the execution. To complete the investigation work, a report was issued, which shows in a concrete and transparent way the opinions and recommendations as the implementation of an Information and Communication Technologies Area to eliminate the problems identified during the audit process in order to make appropriate and effective decisions for the successful development of the company.

Keywords: <ECONOMIC AND ADMINISTRATIVE SCIENCES> < INFORMATICS AUDITING PROCESS> <COSO II> <COMPUTING RESOURCES>.

INTRODUCCIÓN

La Auditoría Informática aplicada a la Empresa Master Technology, del Cantón Quito, Provincia de Pichincha, Período 2019, tema del presente trabajo de investigación tiene como objetivo, valorar la integridad, confidencialidad y disponibilidad de los recursos, equipos informáticos y su información mediante el uso de métodos, técnicas, estándares y herramientas de auditoria informática para la empresa, este trabajo consta de 3 capítulos los cuales se detallan a continuación:

CAPÍTULO I: Denominado como marco teórico referencial, menciona el estado actual de la empresa detallando los problemas de la misma, planteamiento de objetivos tanto general como específicos, su respectiva justificación tanto, teórica, metodológica como práctica, sus antecedentes investigativos, dentro de este capítulo se fundamentara y estructurara el marco teórico mediante la revisión bibliográfica de diferentes autores para sustentar el presente trabajo de titulación así como el marco conceptual.

CAPÍTULO II: Marco metodológico, se detalla el enfoque, nivel, diseño de investigación, el tipo de estudio, la población y muestra a la cual se realizaran las encuestas y los diferentes métodos, técnicas e instrumentos que se van a utilizar en el proceso de la auditoria informática para la determinación u obtención de evidencias y posterior elaboración del informe, así como los resultados que arrojaron las encuestas que fueron aplicadas al personal técnico, administrativo y al gerente de la entidad.

CAPÍTULO III: Refiriéndose al Marco de Resultados, discusión y análisis de resultados, el cual fue desarrollado en base a las 3 etapas de la Auditoria que son: Planificación, Ejecución y Comunicación de Resultados, este capítulo tiene como fin presentar el informe final de auditoria, con las conclusiones y recomendaciones orientadas a mejorar el uso y gestión de la información con respecto a la integridad, disponibilidad y confidencialidad de los sistemas y recursos informáticos de la empresa.

CAPÍTULO I

1. MARCO TEÓRICO REFERENCIAL

1.1. Planteamiento del Problema

El aumento de nuevas tecnologías obliga a las empresas a nivel mundial a actualizar sus formas y métodos de tratar la información de sus negocios, manteniendo el nivel competitivo con empresas que nacen directamente con nuevas formas de orientar el trabajo que realizan en sus respectivas áreas; es necesaria la modernización de equipos y métodos obligándolas a invertir cada vez más en campos de investigación y de capacitación.

Las pequeñas y medianas empresas (pymes) se pueden encontrar de diferentes dimensiones o formas, como por ejemplo siendo de un solo propietario o perteneciente a una sociedad dentro de un mercado con la capacidad de desenvolverse en distintas actividades, ya sean estas de prestación de servicios, de comercialización, o a su vez de producción. Con la finalidad de obtener una rentabilidad de acuerdo a su área de trabajo y a la demanda de la misma.

Según la organización de las naciones unidas (ONU), a nivel mundial las pymes simbolizan el 80% de los negocios existentes de la economía, donde generan entre el 60% y 70% de los empleos, a su vez las pymes vienen representando el 50% del producto interno bruto (pib) a nivel mundial. Una gran cantidad de estas empresas empiezan hacer usos de recursos tecnológicos y herramientas innovadoras en los diferentes campos de trabajo, muchas de estas empresas no cuentan con las capacidades para explorar o aprovechar estos recursos en los nuevos campos de acción dispuestos por la modernización del mundo lo que hace necesaria la auditoria informática dentro de ellas.

Con estos datos se demuestra la migración de muchas pymes a un ambiente tecnológico más desarrollado en el cual se hace presente el reto de controlar o gestionar de forma adecuada y eficiente los nuevos recursos tecnológicos que estas empresas están implementando o recursos con los que ya contaban previamente.

Las pymes en latino américa forman un grupo compacto y diverso, las cuales pueden ser desde microempresas donde se genera autoempleo informal hasta empresas innovadoras con alta eficiencia y recursos tecnológicos modernos de acuerdo a su modelo de actividad económica. Aplicando políticas y normas coordinadas junto con una inversión adecuada en ciencia e

investigación, las pymes podrían ayudar a generar un cambio estructural mediante la contribución de sus ingresos al aumento de la productividad.

Las pymes en el ecuador tienen una buena adaptación a los cambios en el ambiente que se generan en el país ya sea en los social, en la reinvención de sus negocios o en lo tecnológico, su representación en el país es del 95% en donde la mayoría de estas se encuentran ubicadas en el oro, Manabí, pichincha, Azuay y el Guayas. De entre las cuales las que se han sometido a una auditoria informática han presentado beneficios tales como: la optimización de los recursos disponibles, implementar estrategias a futuro según resultados de los estudios, implementar normas y políticas de mantenimiento y prevención del estado de los equipos informáticos, mayor fluidez de información de la empresa, se establecieron políticas de seguridad web, creación e protocolos de acción en caso de intromisiones informáticas.

Las seguridades que se implementaron dependen totalmente de las empresas que han realizado la auditoria informática, dependiendo de las necesidades que la empresa tenga se pueden implementar seguridades de software como programas especializados en seguridad tanto de equipos individuales como de las redes existentes en la empresa encargados de prevenir y evitar posibles ataques informáticos; también se implementan seguridades de hardware como un protocolo de mantenimiento o revisión constante de los equipos, así como preparar sitios con las configuraciones técnicas para soportar la ubicación de diferentes equipos de hardware; con respecto a seguridad en redes se pueden establecer diferentes tipos de seguridad a diferentes niveles ya sean de clientes o servidores como diferentes topologías de red para controlar de mejor forma la distribución de información.

La misma capacidad de adaptación de las empresas genera en las más visionarias el deseo de incursión en mercados más modernos recurriendo a la innovación tecnológica como uno de sus mejores recursos, sin embargo, al hacer uso de este recurso no toman en cuenta los cuidados y las necesidades que dicha innovación requieren, generando en una gran cantidad de ocasiones la mala administración de recursos tecnológicos o una pésima distribución de los mismos. Al no enfocarse en los percances que conlleva una inversión mal empleada se hace necesaria una forma de corregir o prevenir dichos problemas que ponen en riesgo la imagen y estabilidad económica de la empresa, dejando en evidencia la importancia de la auditoria informática.

Los beneficios que una empresa, en este caso privada, los resultados obtenidos después de la aplicación de una auditoria informática han sido, un incremento significativo de la seguridad de su información y privacidad de la misma, aumentando el nivel de confianza de tanto de sus usuarios como para el personal de la entidad, se han implementado políticas de contingencia para

hacer frente a los problemas informáticos, mejora la velocidad de respuesta de los diferentes departamentos y ayuda con la optimización de las redes informáticas manejadas por la organización. Dando a conocer el beneficio de la misma en este tipo de empresas que manejan sus recursos con un escaso conocimiento respecto al tema.

El diagnóstico realizado a revelado los siguientes problemas dentro de la empresa:

- El sistema informático instalado en cada uno de los equipos que posee la empresa no cuenta con las seguridades necesarias para impedir acceso no autorizada a la información que manejan lo que ya ha generado varios percances en el manejo de la base de datos.

- Determinadas áreas de la empresa no disponen de los recursos tecnológicos necesarios y las seguridades correspondientes en los mismos, impidiendo el correcto desempeño de estos departamentos, provocando estancamiento en su área de trabajo, así como manteniendo un riesgo de seguridad.

- No cuenta con personal especializado para el área de recursos tecnológicos e informáticos (soporte y servicio técnico) que brinde un correcto mantenimiento a las redes de comunicación, lo que no permite establecer el seguro funcionamiento de su red interna ni detectar posibles filtraciones de información.

- No existe procedimientos de seguridades físicas internas o externas, así como seguridades lógicas en los sistemas de la empresa lo que no permite dar seguimiento a las condiciones en las que los usuarios desarrollan sus actividades como consecuencia se han generado graves vulnerabilidades a los sistemas usados por la empresa para manejar la información de la entidad y de sus clientes.

Los problemas expuestos evidencian la necesidad de realizar un estudio profundo de las estrategias y modelos que se están siguiendo para el manejo de los recursos informáticos tanto físicos como lógicos siendo la auditoría informática el medio principal para avaluar y examinar las seguridades de los procesos de la empresa actualmente y poder generar estrategias que permitan mejores procedimientos para las actividades de la empresa en el futuro, motivo de este trabajo de titulación.

1.2. Formulación del Problema

De qué manera la auditoría informática aplicada a la empresa Master Technology, Cantón Quito, Provincia de Pichincha, Período 2019, ¿ayudará a evaluar los niveles de integridad, confidencialidad, disponibilidad y autenticación de los sistemas y recursos informáticos de la empresa?

1.2.1. Delimitación del Problema

Campo de Acción: Auditoría
Objeto de Estudio: Auditoría Informática
Espacio: Empresa Master Technology
Tiempo: Período 2019
Aspecto: Norma 410 Tecnología de la Información Establecida Contraloría General del Estado

1.3. Sistematización del Problema

¿la aplicación de políticas de seguridad física dentro de la empresa permitirá controlar el ingreso de personal no autorizado?

La implementación de las correctas políticas de seguridad física permitirá mantener la información y recursos de la empresa siempre bajo control o monitoreo, permitiendo identificar con relativa facilidad los intentos de acceso de personal no autorizado, como puede ser el intento de conectar dispositivos desconocidos o comprometidos a la red interna de la empresa.

¿implementar un sistema de control interno informático permitirá administrar de mejor manera los recursos informáticos de la empresa?

La implementación de un sistema de control interno informático permitirá realizar observación y evaluación del manejo que se dan a los recursos informáticos permitiendo desarrollar estrategias y planos de distribución la los mismo acorde a las necesidades de cada área de trabajo, como puede ser el direccionamiento de información estrictamente necesaria para áreas específicas o la distribución adecuada de equipos en áreas que demanden más su uso.

¿es requerida la capacitación de personal existente sobre las políticas de seguridad físicas y lógicas que ha implementado la empresa para proteger los bienes y recursos informáticos?

Es indispensable realizar capacitaciones al personal sobre las políticas que se establecerán en la empresa y así mantener la armonía y el adecuado monitoreo de la empresa adicionalmente es necesaria la capacitación sobre manejo básico de equipos y recursos informáticos, adicionalmente

al ser una empresa en crecimiento es recomendable la contratación de personal especializado en el manejo de dichos recursos y equipo (soporte y servicio técnico) así como de mantenimiento a todos los recursos informáticos de la empresa acorde con las políticas que se implementaren en ella.

¿incorporar seguridades lógicas en los sistemas informáticos mejorará el tratamiento y seguridad de la información dentro de la empresa?

La empresa debe establecer un nivel de seguridad para sus cliente y empleados aplicando los diferentes estándares de seguridad entre ellos la implementación de software especializado en la seguridad informática de la empresa, garantizando la seguridad de la información que esta maneja al mismo tiempo que podrá reflejar mayor seguridad para sus clientes y empleados dejando en el porcentaje de lo posible fuera la posibilidad de vulneraciones a la seguridad.

1.4. Objetivos

1.4.1. General

Aplicar una auditoría informática a la empresa Master Technology, cantón quito, provincia de pichincha, período 2019, para valorar la integridad, confidencialidad y disponibilidad de los recursos, equipos informáticos y su información mediante el uso de métodos, técnicas, estándares y herramientas de auditoria informática para la empresa.

1.4.2. Específicos

- Fundamentar y estructurar el marco teórico mediante la revisión bibliográfica de diferentes autores para sustentar el presente trabajo de titulación.
- Aplicar la metodología establecida en el proceso de la auditoria informática para la determinación u obtención de evidencias y posterior elaboración del informe.
- Presentar el informe final de auditoria, con las conclusiones y recomendaciones orientadas a mejorar el uso y gestión de la información con respecto a la integridad, disponibilidad y confidencialidad de los sistemas y recursos informáticos de la empresa.

1.5. Justificación

El avance en el uso de tecnología que presenta la Empresa Master Technology del Cantón Quito, Provincia de Pichincha en la administración de varias aplicaciones informáticas y procesamiento de datos en sus departamentos, es necesaria la corrección de sus fallos y errores en la ejecución del trabajo de las diversas áreas por lo tanto es indispensable la realización de una Auditoria

Informática la cual ofrezca resultados efectivos para eliminar o reducir los fallos y errores; ayudando a la optimización de los recursos informáticos dentro de la empresa.

El análisis del uso de los recursos informáticos y disponibilidad, confidencialidad e integridad de la información deberá cumplir con las respectivas seguridades tanto lógicas como físicas con el objetivo de poder determinar el nivel de riesgo en la que se encuentra la empresa para así implementar medidas que permitan salvaguardar los equipos informáticos y su información.

La Auditoria Informática lograra mediante el uso de métodos, técnicas y herramientas; determinar los estándares a través de los cuales se obtendrán los resultados que nos permitirán aplicar de forma adecuada las medidas necesarias para mejorar la seguridad de las redes de comunicación junto con la administración de los recursos informáticos y la información que se guarde en los mismos.

1.5.1. Justificación Teórica

Se justifica teóricamente el presente trabajo de titulación al haber usado la información obtenida de varios recursos como, por ejemplo; libros, páginas web, normativas relacionadas al tema de auditoria informat6ica de forma que sustente adecuadamente la ejecución de la auditoria informática en la empresa Master Technology, cantón quito, provincia de pichincha, y pueda ser de ayuda para aquellas empresas que estén pasando por problemas similares.

1.5.2. Justificación Metodológica

El trabajo de titulación esta metodológicamente justificado al haberse usado métodos, técnicas e instrumentos asociados a la correcta ejecución de una auditoria informática y acorde con las normas que esta exige, resultando en la recopilación de información necesaria para dar cabalidad a los objetivos expuesto en el trabajo de titulación.

1.5.3. Justificación Académica

Académicamente el proyecto se justifica ya que se pone en práctica los conocimientos adquiridos durante la formación académica en la Escuela Superior Politécnica de Chimborazo, Facultad de Administración de Empresas, Escuela de Contabilidad y Auditoría, y la experiencia adquirida en la duración de las prácticas preprofesionales, aportando con bases útiles y en la resolución de problemas que presentaba la entidad.

1.5.4. Justificación Práctica

Desde el punto de vista práctico-social el trabajo de titulación aporta con la evaluación de los niveles de manejo de la información y de recursos informáticos y tecnológicos que servirá para que empresas en similares condiciones tomen los correctivos necesarios usando los métodos prácticos para obtener la información necesaria para la ejecución de la auditoria informática.

1.6. Antecedentes de Investigación

A finales del siglo XX la informática comenzó a formar parte de la gestión de las organizaciones que hayan sido conformadas en aquella época, volviéndose relevante a comienzos de los años cuarenta, sirviendo como ayuda para los militares que buscaban una forma de salvaguardar los equipos y la información que contenían los mismos, de la misma manera se trataba de asegurar que solo el personal de alto rango tuviera acceso a ella.

Con el paso del tiempo las necesidades que han surgido tras la creación de nuevas organizaciones, se han ido originando de modo que el avance de la informática solventara dichas necesidades convirtiéndose en una herramienta base para la toma de decisiones en las empresas, tornando a los recursos informáticos como una necesidad para la conformación de entidades (Infante-Moro, a., Infante-Moro, J. C., Martínez-López, F. J., García-Ordaz, M., & Gallardo -Fernández, M., 2017).

En los párrafos anteriores destacamos la necesidad actual establecida por las empresas de contar con recursos informáticos ya sean estos físicos o digitales (computadoras, bases de datos informáticas), debemos también resaltar los diversos enfoque, propuestas y aplicaciones que han surgido al pasar de los años donde se hace evidente la necesidad de tratar el tema de auditoria informática con la relevancia emergente que esta constituye (Proaño Escalante, R. A., Saguay Chafla, C. N., Jácome Canchig, S. B., & Sandoval Zambrano, F., 2017).

Por ende, la auditoria informática consiste en reunir, clasificar y probar de forma sistemática si los recursos informáticos y la fluidez de la información son efectivas al momento de resguardar información fundamental acerca de las actividades realizadas por la empresa, a su vez se encarga de verificar si se está manejando de manera eficiente todos los recursos informáticos disponibles en la empresa. En el proceso es importante identificar errores, necesidades, trabas y costos que se comprendan un obstáculo o un bloqueo para el correcto flujo de la información dentro de la empresa (Velthuis, M. G. P., 2008).

Anteriormente hemos dejado algunos rasgos de la creciente importancia de la auditoria informática, es adecuado que detallemos con un grado más de profundidad el porqué de la

importancia de esta en la actualidad dentro de las empresas en general pero mayormente dentro de las privadas. Las empresas privadas por su misma naturaleza pueden decidir con más facilidad y rapidez incursionar o renovar sus equipos tecnológicos, al realizarse esta innovación se pueden incurrir en varios errores que pueden llevar a un desastre mayor.

Entonces para evitar caer en estos errores es necesaria una revisión profunda de los proyectos que se pusieron en marcha, esta revisión es el área de trabajo de la auditoria informática, que se encargara de proporcionar toda la información y análisis necesarios para corregir o prevenir problemas en las empresas generados por estas renovaciones o por la falta de las mismas. Las auditorias informáticas se llevarán a cabo con base a las regulaciones normas y estándares correspondientes para lograr la construcción.

De un sistema de control para la ejecución de los procesos, manejo de la información, seguridad lógica y física, etc. Este tipo de auditorías nunca esta excepto de posibles mejoras por lo que es recomendado para realizarse al menos una vez por año.

En el Repositorio Digital de la ESPOCH

La autora Cando, N. (2019.) Con el tema denominado auditoría informática a Metriza Metropolitana Riobamba Clínica de Servicios Médicos Especializados S.A arrojo en los resultados la detección de falencias dentro del sistema de control interno y las tecnologías de información y comunicación, aportando positivamente a la toma de decisiones de la alta dirección contribuyendo de esta manera la gestión de las tecnologías informáticas.

La autora Valdiviezo, C. (2012) con el tema denominado auditoría de seguridad física y lógica de los sistemas informáticos a la empresa Sumatex, de la ciudad de Riobamba, los resultados obtenidos de esta empresa revelan una gran cantidad de falencias dentro de la misma evidenciando la necesidad de implementar sistemas de seguridad física y lógica, puesto que sus dispositivos tecnológicos no guardan ningún tipo de seguridad de la empresa o sus clientes, al mismo tiempo que detecta la falta de capacitación de los empleados, los cuales no cuentan con ningún tipo de cultura y de cuidado de la conservación de la información.

La autora Bonilla, F. (2012) Con el tema denominado auditoría de sistemas informáticos, de la Compañía Hidalgo Broncano Cía. Ltda. A expuesto circunstancias similares a las expuestas en la tesis referenciada con anterioridad, revelando a través de los estudios realizados la falta parcial o completa de un sistema de seguridad física y lógica, provocando que se hayan generado varios percances y problemas dentro de la misma; al mismo tiempo se detectan problemas en la fluidez

del trabajo en sus áreas provocada por el estancamiento de la información y por el mal uso de la misma.

1.7. Marco Teórico

1.7.1. Auditoría

1.7.1.1. Definición

El trabajo de Sánchez Gómez, A. R. (2005) nos dice que la definición de auditoria no se puede determinar como una sola, es decir, existe varias definiciones acerca de la auditoria, para efectos de este trabajo tomaremos como referencia, definiciones que nos ayuden a entender de manera más amplia su función.

- Una recopilación, acumulación y evaluación de evidencia sobre información de una entidad, para determinar e informar el grado de cumplimiento entre la información y los criterios establecidos

- Un proceso sistemático para obtener y evaluar de manera objetiva, las evidencias relacionadas con informes sobre actividades económicas y otras situaciones que tienen una relación directa con las actividades que se desarrollan en una entidad pública o privada. El fin del proceso consiste en determinar el grado de precisión del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando principios establecidos para el caso

Por lo tanto, la auditoria es la recopilación de información respecto a la actividad que realiza la empresa con el fin de que toda la evidencia obtenida por parte del auditor profesional encargado de auditar a dicha organización, certifique que todo lo que se realiza sea verídico y legal. Entregando un informe final donde se detalle de manera concreta todo lo que la entidad necesita mejorar, es decir sus conclusiones y sus recomendaciones para que esta pueda tener un crecimiento económico dentro del mercado.

1.7.1.2. Objetivo

Basándose en las definiciones dichas anteriormente se puede deducir que el objetivo principal de la auditoria es evaluar la situación en todas las áreas que representa la empresa para tener un conocimiento claro de lo que ocurre dentro de ella para determinar qué tipo de acciones se van a tomar dentro de la entidad de acuerdo al criterio del auditor profesional.

A continuación, se mencionará objetivos adicionales que puede contener una auditoria.

- Diagnosticar la realidad de la entidad de manera general mediante observación de cómo se llevan las actividades dentro de la empresa, manejo de situaciones conflictivas, cumplimiento del reglamento de la empresa (horarios de entrada y salida), para determinar las áreas a intervenir y realización de posibles mejoras.
- Interactuar con el personal de la empresa para tener conocimiento de que tan eficiente es en su área de trabajo, y así determinar si se cumple con las actividades encomendadas a cada uno de los trabajadores de la entidad.
- Obtener evidencia la cual contenga información suficiente, competente y relevante de la empresa a auditar para revelar en que áreas de la empresa es necesario mejorar mediante el análisis del tipo de información recopilada.

De acuerdo con Soldevilla Paredes, J. (2014) menciona que los objetivos de la auditoria son:

- Recopilar información de manera general acerca de la empresa, por ejemplo; que actividad realizas, el tipo de producto o servicio que oferta, forma en la que presta el servicio/producto, procedimiento para los cobros respectivos y orden jerárquico que posee la entidad.
- Dar prioridad a las áreas con más problemas en el desarrollo de sus actividades considerando el nivel de riesgo que representa a la empresa.
- Determinar el nivel de eficiencia y eficacia con las que se desarrollan todas las actividades de la empresa para su crecimiento económico.

1.7.1.3. Tipos de auditoría

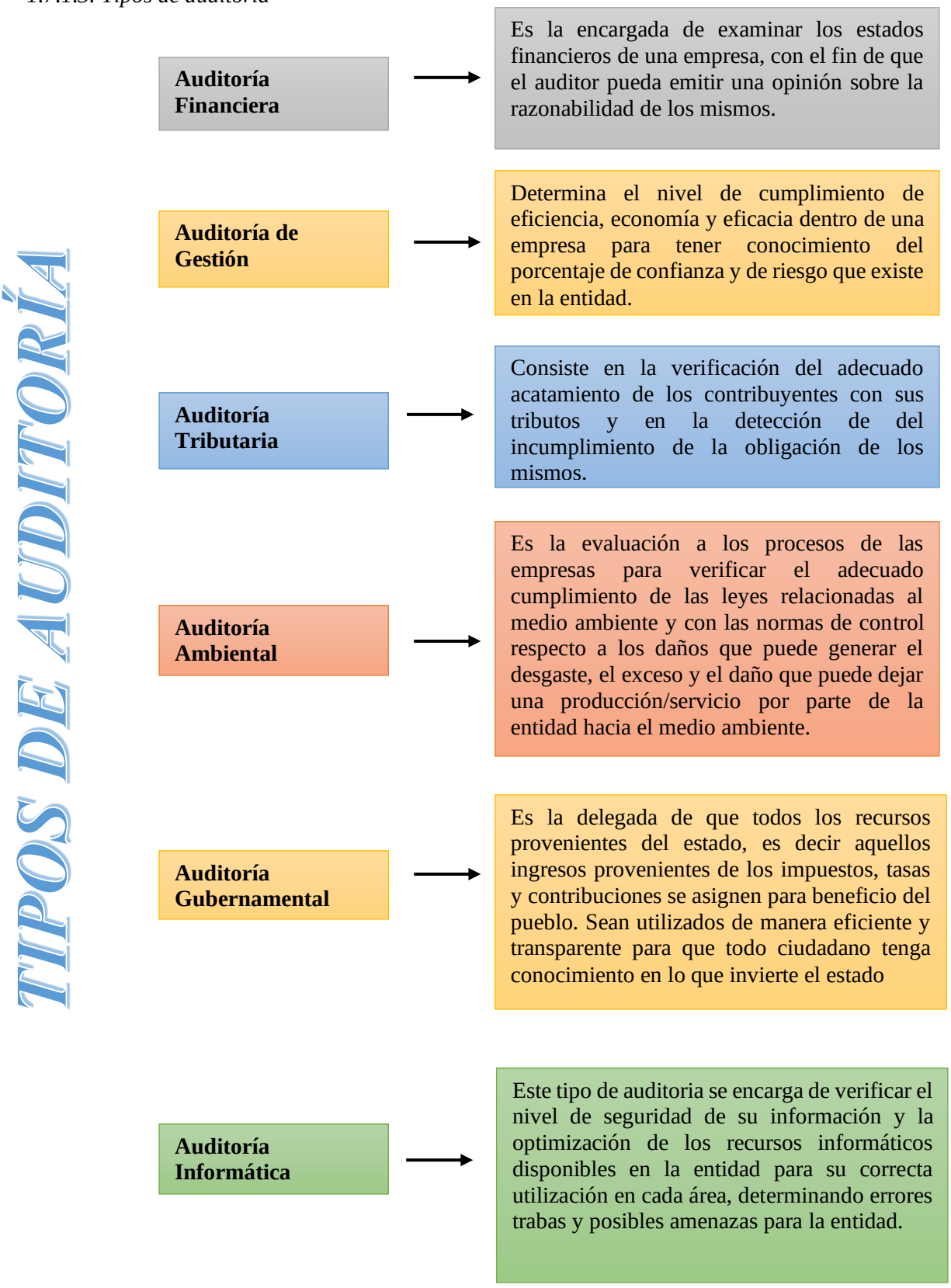


Gráfico 1-1. Tipos de Auditoria

Realizado por: Ucles Romo, D, J. (2020)

1.7.1.4. Riesgos

Según Luna, Y. B. (2015) define al riesgo de auditoria como los eventos que se presentan inesperadamente durante la realización del trabajo las cuales pueden presentarse de manera cuantitativa o cualitativa, a su vez ambas, las cuales pueden alterar la exactitud de los resultados esperados.

1.7.1.5. Tipos de Riesgos

Para Luna, Y. B. (2015) clasifica a los riesgos en 3 tipos los cuales son:

Riesgo Inherente. – Está relacionada con la actividad económica de la entidad dejando de lado la posibilidad de existencia de control interno dentro de la organización.

Riesgo de Control. – Este tipo de riesgo se relaciona directamente con el control interno que posea la empresa, los cuales sean inadecuados o insuficientes para la oportuna detección de posibles irregularidades que se estén desarrollando sin ser identificadas a tiempo ocasionando un nivel de riesgo alto hacia la entidad.

Riesgo de Detección. - Consiste en la posibilidad de no detectar errores dentro de los procedimientos de una auditoria lo que cual hace que el riego control y el inherente sean aún más vulnerables, convirtiendo el principal responsable la persona a cargo de la auditoria.

1.7.1.6. Análisis del Riesgo

Permite obtener información suficiente y relevante para brindar recomendaciones que sean útiles para la implementación de medidas que ayuden a la entidad como saber defenderse ante posibles escenarios que representen una amenaza o un riesgo para la entidad, en el análisis del riesgo se pueden nombrar cuatro etapas que son:

- La detección oportuna del peligro la cual permita saber qué nivel de riesgo (alto, medio o baja) representa para la organización.
- Se deberá evaluar el peligro, es decir, cuál es el nivel de probabilidad de que suceda como de que no suceda, en caso de suceder se deberá identificar las consecuencias a las que la empresa se encuentra si no se actúa de manera oportuna.
- La gestión del riesgo, es decir, la entidad deberá tomar la decisión correcta para dar respuesta al riesgo y poner en ejecución su mejor opción para minimizar el impacto del riesgo o a su vez eliminarlo en su totalidad.

1.7.1.7. Evaluación del Riesgo

Para los autores Gaitán, R. E., & Niebel, B. W. (2015) menciona que para determinar el nivel de riesgo se debe tener en claro el nivel de seguridad detallas a continuación.

Tabla 1-1: Nivel de Riesgo/Confianza

Nivel de confianza		
Alto	***Moderado***	***Bajo***
95% - 76%	*75% - 51%*	*50% - 15%*
5% - 24%	*25% - 49%*	*50% - 85%*
Bajo	***Moderado***	***Alto***
Nivel de riesgo		

Fuente: Trabajo de Campo

Realizado por: Ucles Romo, D, J. (2020)

Alto. - Mientras más alto sea el nivel de confianza, menor es el nivel de riesgo que enfrenta una entidad, por lo tanto, menor es el impacto del riesgo en la empresa y viceversa, es decir, cuanto más bajo sea el nivel de confianza, más alto es el nivel de riesgo. Esta se encuentra comprendida entre los porcentajes del 76% - 96% de confianza y 5% - 24 % de riesgo o viceversa que se explicó anteriormente.

Moderado. – Esta se encuentra comprendida entre 51% - 75% de confianza, así como también de 25% - 49% de riesgo o viceversa a la cual se le considera un nivel moderado, ya que, el riesgo tiene un impacto parcial dentro de la entidad.

Bajo. - Es decir que cuando el nivel de confianza es bajo, el nivel de riesgo es alto, por lo que el nivel de impacto en la organización es significativo, esta se encuentra comprendida entre el 15% - 50% de confianza y 50% – 85% de riesgo.

Para la obtención del nivel de riesgo que enfrenta una empresa se lo hará mediante cuestionarios de control interno donde se efectuaran preguntas dirigidas al personal de la empresa y de esta manera poder saber mediante la auditoria en que áreas deberá centrarse.

Para hallar el nivel de confianza se tomará mediante:

$$\textbf{Nivel de Confianza (NC)} = \frac{Respuestas\ Positivas}{PTRespuestas\ Negativas} * 100\%$$

En cambio, para encontrar el nivel de riesgo se restará el nivel de confianza con el número de respuestas negativas representado en porcentajes.

Nivel de Confianza (NC)-Respuestas Negativas

1.7.1.8. Gestión del Riesgo

Es de suma importancia que la entidad cuente con una gestión de riesgo, los cuales deberán ser diseñados considerando los posibles riesgos que la empresa puede enfrentar a futuro analizando las consecuencias que esta puede dejar y el impacto que llegaría a tener en caso de que la organización no actuara con tiempo con la opción más factible para dar respuesta a dicho riesgo, para así implementarlos en el momento oportuno minimizando su impacto o a su vez eliminarlo en su totalidad.

1.7.1.9. Control Interno Informático

Son todas las acciones que trabajan de manera vinculada para garantizar la eficiencia del uso de los recursos informáticos de la entidad, los cuales también pueden ser asignados para alcanzar los objetivos y metas planteados por la empresa. A su vez el control interno informático ayuda a mantener la seguridad de la información perteneciente a la empresa previniendo posibles errores ataques o amenazas que puedan perjudicar el funcionamiento de la organización.

Objetivo

Para Razo, C. M. (2002) nos dice que el control interno informático debe basarse en objetivos fundamentales para tener conocimiento claro y concreto de lo que consiste la misma.

- Tener como prioridad la seguridad de la información y la protección de los recursos informático de la entidad.
- Impulsar la recolección confiable, oportuna y veras de información, su integración en los sistemas y la obtención de informes en la organización.
- Fomentar procedimientos, métodos y técnicas para facilitar las actividades y procesos de los servicios informáticos para cumplir las metas de la empresa.
- Implementar y cumplir con los procedimientos, normas y políticas para que las actividades de tratamiento de información puedan ser reguladas.
- Instaurar los protocolos adecuados para el correcto diseño e implementación de los sistemas informáticos con la finalidad de proporcionar de forma eficiente la información procesada necesaria para la empresa.

Elementos del Control Interno Informático

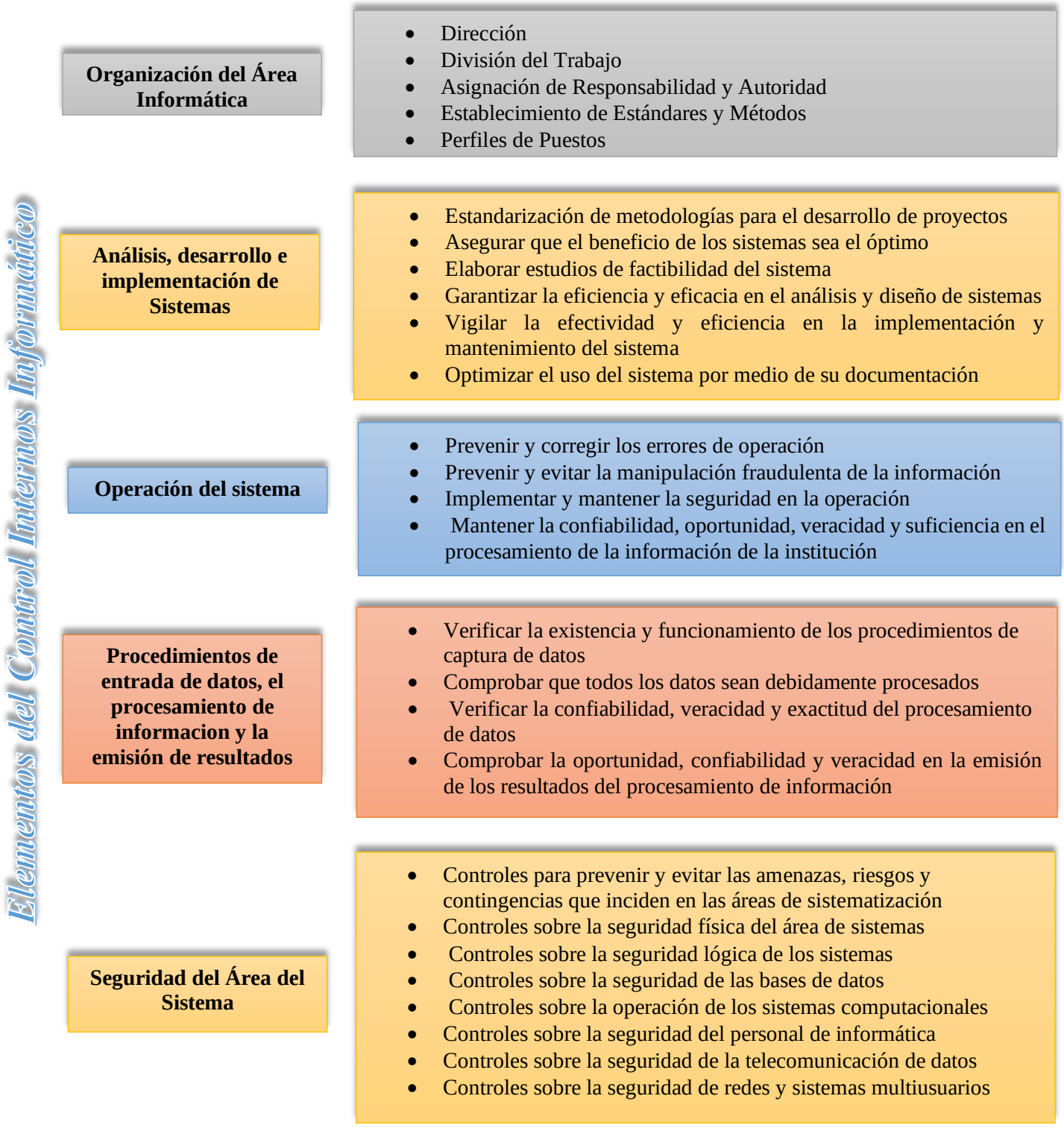


Gráfico 2-1. Elementos del Control Interno Informático

Realizado por: Ucles Romo, D, J. (2020)

1.7.2. Auditoría Informática

1.7.2.1. Definición

Para los autores Soto, M. D. C. S., Millán, N. D. C. O., Caro, M. S., & Garfias, J. I. M., (2018) mencionan que consiste en la evaluación de los sistemas y procedimientos informáticos que posee una entidad para determinar su nivel de seguridad y fluidez en el manejo de la información, tornándose en una herramienta de detección de errores o fallas a través de la evaluación del manejo de la información y recursos informáticos de una empresa o entidad

1.7.2.2. Objetivos

El trabajo de Soto, M. D. C. S. (2018) menciona que de los objetivos más relevantes se pueden tomar los siguientes:

- Constatar la óptima distribución de los recursos informáticos a las áreas que conforman la empresa para su adecuado desempeño en sus respectivas actividades.
- Verificar que la información contenida en medios electrónicos como son computadoras, tablets o celulares pertenecientes a la entidad, sean útiles y se mantengan relacionadas a los procesos y actividades de la misma, facilitando la toma de decisiones para beneficio de la empresa.
- Analizar los sistemas informáticos y su funcionamiento para mantener la eficiencia de dicho sistema dentro de la empresa evitando perdidas de información o mala administración de la misma.

Se puede deducir que de entre los objetivos de la auditoria informática resalta el cuidado que deben tener las entidades con su información, la forma en la distribuyen sus recursos informáticos entre las áreas que requieren o necesitan de los mismo para un adecuado desempeño de sus actividades para beneficio de la entidad.

1.7.2.3. Importancia

El avance de la tecnología con el transcurso de los años ha obligado a que las empresas se adapten a las necesidades que el mercado a generando, optando por recurrir a sistemas informáticos que ayudan a la entidad a crecer económicamente no obstante una mala toma de decisiones debido a fallas en dicho sistema o decidir no adaptarse que no logre cumplir con las expectativas y necesidades de los clientes o incluso la desaparición de la empresa. Se considera que la

consecuencia de que sus actividades ocupen más tiempo de lo necesario, ocasionado el riesgo de perdidas dentro del mercado.

1.7.2.4. Seguridad

Para el autor de Luis Gargallo, E. (2018) menciona que la seguridad es la protección de la información perteneciente a una entidad incluidos los sistemas con los que trabajen de acuerdo a su actividad económica, la seguridad tiene 3 características para llevar a cabo su propósito de proteger, conocidas en el área de informática como la triada confidencialidad, integridad y disponibilidad (CID) explicadas a continuación:

Confidencialidad. - Hace referencia a que la información debe ser única y exclusivamente conocida solo por personal autorizado que el encargado designe, de esta manera solo podrán tener acceso un número limitado de personas que conocerán lo que contiene dicha información, dejando en claro que las personas que tengan la autorización no deben dar permiso a terceras personas de acceder a la misma.

Integridad. – Consiste en que la información que se introdujo dentro un sistema por la o las personas autorizadas a ingresarla, no debe estar alterada por ningún motivo sin orden directa de la alta dirección, ya que cualquier intento de manipulación de la información pone en riesgo la veracidad de su contenido, arrojando como consecuencia una mala toma de decisiones.

Disponibilidad. – Como su nombre lo dice la información deberá estar disponible en cualquier momento que el personal autorizado considere necesario ya sea para la toma de decisiones, constatación de información o para la verificación de que no haya existido ningún tipo de problema al momento de acceder a la misma.

1.7.2.5. Seguridad Física

De Luis Gargallo, E. (2018) nos dice respecto a la definición de seguridad física que:

> La seguridad física es aquella que se encuentra asociada a la protección de un sistema contra amenazas exteriores como, por ejemplo: incendios, inundaciones, es decir, es la que se encarga de salvaguardar físicamente cualquier recurso, suministrando medidas de seguridad física para dichos recursos. Dando por entendido que al referirse al termino recurso abarca

desde un USB hasta el control por los que tienen acceso el personal autorizado. Dentro de la seguridad física existen 3 posibles riesgos.

Protección del Hardware. – El hardware es el elemento más costoso dentro de la empresa, por lo que las medidas que se adopten para la seguridad de la integridad constan como la parte más importante de la seguridad física para cualquier tipo de entidad como, por ejemplo: routers seguros y vías rápidas de transmisión de información como lo es la fibra óptica.

Acceso Físico. – Hace referencia a que a pesar de las medidas de seguridad físicas encarga de proteger los recurso terceras personas logran tener acceso al mismo, ya sean con facilidad o inconvenientes, por lo que es importante que las medidas a implementar tengan garantías de su función a cumplir.

Desastres Naturales. – Son eventos inesperados para lo cual ningún tipo de medidas de seguridad podrá garantizar su cuidado, por lo que la entidad deberá contar con planes de contingencia y protocolos de seguridad la cual consista en realizar copias para llevarlas a sitios lejos del original en casos de desastres naturales recalcando que, aunque el recurso físico se pierda no se puede permitir la perdida de datos que estos guardan.

Tormentas Eléctricas. - En la gran mayoría suelen ser predecibles por lo que el encargado cuenta con tiempo suficiente para desconectar los equipos de la energía eléctrica, pero al no actuar rápidamente pueden llegar hacer perjudiciales para la entidad incluso llegar al punto de tener una pérdida total del hardware por lo que las tormentas eléctricas o subidas y bajadas de tensión en el servicio de electricidad pueden destruirlas en su totalidad, aunque estas se encuentren protegidas.

Inundaciones y Humedad. – Al tocar el tema de inundaciones es fácil de deducir que cualquier tipo de elemento electrónico que no cuente con una protección especializada quedara totalmente inutilizado u obsoleto en caso de ser afectado por dicha situación para evitar esto es necesario tener en cuenta la correcta ubicación de los elementos por ejemplo en el caso de contar con una estructura adecuada para la implementación de un servidor esta debería pertenecer en un área como una segunda planta o similares. En el caso de la humedad cuando no se controla de forma correcta puede significar un riesgo importante a la integridad de los equipos electrónicos sin embargo con el manejo adecuado forma parte importante del control térmico de las diferentes áreas.

Alteraciones en el Entorno. - Refleja algo inesperado dentro de la empresa que se encuentra fuera del alcance del personal autorizado como, por ejemplo: una repentina subida de tensión de la electricidad, lo suficiente para sobrecalentar el sistema y provocar daños ya sean temporales o permanentes que puedan afectar a la información que los recursos físicos guardan por lo que se debe aplicar los mismo protocolos mencionados n el punto anterior.

Prevención. - Se controla el acceso a los diferentes departamentos o lugares seguros. Con la capacidad de limitar a los usuarios la entrada a determinadas áreas restringidas por la empresa, permitiendo o negando accesos a lugares específicos o protegidos dependiendo no solo de sus permisos sino también del nivel de autorización.

Detección. – Cuando la prevención no es suficiente se intervendrá a través de dispositivos técnicos como videocámaras, alarmas, circuito cerrado, en caso de fallas en la detección la amenaza se enfocará en el personal con autorización de acceso a las áreas restringidas ya sea personal que interactúa de manera directa con el área protegida o con el personal que tenga relación indirecta con el área en cuestión.

Ruido Eléctrico. – Como se hablo en conceptos anteriores la ubicación de los elementos es muy importante retomando mas sentido al saber que los equipos especializados pueden ser afectados por dispositivos emisores de ondas que normalmente no representarían una amenaza sin embargo al existir dispositivos sensibles pueden llegar a provocar graves daños en estos.

Incendios y Humo. - Lo común en los incendios es que sean a causa de las subidas y bajadas de la tensión eléctrica en conjunto con fallas del tendido eléctrico debido a que esto ocasiona cortocircuitos, otra causa se puede considerar el exceso de dispositivos conectados o un dispositivo defectuoso que genere calor excesivamente peligroso.

Para lo cual uno de los métodos son los extintores con componente no liquido sino gaseoso o pulverizarte, existen métodos más avanzados, pero a su vez más costosos como, por ejemplo: el aislado al vacío y extracción del oxígeno del área afectada, aunque este método solo puede ser aplicado en áreas libres de interacción humano.

Temperaturas Extremas. - El frio intenso o calor excesivo puede llegar a perjudicar gravemente los equipos informáticos que se encuentren expuestos por lo que es necesario controlar la temperatura adecuadamente dentro de la estructura donde estos se encuentren,

además de una correcta ventilación en los equipos para que puedan respirar sin sobrecalentarse y provocar daños internos pese a que la temperatura este idónea.

Otros aspectos que se deben considerar para la seguridad física son:

- **Back-Ups. -** Nos habla acerca de que se deben almacenar y sacar copias de manera periódica de los equipos informáticos manteniendo la confidencialidad e integridad de la información en áreas externas y consideras seguras dentro de la empresa manteniéndome un control adecuado del acceso con aut6orizacion a dicha área.

- **Plan de Contingencia.** - Dentro de estos planes debe estar como prioridad los recursos informáticos, la información que se contiene en los mismos, documentación física que respalden dicha información, el plan de contingencia deberá ser actualizado y mejorado de manera regular acorde a los escenarios posibles también deberá ser socializado a toda la empresa para conocimiento de la existencia del mismo.

- **Pólizas/Seguros. -** Estos cubrirán en su totalidad el valor del hardware y del software perteneciente a la entidad, se debe aclarar que la póliza o el seguro debe estar actualizado de manera permanente para evitar posibles inconvenientes de la caducidad del seguro.

1.7.2.6. Seguridad Lógica

De Luis Gargallo, E. (2018) nos dice respecto a la definición de seguridad lógica que:

> A contrario de lo seguridad física, la seguridad se encarga de todo lo intangible, es decir, de la protección del software que poseen los equipos informáticos de la entidad para desempeñarse correctamente, su objetivo es salvaguardar los datos, las aplicaciones contra robos de información, perdidas de la misma, ingreso de los virus informáticos, entradas sospechosas de vía internet o de modificaciones que no hayan sido autorizadas.

Objetivos de la Seguridad Lógica

1. Permite controlar y saber quiénes acceden a los diferentes programas e información y como lo hacen.
2. Asegurar que la información ingresada no haya sido modificada por usuarios no autorizados sin requerir un control exhaustivo.
3. Garantizar que los procesos de la empresa usen los recursos informáticos adecuados y necesarios.

4. Verificar que la información transmitida llegue de forma adecuada y sea recibida exclusivamente por el personal autorizado.
5. Asegurar la integridad de los datos.
6. Garantizar la transmisión de información de forma segura desde y hacia diferentes puntos de acceso.
7. Contar con medidas emergentes para la transmisión de información.

Niveles de Seguridad Lógica

Según Solarte, F. N. S., Rosero, E. R.E., & del Carmen Benavides, M. (2015) nos menciona que:

> La seguridad lógica establece estándares de niveles de seguridad, siendo uno de los más usados el estándar internacional TCSEC (Trusted Computer System Evaluation) y Orange Book desarrollado según las normas de seguridad de computadores del departamento de defensa de los estados unidos en el año de 1982. Estos niveles establecen diversos tipos de seguridad del sistema operativo y se enlistan desde el de menos gravedad al de mayor gravedad. El estándar antes mencionado ha sido base para la creación de estándares europeos como el ITSEC/ITSEM (Information Technology Security Evaluation Criteria / Methodology) y también de estándares internacionales como el ISO (International Organization For Standardization) y el IEC (International Electrotechnical Commission). Los diferentes niveles requieren en sí de los niveles anteriores de modo que el subnivel B2 abarca los subniveles B1, C2, C1 y D.

Nivel D

En este nivel podemos encontrar aquellos sistemas que no cuentan con algún estándar o especificación de seguridad, a lo que deriva en la inestabilidad del sistema operativo y la falta de métodos de verificación de la identidad de los usuarios y sus permisos de acceso tanto a la información como a las aplicaciones. Podemos poner como ejemplo el sistema MS-DOS**.**

Nivel C1: Protección Discrecional

La identificación de usuarios es necesaria para acceder a la distinta información, se maneja la información de cada usuario de forma privada y se diferencia entre un usuario común y un administrador, este último tiene acceso total.

Una gran cantidad de tareas de la administración se puede realizar por este usuario administrador el cual conlleva una enorme responsabilidad en la seguridad, con la actual capacidad de delegación de los sistemas se torna en algo común encontrar a una o más personas ejerciendo el papel de usuario administrador.

Los requisitos que el C1 debe cumplir son los siguientes:

- **Acceso De Control Discrecional. -** Se distinguirá todos los usuarios y recursos, diferenciándose entre usuario o grupos de usuarios.

- **Identificación y Autenticación. -** El usuario deberá registrar su ingreso identificándose correctamente antes de realizar cualquier actividad en el sistema, tomando en cuenta que sin identificación o autorización no podrá acceder a los datos de otro usuario.

Nivel C2: Protección de Acceso Controlado

Es decir, se logra tener un ambiente de acceso controlado, se controla una cierta cantidad de accesos o intentos fallidos de acceso a las diferentes aplicaciones. Con la capacidad de limitar a los usuarios la ejecución de ciertas acciones o la entrada a determinada información, permitiendo o negando información a usuarios específicos dependiendo no solo de sus permisos sino también del nivel de autorización.

La auditoría en este nivel se usa para crear un registro de acciones realizadas respecto a seguridad por ejemplo las actividades realizadas por los administradores y/o usuarios, siempre es necesario un método de verificación extra para asegurar la identidad del usuario. La gran desventaja se encuentra en la necesidad de recursos adicionales.

Nivel B1: Seguridad Etiquetada

Es la clasificación de los usuarios mediante etiquetas las cuales poseen niveles jerárquicos, donde cada usuario podrá acceder a la información que su posición o status le permita, en donde para poder ingresar a un tipo de información deberá contar con la autorización adecuada, es decir que cada usuario tiene acceso a un tipo específico de información asociado a su rol en la empresa.

Nivel B2: Protección Estructurada

En este nivel es necesario que se identifiquen objetos de nivel superior y objetos de nivel inferior distinguiendo los objetos de nivel superior que sean padre de objetos inferiores, en este nivel la protección estructurada es la principal en hacer referencia a los problemas de un objeto de nivel elevado de seguridad con otro de nivel inferior. El sistema cuenta con la capacidad de informar a los usuarios si sus permisos de acceso y nivel de seguridad han sido modificados; el administrador esta encargada de establecer los canales de comunicación y las características de dichos canales.

Niveles B3: Dominios de Seguridad

Refuerza a los dominios con la instalación de hardware, por ejemplo: el hardware especializado en administrar las redes se usa para proteger la intranet de accesos no autorizados e impedir la modificación o extracción de la información.

Para facilitar el análisis de las estructuras de seguridad estas deben ser lo suficientemente pequeñas. El nivel b3 necesita que el dispositivo del usuario se enlace al sistema a través de una conexión segura, considerando que cada usuario cuenta con un lugar y objeto asignados para acceder.

Nivel A: Protección Verificada

Este nivel incluye procesos de diseño, control y verificación, usando métodos formales para establecer todos los procesos que desempeña un usuario en el sistema, estableciendo este nivel como el más alto.

Al llegar a este nivel los componentes de nivel inferior ya se encuentran incluidos, el diseño ha sido verificado con métodos matemáticos y se cuenta con canales encubiertos y de distribución fiable, se cuenta con una protección sobre el software y el hardware para impedir infiltraciones ante cualquier tipo de movilización de los dispositivos.

Medidas De Protección Y Aseguramiento

Según Solarte, F. N. S., Rosero, E. R.E., & del Carmen Benavides, M. (2015) nos dice que se hablará de medidas de protección y aseguramiento que, aunque por su costo no se pueda lograr en un 100% se pueden aplicar medidas de protección para controlar una serie puntos débiles que hacen vulnerable a un sistema, entre estas medidas las más usadas son:

Controles de acceso

Los controles pueden implementare en paquetes específicos de seguridad o en cualquier otro sistema usado, sobre los sistemas de aplicación en base de datos, los cuales ayudan a la protección del sistema operativo de modificaciones o alteraciones no autorizadas y así mantener la información intacta desde que se la ingreso. Para mantener un control en el sistema se pide lo siguiente.

- **Identificación y Autenticación. -** El usuario deberá portar una identidad validad y autorizada para el acceso a la información, las formas de saber si la identidad es verídica el usuario deberá contar con tarjetas magnéticas, claves numéricas, huella dactilar permitida, un patrón de escritura, contraseñas o a su vez una identificación que se entrega de manera personal a cada usuario como, por ejemplo: pin.

- **Roles. -** Se podrá ingresar a la información de acuerdo a la posición en el nivel jerárquico que la persona representa en la empresa, es decir, el administrador del sistema, gerente, jefes de área o programadores, se tendrá acceso de acuerdo al rol que cumpla en la entidad y si el mismo está autorizado.

- **Limitaciones a los Servicios. –** Se definen como un conjunto de reglas o parámetros que restringen las acciones de los usuarios de acuerdo con su categoría, estas reglas pueden estar preestablecidas por una aplicación o pueden ser establecidas por el administrador de la aplicación.

- **Modalidad de Acceso.** – Todo tipo de información a la cual se requiera acceso deberá ingresar mediante una modalidad, es decir, lectura donde al usuario solo se le permite visualizar los datos, así como copiarlos e imprimirlos; escritura se permite al usuario alterar ingresar o borrar datos; ejecución que permite ejecutar aplicaciones/programas y borrado que permite eliminar recursos del sistema.

  Además de un modo adicional que incluye todos los modos mencionados que seria otorgado a un usuario administrador o super usuario.

- **Ubicación y Horario. –** Asegura un acceso limitado, es decir, no se podrá ingresar en cualquier momento ni en cualquier lugar a información que no le corresponda al usuario proporcionando seguridad a la información de los usuarios.

Control De Acceso Interno

- **Palabras Clave (Password). –** El modo más común de autenticación de un usuario que sirve para mantener protegidos los datos o aplicaciones de un sistema, al ser necesario en muchos casos la creación de varias palabras clave se torna complicado para el usuario el recordarlas lo que deriva en la creación de palabras muy simples y de fácil deducción, para evitar esto se aplica sincronización de password que permite al usuario tener una sola password para diferentes aplicaciones contando con actualización de la password en todas ellas en caso de necesitar ser modificada; también se aplica un periodo de caducidad y control que establece el periodo mínimo de valides de una password así también el periodo máximo tras el cual se puede realizar el cambio de la misma.

- **Encriptación. -** La información que se considera confidencial o relevante para la entidad se encontrará encriptada y solo el personal que tenga conocimiento de la clave podrá desencriptarla sin ningún tipo de inconveniente.

- **Listas de Control de Accesos. -** Consiste en un registro o lista donde se encuentra almacenados los datos de los usuarios sus permisos de acceso y los recursos permitidos para ese usuario.

- **Límites Sobre La Interfaz De Usuario.** - Son límites establecidos que trabajan en base o en conjunto con las listas de control de acceso, en su forma básica pueden ser de 3 tipos tales como menú, visualización de la base de datos y límites físicos sobre una interfaz como ejemplo se pueden mencionar páginas web donde se requiere registrase para poder acceder a las funciones más avanzadas o a descargar contenido de las mismas.

- **Etiquetas de Seguridad. -** Consiste en clasificaciones otorgadas a los recursos con el propósito de controlar los accesos que se tenga a la información dejando en claro que estas no se pueden modificar.

Control de Acceso Externo

- **Dispositivos de Control De Puertos. –** Comúnmente conocidas como llaves que dan acceso al personal autorizado, en la actualidad pueden ser diferentes dispositivos como tarjetas magnéticas, aplicaciones en dispositivos móviles.

- **Firewalls o Puertas De Seguridad. –** Es una pared que elimina o impide que pasen o ingresen aplicaciones que no son permitidas en la red privada, también puede permitir que usuarios autorizados pueden acceder a redes externas como el internet.

- **Acceso de Personal Contratado o Consultores. –** Se requiere la contratación de personal especializado para el control y mantenimiento de los recursos tecnológicos.

- **Accesos Públicos. –** Para el público general que busque consultar información específica, o para la transmisión distribución y recepción de datos deberán contar con medidas de seguridad especificas ya que por estos canales se incrementa el riesgo de vulnerabilidad.

1.7.2.7. Norma ISO 27000 sistema de gestión de seguridad de la información.

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017) habla acerca de los sistemas de gestión de la seguridad de la información en la forma que debe ser implantada por una entidad, cuyo objetivo general la protección de la información. Dentro de esta norma sus objetivos específicos se basan en la triada conocida como confiabilidad, integridad y disponibilidad (CID):

- Confiabilidad de los datos de la entidad
- La integridad de su información
- Su disponibilidad al momento de ser requerida

La correcta implantación de esta norma asegura a la empresa que los posibles riesgos de seguridad informática que puedan presentarse, sean controladas y esperados por la organización teniendo conocimiento de cómo deben enfrentar dichos riesgos.

Beneficios de la ISO 27000

- Brinda una metodología bien estructurada del sistema de gestión de seguridad de la información y de fácil entendimiento respecto.
- Disminución considerable de riesgo de pérdida o robo de información considerada confidencial para la entidad.
- Los usuarios como el personal de la empresa podrán ingresar información relevante bajo medida de seguridad los cuales logren la sensación de confianza en la misma al momento de ser entregada.
- Realización de monitoreos de manera regular para la verificación del correcto manejo de la información evitando posibles riesgos.

1.7.2.8. Norma ISO 27001 Requisitos Para Implementar SGS

Según Herrera, C. Y. C., Soto, D. Y. E H., & Efrén, D. Y. (2015) menciona que estos requisitos son un estándar internacional las cuales se encuentra en una estructura dividida por 10 capítulos, donde sus 3 primeras normas hacen referencia a las generalidades, definiciones y términos, parecidas a otras normas de las ISO, pero el resto de capítulos hacen mención a los requisitos específicos a cumplir que se detallaran a continuación

Tabla 2-1: Estructura ISO 27001

Capítulos: ISO 27001	
1.- Alcance	Aquí es donde se define su campo de actuación o alcance que tendrá dentro de la empresa.
2.- Referencias normativas	Consiste en la información adicional que sirva como guía para la implementación de esta ISO.
3.- Términos y definiciones	Trata de redactar un glosario donde se expliquen todas las palabras que no sean de fácil entendimiento y así poder comprender de lo que trata la norma.
4.- Contexto de la organización	Se coloca en claro el contexto de organización tanto interna como externa, de ahí se procede a la identificación de los problemas que afecta a la entidad y a sus objetivos.
5.- Liderazgo	Exige la participación de la alta dirección para llevar a cabo este punto, además de exigir una política para la seguridad de la informar y así liderar la empresa.
6.- Planificación	Consiste en que los objetivos deben ir acorde a los lineamientos estratégicos del negocio y los posibles riesgos que pueden afecta al cumplimiento de los mismos.
7.- Soporte	Es la encargada de asegurar los recursos que se necesiten para el buen manejo de un sistema, desde el momento en que se lo implanta y asi supervisarlo de manera periódica.
8.- Operación	Contempla un requisito único de la norma contemplándose a través de los procesos y objetivos que la empresa tenga establecido.
9.- Evaluación del desempeño	Exige un correcto control y supervisión de la implantación de la norma, considerando el modelo de deming que es: planificar, hacer, verificar y actuar (PDCA).
10.- Mejora continua	Aquí se comprueba la efectividad de este sistema mediante la aplicación de medidas que ayuden a prevenir posibles errores y dar soluciones inmediatas.

Fuente: Trabajo de Campo

Realizado por: Ucles Romo, D, J. (2020)

1.7.2.9. Norma ISO 27002 Buenas Prácticas Para El SGSI

Definición

Según Calder, A. (2017) nos dice que:

> Esta norma establece controles los cuales ayudan previa a una evaluación de los riesgos a la entidad acerca de los activos más importantes que la organización tenga, se pensó en esta norma para ayudar a la implantación del sistema de gestión de seguridad de la información

(SGSI) la cual puede ser aplicada a cualquier tipo de empresas independientemente de que sean con o sin fines de lucro, pública o privada sin ser necesariamente una empresa de tecnología.

Objetivo

Ayudar a la organización a establecer ciertos principios y guías para tener una mejora continua y seguridad de la información que se maneje por la entidad, a su vez se implementara controles, seguimiento y revisión que proporciones una detección oportuna de posibles riesgos que pueda sufrir la información.

Beneficios de la ISO 27002

- Lograr una concientización respecto a la información, su seguridad, los riesgos, posibles ataques que puede sufrir por personas internas, externas y provenientes de internet.

- Identificar posibles debilidades que puedan vulnerar el acceso de la información y corregir antes de estas represente un problema serio para la empresa.

- Ayuda con la optimización de gastos innecesarios mediante la detección oportuna de posibles riesgos que necesiten medios económicos para corregir lo antes mencionado.

- Con la implementación de esta norma la entidad se vuelve más competitiva dentro del mercado generando más ingresos con la captación de nuevos clientes los cuales han depositado su confianza en la organización, la misma que demostró estar mejor preparada a comparación de otras entidades.

1.7.2.10. Norma 410 Tecnología De La Información

Villena (2016, p. 31) cita a la Contraloría General del Estado (2014) que instituye las normas técnicas de control interno incluyen:

410-01 Organización Informática

La Unidad de Tecnologías de la Informacion deberá constar dentro de una estructura organizacional para brindar tanto sus servicios de apoyo como de asesoría a todas las áreas de la empresa en el momento que esta sea requerida (…)

410-02 Segregación De Funciones

El personal de la Unidad de Tecnologia de la Informacion estarán definidos de manera clara y concreta detallando sus perfiles de puestos, funciones y responsabilidades a realizar. (…)

410 – 03 Plan Informático Estratégico De Tecnología

Para un adecuado control de los recursos informáticos la Unidad de Tecnologia de la Informacion y Comunicación deberá realizar e implementar planes informáticos previamente aprobados para su ejecución. (…)

410 – 04 Políticas y Procedimientos

Se deberá realizar políticas y procedimientos previamente elaborados e implementados por gerencia que sea de utilidad como un documento de respaldo con el fin que sea una guía para que el personal desempeñe sus actividades de manera correcta. (…)

410 – 05 Modelo De Información Organizacional

La Unidad de Tecnologías de la Informacion se encargará de que la información llegue por medios seguros a todas las áreas de entidad de manera segura, integra y confiable, disponible en todo momento. (…)

410 – 06 Administración De Proyectos Tecnológicos

Se facilitará un adecuado control de los proyectos que se vayan a ejecutar en las diferentes áreas por parte de la Unidad de Tecnologías de la Informacion y Comunicación. (…)

410 – 07 Desarrollo Y Adquisición De Software Aplicativo

Abarca todo lo necesarios para que el software, su desarrollo y adquisición se acorde a la necesidad que afronte la empresa y ayude en sus actividades. (…)

410 – 08 Adquisición De Infraestructura Tecnológica

Estará encargada la Unidad de Tecnologías de la Informacion y Comunicación de actualizar o modificar la estructura tecnológica donde se encuentren los recursos de la entidad para un monitoreo adecuado. (…)

410 – 09 Mantenimiento Y Control De La Infraestructura Tecnológica

La Unidad de Tecnologías de la Informacion y Comunicación definirá los controles de un mantenimiento adecuado para el correcto funcionamiento de los equipos durante su uso. (…)

410 – 10 Seguridad De Tecnología De Información

Su fin será el salvaguardar la seguridad tanto física como lógica de perdidas totales como parciales de sus equipos físicos y de la información contenidas en ellos. (…)

410 – 11 Plan De Contingencias

La Unidad de Tecnologías de la Informacion y Comunicación elaborara para luego implementar planes de contingencia que sirva como respaldo de las acciones a tomar en caso de presentarse escenarios de riesgos que involucren a la entidad. (…)

410 – 12 Administración De Soporte De Tecnología De Información

Ayuda a mantener un buen estado de los recursos informáticos tomando sus debidas medidas de prevención y corrección, dando soluciones a los fallos que afecten el desempeño de los mismos.

410 – 13 Monitoreo y Evaluación De Los Procesos y Servicios

Se definirá el alcance que tendrá la evaluación para su metodología y de acuerdo a eso realizar sus debidas correcciones. (…)

410 – 14 Sitio Web, Servicios De Internet E Intranet

Su objetivo será mantener la información segura sin que haya peligro de alguien externo tenga acceso al sistema, manteniendo un envió seguro de la información a gran velocidad. (…)

410 – 15 Capacitación Informática

Su fin es mantener actualizado ante el adelanto de la tecnología año tras año para adaptarse a las nuevas formas de mantener seguro los equipos contra ataques de terceros. (…)

410 – 16 Comité Informático

Su utilidad se basa en establecer estrategias acordes al avance de la tecnología que pueda garantizar la calidad de los servicios de la entidad. (…)

410 – 17 Firmas Electrónicas

Es un conjunto de datos que están asociados a documentación electrónica cuya función e importancia es permitir identificar de manera exacta y sin errores al usuario firmante, manteniendo la integridad y valides del documento firmado. (…)

1.7.2.11. Norma EIA/TIA 568 A

"El estándar de cableado estructurado TIA / EIA definen la forma de diseñar, construir y administrar un sistema de cableado que es estructurado, lo que significa que el sistema está

diseñado en bloques que tienen características de rendimiento muy específicos. Los bloques se integran de una manera jerárquica para crear un sistema de comunicación unificado. Por ejemplo, el grupo de trabajo LAN representan un bloque con los requerimientos de menor rendimiento que el bloque de red troncal, que requiere un cable de alto rendimiento de fibra óptica en la mayoría de los casos.

La norma EIA/TIA 568A específica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. Se hacen recomendaciones para:

- La topología
- La distancia máxima de los cables
- El rendimiento de los componentes

La toma y los conectores de telecomunicaciones

Se pretende que el cableado de telecomunicaciones especificado soporte varios tipos de edificios y aplicaciones de usuario. Se asume que los edificios tienen las siguientes características:

- Una distancia entre ellos de hasta 3 km
- Un espacio de oficinas de hasta 1, 000,000 m2
- Una población de hasta 50,000 usuarios individuales

Las aplicaciones que emplean los sistemas de cableado de telecomunicaciones incluyen, pero no están limitadas a:

- Voz
- Datos
- Texto
- Video
- Imágenes

La vida útil de los sistemas de cableado de telecomunicaciones especificados por esta norma debe ser mayor de 10 años.”

Según los conceptos expuestos anteriormente nos dice que el uso de estándares en los sistemas de redes estructuradas simplifica el establecimiento de un sistema físico de redes, al guiarnos a través de normas probadas y establecidas científicamente dejando de lado el uso de estrategias empíricas; finalmente logrando el adecuado funcionamiento de una red que será evaluada y controlada constantemente.

1.7.2.12. Tipos De Seguridades En Las Redes Informáticas

Para el autor Urbina, G.B (2016) los tipos de seguridades en las redes informáticas son:

Seguridad de Red: Procura la protección de la información que se puede acceder vía internet sean que estén reflejadas en imágenes, fotos o documentos las cuales pueden servir para malicia de terceras personas, es decir, este tipo de seguridad se encarga de las amenazas que pueden existir en la red como, por ejemplo: troyanos, virus, phishing, robo de datos, spyware, suplantación de identidad.

Seguridad de Software: Es la encargada de proteger la integridad de programas y aplicaciones para evitar o eliminar posibles amenazas exteriores que pretendan alterar, sustraer o eliminar la información que maneja el software autorizado, esta información puede ser tanto propia de una empresa como de las aplicaciones y programas que se usen dentro de la misma.

Seguridad de Hardware: Esta destinada a la protección de las computadoras y dispositivos que se encuentren expuestas ante posibles amenazas o intromisiones como son los ataque por saturación o intervención directa de los equipos, se encarga de mantener los equipos operando de forma segura y estable manteniendo la información que contienen fuera del entendimiento no autorizado a través de la encriptación de la misma.

1.7.2.13. Protocolo De Red Segura

Según Dordoigne, J., & Atelin, P. (2016). Los protocolos de red segura se encargan de garantizar la integridad y seguridad que se transfieren por medio de una red como, por ejemplo: el internet, estos protocolos están específicamente desarrollados para impedir que usuarios, programas o dispositivos que no estén autorizados por tu red puedan acceder libremente a la información.

Para Dordoigne, J., & Atelin, P. (2016), los protocolos de red seguro son:

Protocolo SSH

El protocolo Secure Socket Shell (SSH) establece una forma de acceso a internet a través de un ordenador remoto proporcionando autenticación y encriptado entre dos dispositivos que se conectan a internet todo esto de manera segura. Generalmente se utiliza por administradores de red para realizar su trabajo por acceso remoto.

Protocolo HTTP

El protocolo de transferencia de hipertexto (http) está basado en la World Wide Web (WWW) principalmente usado para transmitir mensajes por la red, usando softwares específicos llamados

navegadores los cuales se encargan de interpretar los mensajes recibidos desde un servidor web que haya respondido a nuestra petición.

Protocolo HTTPS

Es el mismo concepto tratado anteriormente solo que agregándole la S, que significa seguro, este protocolo cuenta con un cifrado SSL que mantiene las conexiones seguras.

SMTPS Para Transferencia Correo Electrónico

El SMTPS es un protocolo utilizado para la transmisión de emails, es decir, que está integrado a los protocolos de internet es usado para que los usuarios puedan enviar y recibir emails, con el agregado de estar usando una red segura ya que cuentan con un certificado SSL.

IMAPS Protocolo De Acceso A La Mensajería De Internet

Es un protocolo que permite a los usuarios a los correos electrónicos almacenados en un servidor desde cualquier dispositivo que tenga conexión a internet dejando en claro que no es un protocolo de envió de emails, con el agregado s al usar una red segura que cuenta con un certificado SSL.

1.7.2.14. Análisis DAFO

Speth, C., (2016). Menciona que:

> El análisis de las debilidades, amenazas, fortalezas y oportunidades (DAFO), muestra la situación real de una empresa para saber aplicar una estrategia con el uso de esta herramienta desde el punto de vista externo que consiste en la amenazas y oportunidades y desde el punto de vista interno que son las debilidades y fortalezas que posee la empresa.
>
> **Debilidades. – S**on los puntos vulnerables que tiene una entidad las cuales deben ser identificadas para eliminarlas y transformarlas en fortalezas para beneficio y buen desarrollo de la empresa.
>
> **Amenazas.** – Son todos aquellos puntos que ponen en riesgo la estabilidad económica de la empresa.
>
> **Fortalezas.** – Son todas las capacidades que posee la empresa en cuanto al ambiente laboral, recursos tecnológicos, humano y material que se puede explotar para convertirlas en oportunidad.

Oportunidades. – Consiste en suponer ventajas competitivas a beneficio de la entidad las cuales puedan ayudar al crecimiento económico de la misma.

1.7.2.15. Coso II

Para los autores Gaitán, R. E., & Niebel, B. W. (2015) define al Coso II como un sistema de control interno y de gestión de riesgo donde cuyo objetivo es identificar la raíz de los problemas que ocasionan inconvenientes a la entidad para brindar posibles soluciones y un plan de contingencia para escenarios futuros. El coso II está compuesto por 8 componentes que se detallan a continuación:

Ambiente Interno. – Hace referencia al ambiente que existe dentro de una empresa para el desempeño de las actividades a realizar, es decir, como el personal se siente trabajando en su puesto de trabajo, si la entidad ofrece o cumple con un ambiente adecuado para la correcta eficiencia y eficacia de sus trabajadores.

Establecimiento de Objetivos. – Este componente se relaciona directamente con los objetivos, misión, visión ya establecidos por la entidad, que las actividades que se hicieron, hacen y se encuentran por hacer cumple con lo previsto por la empresa, es decir, si se encamina correctamente con lo que la organización desea cumplir a largo plazo.

Identificación de Eventos. – Consiste en dar con el origen de los posibles escenarios que pueden darse en la entidad los cuales pongan en riesgo el cumplimiento de los objetivos planteados por la empresa, sirviendo como herramienta para saber cómo actuar ante estos posibles eventos sin que dejen consecuencias permanentes en la organización.

Evaluación de Riesgos. - Se procede a realizar un análisis de en qué porcentaje pueden los riesgos llegar afectar a la organización como también se analiza la probabilidad de que esto suceda.

Respuesta al Riesgo. – Una vez analizado el nivel de impacto y la probabilidad de que suceda en el componente antes mencionado la alta dirección deberá determinar posibles respuestas o reacciones que tomara la organización ante el riesgo en beneficio de la misma.

Actividades de Control. - Como su nombre lo indica son aquellas actividades que, de manera cronológica, conjuntamente con las políticas y normas implementadas por la empresa deberán asegurar que las medidas tomadas por la entidad controlen los posibles riesgos a presentarse.

Información y Comunicación. – La información consiste en dar a conocer cómo se está efectuando las medidas que contrarrestaran los posibles riesgos, los resultados que las mismas arrojan mientras que la comunicación hace referencia a la conversación que se debe mantener con todo el personal de la empresa.

Supervisión. - Se lleva a cabo un control de manera regular, monitoreando de cerca que el proceso se esté llevando conforme a lo ya establecido anteriormente para la efectividad de la misma y la mejora continua de la entidad.

1.7.2.16. Ataques Informáticos

Según Vieites, A. G. (2013) nos dice que los ataques informáticos son aquellos intentos de sustraerse información considerada confidencial ya sea de una persona en particular o perteneciente a una entidad para fines maliciosos, es decir, tratar de obtener incentivos económicos a cambio de la información que posee, o hasta la destrucción permanente de la misma.

1.7.2.17. Tipos De Ataques Informáticos

Tabla 3-1: Tipos de Ataques Informáticos

1.- Malware	Se menciona como malware a programas maliciosos como: gusanos, virus y spyware
2.- Suplantación de Identidad (PHISHING)	Phishing es el tipo de ataque informático más común que existe ya que su modo de operar consiste en enviar masivamente correos electrónicos, mensajes en redes sociales o cualquier fuente de información con contenido fraudulento.
3.- Ataques Del Hombre En El Medio (MITM)	Consiste en la intercepción entre dos o más partes con el fin de robar y manipular información.
4.- Ataque De Denegación De Servicio (DOS).	Los ataques dos se encargan de saturar un servicio o una red provocando el colapso de los equipos o de las redes
5.- Inyecciones SQL	Es la inserción de código malicioso realizado de preferencia en una ranura de búsqueda.
6.- Ataque De Fuerza Bruta	Es el uso de software para intentar todas las variables existentes para lograr la combinación correcta de una contraseña.
7.- Secuencias De Comandos Entre Sitios	Este método de ataque trata o inserta código malicioso a través de aberturas o vulnerabilidades en un sitio oficial.
8.- Rootkits	Los rootkits se instalan en programas oficiales desde los cuales puedan lograr acceso remoto a información considerada confidencial
9.- Ingeniería Social	Consiste en la manipulación psicológica con el fin de obtener información que les ayude a

	tener acceso a los equipos informáticos de una empresa.
10.- Ataque por virus	Esta encargada de infectar todos los archivos que se encuentran dentro de un sistema a través de un código maligno.
11.- Troyanos	Aunque este se asemeje al virus su diferencia radica en que el virus destruye por si solo un sistema mientras que el troyano tiene el fin de pasar desapercibido para permitir a un atacante o a un software malicioso acceder al sistema

Fuente: Trabajo de Campo

Realizado por: Ucles Romo, D, J. (2020)

1.7.3. Etapas de una Auditoria

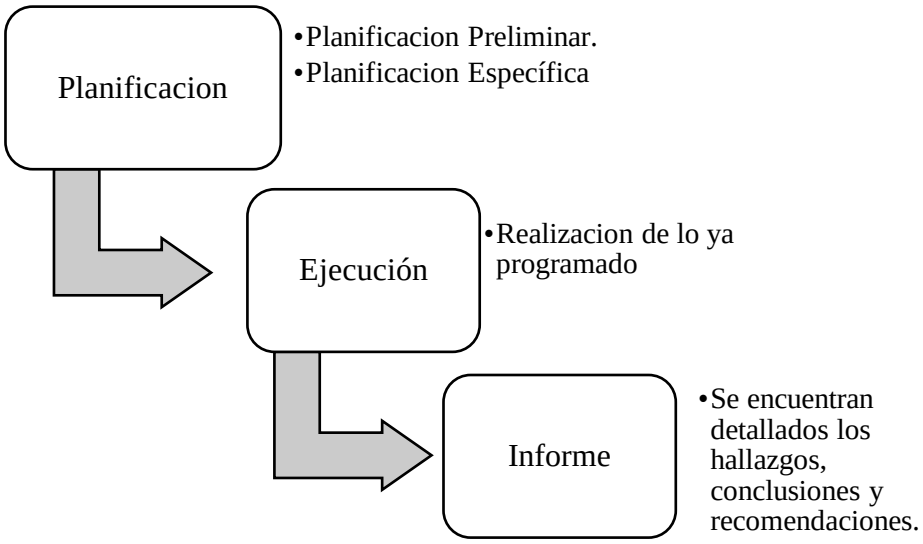


Gráfico 3-1. Fases De La Auditoría Informática

Realizado por: Ucles Romo, D, J. (2020)

1.7.3.1. Planificación

Para el autor Veloz Chunata, J. M. (2015) menciona que:

> Siendo la planificación el primer paso a realizarse se debe considerar de manera estricta todos los recursos que se vayan a utilizar durante la auditoria, detallando los motivos por los cuales se está realizando dicha auditoria, los métodos y técnicas a ejecutarse acorde con la necesidad de la entidad otorgándole el tiempo prudente para completar la planificación de manera cuidadosa, a su vez tomando en cuenta la imparcialidad del

auditor profesional que realizara el trabajo en todas las fases que corresponde una auditoria informática

A su vez la planificación se divide en dos etapas detallas a continuación.

- **Planificación Preliminar**

El objeto de esta etapa es reunir toda la información necesaria que nos brinde un enfoque general de las actividades que se realizan dentro de la entidad tales como producto/servicio que ofertan, reglamentos y políticas. Se determinará también un segundo enfoque mediante observaciones al desempeño de las áreas a auditar, entrevistas tanto al personal como a los clientes con lo cual se obtendrá una perspectiva global de la empresa.

Conforme a la información obtenida y a las observaciones realizadas el auditor profesional procederá a la elaboración de los objetivos y alcance del trabajo, a su vez se emitirá un documento donde conste lo dicho anteriormente de manera detallada para el conocimiento del gerente o jefe a cargo de la entidad.

- **Planificación Específica**

Esta etapa es el complemento de la planificación preliminar ya que indica la manera de cómo se va a conseguir todo lo programado en la anterior etapa, es decir, las estrategias, los métodos a utilizarse para lograr el cumplimiento de los objetivos y metas ya establecidos por la auditoria en base a la información obtenida en la planificación preliminar.

Uno de los objetivos de la planificación especifica es la evaluación del control interno, como esta estructura, a qué nivel se está cumplimiento y las posibles falencia que puedan representar un riesgo para la empresa, en base a las fallas que se puedan encontrar se deberán detallar nuevos procedimientos las cuales lleven a una solución de manera independiente si esta beneficia o perjudica a la entidad considerando que todo lo evaluado sea acorde con la normativa vigente respecto a la actividad que se realice en la organización.

1.7.3.2. Ejecución

El siguiente paso a seguir una vez realizada la planificación preliminar como específica, es la fase de ejecución la cual consiste en poner en marcha el plan que se detallan en la fase anterior para el cumplimiento de todo lo planteado por el auditor, en el tiempo ya especificado, es decir, en la ejecución se llevara a cabo todo lo dicho por el profesional y en caso de encontrar anomalías fuera

de lo ya planificado estas deberán ser tomadas en cuenta y registrarlas dentro de la planificación para poner en consideración el nuevo tiempo estimado para la realización del trabajo.

1.7.3.3. Informe

Esta fase consiste en describir todos los hallazgos del auditor, es decir, todos los problemas que se fueron encontrando durante la ejecución de la auditoria, las consecuencias de dichos problemas y las posibles soluciones a estos, de modo que si surgen inconvenientes similares se contara con una respuesta ante la dificultad.

1.7.4. Fase de una Auditoría Informática

Tabla 4-1: Fases de la auditoria informática

Conocimiento del Sistema	• Relacionado a políticas y aspectos legales. • Las características tanto del sistema operativo como de las aplicaciones de los equipos informáticos.
Análisis de las transacciones y de recursos.	• Analizar e identificar los tipos de recursos informáticos participes en el sistema.
Análisis de Riesgos y Amenazas.	• Identificar tanto los riesgos y amenazas que atente el estado de los equipos y recursos informáticos.
Análisis de Controles	• Si estos en realidad protegen a los recursos informáticos.
Evaluación de Controles	• Determinación de la eficiencia y eficacia de dichos controles.
Informe de Auditoría	• Se abarca conclusiones y recomendaciones de la auditoria.
Seguimiento y Recomendaciones.	• Hace referencia a llevar un control adecuado de las recomendaciones encomendadas.

Fuente: Trabajo de Campo

Realizado por: Ucles Romo, D, J. (2020)

1.8. Marco Conceptual

A

Ataque de Fuerza Buta

Interprétese como la ejecución de un programa que realizará comprobaciones finitas a un sistema de acceso una por una hasta conseguir la clave o el acceso al sistema, la efectividad de este ataque dependerá de la potencia del equipo utilizado o del número de atacantes.

B

Base de datos

Es un repositorio o un almacén que permite guardar cantidades grandes de información de forma ordenada y que sea de fácil acceso.

D

Dispositivo

Es un mecanismo complejo creado para desarrollar una determinada función, los dispositivos tienen que ser físicos como: un teléfono celular, computadoras, tablets, flash memory.

E

Encriptar

Significa ocultar información usando una clave para que no pueda ser entendido por los que no tienen dicha clave.

Enrutar

Que te dirige o define el destino.

F

Fraude

Es el engaño intencional realizado de manera maliciosa para afectar a terceras personas teniendo conocimiento de las consecuencias que implicaría el cometer dicho delito.

H

Hallazgo

Son todas las anomalías, debilidades, problemas que afectan a las actividades realizadas por una entidad, las cuales pueden presentarse en toda empresa ocasionando que la misma no pueda tener un adecuado desempeño.

M

Medios electrónicos

Es un dispositivo a través del cual se puede producir, almacenar o transmitir datos e información en cualquier tipo de red de comunicación, sean abiertas o restringidas como: telefonía móvil o internet.

N

Nodos

Entiéndase como dispositivos o puntos relevantes dentro de una red o puntos de conexión.

P

Phishing

Es estafar usando técnicas de ingeniería social haciéndose pasas por empresa o personas que portan una aparente comunicación oficial.

R

Recursos informáticos

Es cualquier software, aplicación, herramienta, componente o dispositivo que se puede agregar o combinar con una computadora o sistema.

S

Sistemas informáticos

Es un sistema que permite almacenar, procesar y gestionar la información para la cual hace uso de un conjunto de elementos relacionados entre sí como por ejemplo el hardware, software y profesionales informáticos.,

Software

Es el conjunto de programas o rutinas que brinda soporte lógico a un sistema informático para que pueda realizar tareas específicas.

Spyware

Programa malicioso espía que reúne información de un dispositivo informático y la transmite a otro dispositivo externo sin autorización del dueño.

V

Virus

Programa malicioso diseñado para propagarse dentro de un software oficial y causar daños tanto a software como a hardware.

CAPÍTULO II

2. MARCO METODOLÓGICO

2.1. Enfoque de Investigación

El enfoque del trabajo de titulación es mixto; porque se lo realizara de manera cuantitativa porque se reunirá información numérica lo cual ayudara a la realización de encuestas a los empleados y clientes de la empresa Master Technology, y de manera cualitativa se podrán obtener resultados mediante observaciones y entrevistas de la misma manera a empleados y clientes permitiéndonos realizar las conclusiones y recomendaciones correspondientes.

2.2. Nivel de Investigación

Para la realización del trabajo de titulación se utilizó lo siguiente:

- **Investigación de Campo:** Se realizaron visitas de manera regular a la empresa Master Technology de lo cual se obtuvo información relevante, oportuna y suficiente de sus distintas áreas de trabajo, permitiendo la realización del presente trabajo de titulación.
- **Investigación Descriptiva:** Para el proyecto de titulación se hizo uso de las siguientes herramientas de investigación: observación, entrevistas y encuestas; las que proporcionaron los datos necesarios para ejecutar la auditoria informática.
- **Investigación Bibliográfica-Documental:** Para el complemento del presente trabajo de titulación se tomó información correspondiente de libros de autores varios, páginas web, normativas vigentes que se encuentren relacionados al tema de auditoria informática, siendo indispensable su uso para la realización de este trabajo.

2.3. Diseño de Investigación

El presente trabajo de titulación es no experimental porque no existe la manipulación o control de las variables independientes ya que se las observa y se las recopila tal y como se presenta en el entorno productivo

2.4. Tipo de Estudio

Aplicada. - Se solucionaron los problemas detallados en el trabajo de titulación que presentaba la empresa Master Technology, mejorando la eficiencia, eficacia en el manejo de la información y el nivel de seguridad de la misma, aportando un informe con sus respectivas recomendaciones para la mejora continua.

2.5. Población y Muestra

De acuerdo con la información proporcionada por la empresa, cuenta con 47 empleados laborando actualmente para la empresa, la cual se detalla a continuación.

Tabla 1-2: Personal Master Technology

Área	Número de empleados
Área comercial	18
Marketing	4
Área financiera	9
Área operativa	9
Servicio técnico	7
Total	47

Fuente: Trabajo de Campo

Realizado por: Ucles Romo, D, J. (2020)

Una vez determinado el personal correspondiente a la empresa se efectúa la fórmula para determinar que se va a representar en el presente trabajo de investigación.

$$n = \frac{Z^2 NPQ}{Z^2 PQ + (N-1)e^2|}$$

En donde:

n= tamaño de la muestra

Z= nivel de confianza 95% (1,96)

P= probabilidad de ocurrencia 0,5

Q= probabilidad de no ocurrencia 1-0,5= 0,5

N= población (47)

E= error de muestreo

$$n = \frac{1,96^2 * 47 * 0,5 * 0,5}{1,96^2 * 0,5 * 0,5 + (47 - 1) * 0,5^2}$$

$$n = \frac{45,1388}{0,9604 + 0,1150}$$

$$n = \frac{45,1388}{1,0754}$$

$$n = 41,97$$

$$n = 42$$

La muestra a realizar para el presente trabajo de investigación es de 42.

2.6. Métodos, Técnicas E Instrumentos De Investigación

Métodos

Para el presente trabajo de titulación se usaron los siguientes métodos.

- **Método Deductivo:** Se uso para la obtención de información requerida para estructurar correctamente el marco teórico enfocándose de lo general a lo especifico, obteniendo además información oportuna de libros, normativas vigentes, siendo esta, la base para la realización de la parte práctica del trabajo de titulación.
- **Método Inductivo:** Se uso para redacción del informe de auditoría donde se detallan conclusiones y recomendaciones para la empresa Master Technology, canto quito, provincia de pichincha, apoyándose en los resultados obtenidos durante la realización de la auditoria informática tema de este trabajo de titulación.

Técnicas

- **Entrevista:** Se realizo una entrevista al gerente de la empresa con el objetivo de conseguir información suficiente respecto a los problemas observados dentro de la entidad, adicional se realizó la entrevista de personal al azar con el objetivo de recopilar información relevante respecto a los problemas propuestos.

- **Observación No Participativa:** Se efectuaron visitas de manera regular a las diferentes áreas que conforman la empresa Master Technology, cantón quito, con el fin de observar las funciones, actividades

- **Encuesta:** Se logro aplicar una encuesta basada en una serie de preguntas relacionadas a la actividad de la empresa para conocer la situación de la misma con el fin de obtener información necesaria acerca de la seguridad, control y manejo de los recursos informáticos.

2.7. Análisis e Interpretación de Resultados

Resultados de la Encuesta Aplicada al Personal Técnico de la Empresa Master Technology, Cantón Quito, Provincia de Pichincha.

1) El acceso al lugar donde se ubica el servidor de la empresa está restringido para el personal no autorizado.

Tabla 2-2: Restricción del Personal no Autorizado

Alternativa	Respuesta	Porcentaje %
SI	7	100%
NO	0	0%
TOTAL	**7**	**100%**

Fuente: Personal Master Technology

Realizado por: Ucles Romo, D, J. (2020)

Gráfico 4-2. Restricción del Personal No Autorizado

Realizado por: Ucles Romo, D, J. (2020)

Análisis: El 100% de las personas encuestadas que corresponden al personal técnico respondieron que el lugar donde se encuentra el servidor SI se encuentra restringido para el personal no autorizado.

2) El área informática cuenta con las seguridades internas y externas.

Tabla 3-2: Cámaras de Seguridad

Alternativa	Respuesta	Porcentaje %
SI	4	57%
POCO	2	29%
MUY POCO	1	14%
NINGUNA	0	0%
TOTAL	**7**	**100%**

Fuente: Personal Master Technology

Realizado por: Ucles Romo, D, J. (2020)

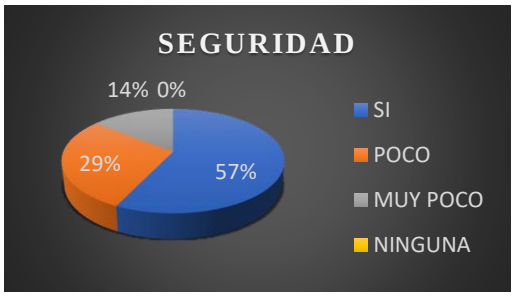


Gráfico 5-2. Seguridad Interna y Externa

Realizado por: Ucles Romo, D, J. (2020)

Análisis: Del 100% de las personas encuestadas que corresponden al personal técnico el 57% respondieron que en el área informática si cuenta con las seguridades interna y externas; el 29% respondió que la misma cuenta con pocas camas de seguridad mientras que el 14% menciono que existe muy pocas cámaras.

3) En caso de fallo de los sistemas informáticos la empresa cuenta con medidas de seguridad y respaldo de la información.

Tabla 4-2: Medidas de Seguridad y Respaldo

Alternativa	Respuesta	Porcentaje %
SI	2	29%
NO	5	71%
TOTAL	**7**	**100%**

Fuente: Personal Master Technology

Realizado por: Ucles Romo, D, J. (2020)

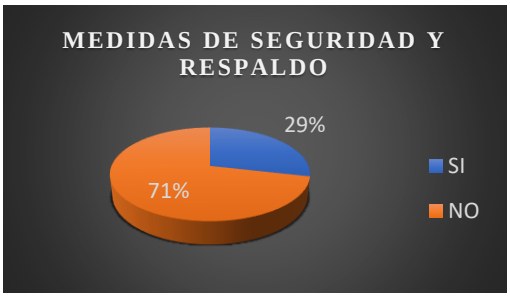


Gráfico 6-2. Medidas de Seguridad y Respaldo

Realizado por: Ucles Romo, D, J. (2020)

Análisis: Del 100% de las personas encuestadas que corresponden al personal técnico el 71% respondieron que en el caso de que exista fallo en sus sistemas informáticos estos NO con cuentan medidas de seguridad ni de respaldo de la información; mientras que el 29% menciono que SI existe dichas medidas de seguridad y respaldo de la información.

4) El servidor dispone de aire acondicionado para regular la temperatura.

Tabla 5-2: Regulación de Temperatura

Alternativa	Respuesta	Porcentaje %
SI	7	100%
NO	0	0%
TOTAL	**7**	**100%**

Fuente: Master Technology

Realizado por: Ucles Romo, D, J. (2020)

Gráfico 7-2. Regulación de Temperatura

Realizado por: Ucles Romo, D, J. (2020)

Análisis: Del 100% de las personas encuestadas que corresponden al personal técnico el 100% respondieron que servidor SI cuenta con aire acondicionado para regular la temperatura de sus equipos.

5) **Los dispositivos electrónicos que se conectan a la red informática (celulares, computadores) de la empresa cuentan con programas de protección para evitar riesgos informáticos.**

Tabla 6-2: Programas de Protección

Alternativa	Respuesta	Porcentaje %
SI	3	43%
NO	4	58%
TOTAL	**7**	**100%**

Fuente: Personal de Master Technology

Realizado por: Ucles Romo, D, J. (2020)

Gráfico 8-2. Programas de Protección

Realizado por: Ucles Romo, D, J. (2020)

Análisis: Del 100% de las personas encuestadas que corresponden al personal técnico el 57% respondieron que todos los dispositivos electrónicos, es decir, celulares computadores NO cuentan con programas de protección para evitar riesgos informáticos; mientras que el 43% menciono que SI existe dichos programas de protección para evitar el riesgo informático.

Resultados de la Encuesta Aplicada al Personal Administrativo de la Empresa Master Technology, Cantón Quito, Provincia de Pichincha.

1) **El área informática cuenta con una salida de emergencia.**

Tabla 7-2: Salida de Emergencia

Alternativa	Respuesta	Porcentaje %
SI	39	100%
NO	0	0%
TOTAL	**39**	**100%**

Fuente: Personal de Master Technology

Realizado por: Ucles Romo, D, J. (2020)

Gráfico 9-2. Salida de Emergencia

Realizado por: Ucles Romo, D, J. (2020)

Análisis: Del 100% de las personas encuestadas que corresponden al personal administrativo el 100% respondieron que la empresa SI cuentan con un a salida de emergencia.

2) La señalética de las áreas del área informática es suficiente y se encuentra visible.

Tabla 8-2: Señalética

Alternativa	Respuesta	Porcentaje %
SI	20	51%
POCO	15	39%
NINGUNA	4	10%
TOTAL	**39**	**100%**

Fuente: Master Technology

Realizado por: Ucles Romo, D, J. (2020)

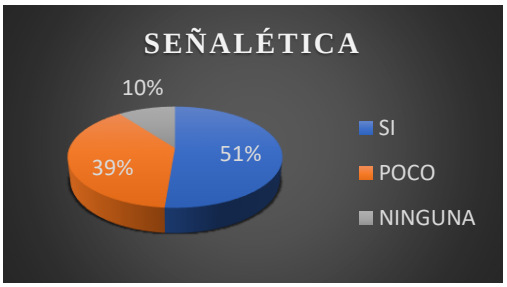


Gráfico 10-2. Señalética

Realizado por: Ucles Romo, D, J. (2020)

Análisis: Del 100% de las personas encuestadas que corresponden al personal administrativo el 51% respondieron que la señalética en la empresa es suficiente y se encuentra visible; el 39% respondió que la señalética no es suficiente y es poco visible; mientras que el 10% menciono que no existe señalética en la empresa y que por lo tanto no es visible.

3) **Usted ha participado en las capacitaciones institucionales relacionadas al área informática.**

Tabla 9-2: Capacitaciones Institucionales

Alternativa	Respuesta	Porcentaje %
SI	23	59%
NO	16	41%
TOTAL	**39**	**100%**

Fuente: Personal Master Technology

Realizado por: Ucles Romo, D, J. (2020)

Gráfico 11-2. Capacitaciones Institucionales

Realizado por: Ucles Romo, D, J. (2020)

Análisis: Del 100% de las personas encuestadas que corresponden al personal administrativo el 59% respondieron que SI asisten a las capacitaciones institucionales que la empresa realiza; mientras que el 41% menciono que NO asiste a las capacitaciones institucionales.

Resultados de la Encuesta Aplicada al Gerente Administrativo de la Empresa Master Technology, Cantón Quito, Provincia de Pichincha.

1) **Los usuarios que ingresan al sistema cuentan con claves de acceso personal.**

Tabla 10-2: Perfiles de Usuario

Alternativa	Respuesta	Porcentaje %
SI	0	0%
NO	1	100%
TOTAL	**1**	**100%**

Fuente: Gerente Administrativo

Realizado por: Ucles Romo, D, J. (2020)

Gráfico 12-2. Claves de Acceso

Realizado por: Ucles Romo, D, J. (2020)

Análisis: El Gerente Administrativo de la Empresa Master Technology respondió que los usuarios no ingresan al sistema con claves de acceso personal.

2) Se cuenta con los recursos informáticos necesarios para el buen funcionamiento del negocio.

Tabla 11-2: Recursos Informáticos

Alternativa	Respuesta	Porcentaje %
SI	0	0%
NO	1	100%
TOTAL	**1**	**100%**

Fuente: Gerente Administrativo

Realizado por: Ucles Romo, D, J. (2020)

Gráfico 13-2. Recursos Informáticos

Realizado por: Ucles Romo, D, J. (2020)

Análisis: El Gerente Administrativo de la Empresa Master Technology respondió que la entidad NO cuenta con los recursos informáticos necesarios para que su negocio funcione correctamente acorde a su actividad.

3) La empresa cuenta con un plan establecido para la actualización de software de sus sistemas informáticos.

Tabla 12-2: Actualización Lógica

Alternativa	Respuesta	Porcentaje %
SI	0	0%
NO	1	100%
TOTAL	**1**	**100%**

Fuente: Gerente Administrativo

Realizado por: Ucles Romo, D, J. (2020).

Gráfico 14-2. Actualización de Software

Realizado por: Ucles Romo, D, J. (2020)

Análisis: El Gerente Administrativo de la Empresa Master Technology respondió que la entidad NO cuenta con un plan establecido para la actualización de software de sus sistemas informáticos.

4) La empresa cuenta con un plan estratégico establecido para la actualización de sus sistemas informáticos físicos.

Tabla 13-2: Actualización Física

Alternativa	Respuesta	Porcentaje %
SI	0	0%
NO	1	100%
TOTAL	**1**	**100%**

Fuente: Gerente Administrativo

Realizado por: Ucles Romo, D, J. (2020).

Gráfico 15-2. Actualización Física

Realizado por: Ucles Romo, D, J. (2020)

Análisis: El Gerente Administrativo de la Empresa Master Technology respondió que la entidad NO cuenta con un plan establecido para la actualización física de sus sistemas informáticos.

5) Se están destinando los recursos informáticos en las cantidades necesarias para cada área del negocio o empresa.

Tabla 14-2: Recursos Necesarios por Área

Alternativa	Respuesta	Porcentaje %
SI	0	0%
NO	0	0%
DESCONOZCO	1	100%
TOTAL	**1**	**100%**

Fuente: Gerente Administrativo

Realizado por: Ucles Romo, D, J. (2020).

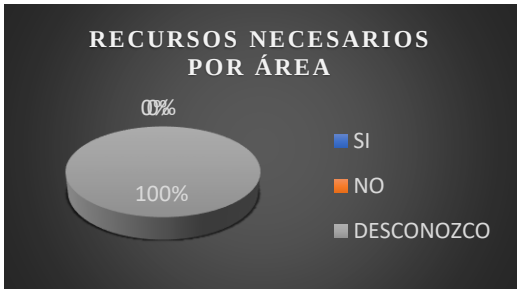


Gráfico 16-2. Recursos Necesarios Por Área

Realizado por: Ucles Romo, D, J. (2020)

Análisis: El Gerente Administrativo de la Empresa Master Technology respondió que DESCONOCE si se asignaran los recursos informáticos necesarios para cada área de la entidad.

6) En caso de contar con un plan estratégico para la actualización de sus equipos informáticos, dentro de qué período de tiempo se ejecutaría el mismo.

Tabla 15-2: Período de Tiempo

Alternativa	Respuesta	Porcentaje %
De 1 a 3 años	0	0%
De 3 a 5 años	0	0%
De 5 a 7 años	1	100%
De 7 a10 años	0	0%
TOTAL	**1**	**100%**

Fuente: Gerente Administrativo

Realizado por: Ucles Romo, D, J. (2020).

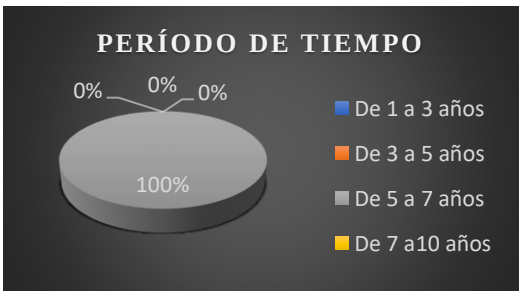


Gráfico 17-2. Período de Tiempo

Realizado por: Ucles Romo, D, J. (2020)

Análisis: El Gerente Administrativo de la Empresa Master Technology respondió que su plan estratégico para la actualización de sus equipos informáticos se ejecute después de 5 o 7 años.

7) Los recursos informáticos pertenecientes a la empresa cuentan con póliza de seguros.

Tabla 16-2: Póliza de Seguros

Alternativa	Respuesta	Porcentaje %
SI	0	0%
NO	1	100%
TOTAL	**1**	**100%**

Fuente: Gerente Administrativo

Realizado por: Ucles Romo, D, J. (2020).

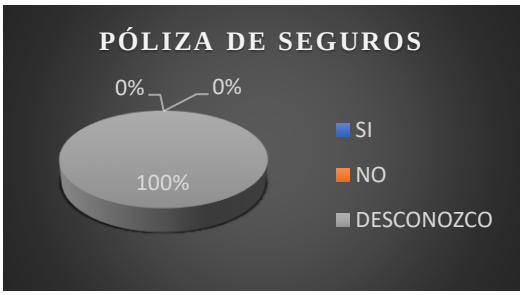


Gráfico 18-2. Póliza de Seguros

Realizado por: Ucles Romo, D, J. (2020)

Análisis: El Gerente Administrativo de la Empresa Master Technology respondió que los recursos informáticos pertenecientes a su empresa NO cuentan con una póliza de seguros como respaldo antes acontecimientos inesperados.

2.8. IDEA A DEFENDER

La Auditoria informática a la Empresa Master Technology, Cantón Quito, Provincia de Pichincha, Período 2019, valorará la integridad, confidencialidad y disponibilidad de los recursos, equipos informáticos y su información mediante el uso de métodos, técnicas, estándares y herramientas.

CAPITULO III

3. MARCO DE RESULTADOS, DISCUSIÓN Y ANÁLISIS DE RESULTADOS

3.1. AUDITORÍA INFORMÁTICA A LA EMPRESA MASTER TECHNOLOGY, CANTÓN QUITO, PROVINCIA DE PICHINCHA, PERÍODO 2019.

3.2. CONTENIDO DE LA PROPUESTA

3.2.1. Archivo Permanente

INSTITUCIÓN	MASTER TECHNOLOGY
GERENTE	JIMENEZ TORRES RICHARD AUGUSTO
RUC	17141587790001
PROVINCIA	PICHINCHA
DIRECCIÓN	SAN GREGORIO Y VERSALLES OE252
TELÉFONO	025126614/ 099-990-8072
CORREO ELECTRÓNICO	gerencia@mastertechnology.com.ec
NATURALEZA DEL TRABAJO	AUDITORÍA INFORMÁTICA
PERÍODO	2019

Elaborado por: **D.J.U. R** **Fecha:** **07/07/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **07/07/2020**

ÍNDICE REFERENCIA

P/T

Reseña Histórica	RH 1/1
Misión/ Visión	MV 1/1
Hoja de Marcas	HM 1/1
Programa de Auditoría	PA 1/1

Elaborado por: **D.J.U. R** **Fecha:** **07/07/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **07/07/2020**

3.2.1.1. Reseña Histórica

Master Technology fue creada en el año 2005 situándose dentro del sector de las nuevas tecnologías de la información y comunicación, la idea de la creación de la entidad surge con la intención de innovar y experimentar el mundo de la tecnología con sus diferentes derivaciones, con las posibilidades de poder ofertar servicios de consultoría solucionado así problemas de la población conjuntamente con los servicios de informática a las pymes en un futuro.

Teniendo como objetivo la creación de soluciones cuyas características se identifiquen con la creatividad, calidad e innovación para que de esta manera el cliente pueda así tener una mejora competitiva y económica de su negocio, la cual también pueda ayudar en el incremento de confianza de cada cliente que pueda pertenecer a la empresa, ayudando y ayudándonos a crecer de igual a igual con otras empresas que persigan un mismo objetivo.

La filosofía de la empresa se concentra en ganarse la confianza, llegar a convertirnos en socios tecnológicos de las pequeñas y medianas empresas consiguiendo el éxito no solo a beneficio propio sino pensando en una sociedad cuyas necesidades tecnológicas varían con el pasar de los años y así adaptarnos cumpliendo las expectativas de todos y cada uno que formen parte de la empresa Master Technology

3.2.1.2. Misión

Somos una empresa enfocada en la innovación con sentido de responsabilidad con la sociedad ofertando servicios/ productos de calidad, de aparatos y equipos de comunicación incluido partes, piezas al por mayor y por menos ofreciendo a su vez servicios de consultoría a las pequeñas y medianas empresas, personas particulares tanto nacionales como extranjeras.

3.2.1.3. Visión

Ser una empresa reconocida por sus productos y servicios de calidad dentro del mercado nacional, adaptándonos día a día a las necesidades cambiantes de la sociedad y al avance tecnológico cumpliendo a cabalidad la expectativa de nuestros clientes mediante la satisfacción de sus necesidades en el ambiente tecnológico y de telecomunicación.

3.2.1.4. Valores

- ✓ Responsabilidad
- ✓ Paciencia
- ✓ Respeto
- ✓ Lealtad
- ✓ Confidencialidad
- ✓ Disciplina
- ✓ Solidaridad
- ✓ Trabajo en Equipo
- ✓ Compromiso
- ✓ Vocación
- ✓ Humildad
- ✓ Ética

EMPRESA MASTER TECHNOLOGY
HOJA DE MARCAS
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

HM 1/1

MARCA	SIGNIFICADO
❖	**Hallazgo**
✓	**Revisado**
♈	**Constatación Física**

Elaborado por: **D.J.U. R** **Fecha:** **07/07/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **07/07/2020**

Objetivo General

Determinar las formalidades que se llevara a cabo entre la Empresa Master Technology y la Profesional encargada de la Auditoria Informática a realizarse.

Objetivo Específico

Establecer los pasos a seguir en la realización de la Auditoria Informática.

N.º	PROCEDIMIENTO	REFERENCIA	ELABORADO POR	FECHA
1	Programa de auditoria.	PA 1/1	D.J.U. R	29/07/2020
2	Carta de Presentación.	CA 1/1	D.J.U. R	29/07/2020
3	Propuesta de Trabajo	PT 1/1	D.J.U. R	29/07/2020
4	Aprobación de la Propuesta	AP 1/1	D.J.U. R	30/07/2020
6	Orden de Trabajo	OT 1/1	D.J.U. R	31/07/2020
7	Notificación del Inicio del Trabajo de Auditoria.	NITA 1/1	D.J.U. R	03/08/2020

Elaborado por: **D.J.U. R** **Fecha:** **07/07/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **07/07/2020**

EMPRESA MASTER TECHNOLOGY
CARTA DE PRESENTACIÓN
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

CP 1/1

Riobamba, 29 De Julio del 2020

Ingeniero.

JIMENEZ TORRES RICHARD AUGUSTO

GERENTE ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

Presente. –

Nos complace mencionarle nuestra propuesta de trabajo para la realización de la Auditoría Informática a la Empresa Master Technology, brindándole un servicio de calidad contando con los conocimientos necesarios para el trabajo de auditoria, nos comprometemos a demostrar trasparencia, puntualidad, responsabilidad, honestidad y ética por parte de la firma auditora, además se entregara un informe final donde se detallaran los problemas detectados con sus soluciones añadiendo conclusiones y recomendaciones que ayuden a la correcta toma de decisiones.

Nuestra firma auditora está conformada por profesionales altamente calificados con experiencia y conocimiento en el ámbito de la Auditoria Informática, dicha firma está representada por un supervisor el cual da certeza la calidad del trabajo a realizar.

A continuación, le ponemos a su consideración nuestra propuesta de trabajo, quedando a su total disposición. De manera anticipada agradecemos la atención prestada a la presente.

Atentamente,

Ing.: Willian Geovanny Yanza Chávez
JEFE DEL EQUIPO DE AUDITORÍA

Elaborado por:	**D.J.U. R**	**Fecha:**	**07/07/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**07/07/2020**

Riobamba, 29 De Julio del 2020

Ingeniero.

JIMENEZ TORRES RICHARD AUGUSTO

GERENTE ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

Presente. –

Estimado Ingeniero Jiménez Torres Richard Augusto, nos complace presentarle a usted la propuesta de trabajo de Auditoría Informática a realizarse dentro de la Empresa Master Technology del Cantón Quito, Provincia de Pichincha, Período 2019.

Esta propuesta se elaboró con la finalidad de cumplir con los requerimientos acorde a las necesidades que competen con las actividades de su entidad.

Objetivo General

Aplicar una auditoría informática a la empresa Master Technology, cantón quito, provincia de pichincha, período 2019, para valorar la integridad, confidencialidad y disponibilidad de los recursos, equipos informáticos y su información mediante el uso de métodos, técnicas, estándares y herramientas de auditoria informática para la empresa.

Objetivos Específicos

- Fundamentar y estructurar el marco teórico mediante la revisión bibliográfica de diferentes autores para sustentar el presente trabajo de titulación.
- Aplicar la metodología establecida en el proceso de la auditoria informática para la determinación u obtención de evidencias y posterior elaboración del informe.
- Presentar el informe final de auditoria, con las conclusiones y recomendaciones orientadas a mejorar el uso y gestión de la información con respecto a la integridad, disponibilidad y confidencialidad de los sistemas y recursos informáticos de la empresa.

Alcance de la Auditoría Informática

El período dentro del cual está comprendida la Auditoria Informática es del 01 de enero al 31 de diciembre del 2019.

Plazo

El plazo estimado para la aplicación de la Auditoría Informática es de 60 días laborables.

Recursos Humanos

La firma auditora Valídate Auditoria está conformada por:

- Ing. Willian Geovanny Yanza Chávez **Jefe de Equipo**
- Dr. Carlos Volter Buenaño Pesántez **Supervisor**
- Ing. Didima Johanna Ucles Romo **Auditora**

Agradecemos anticipadamente por la atención prestada a la presente.

Atentamente,

Ing.: Willian Geovanny Yanza Chávez
JEFE DEL EQUIPO DE AUDITORÍA

Elaborado por: **D.J.U. R** **Fecha:** **07/07/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **07/07/2020**

Centro Comercial Quitus Local 351-352 San Gregorio s/n y Versalles
Teléfonos: 512 6614/ 512 6615/ 0999 908 072 / 0999 630 070
Información: ventas@solve361.com E-mail gerencia@mastertechnology.com.ec
Quito-Ecuador

Riobamba, 30 de Julio del 2020.

Ingeniero

Willian Geovanny Yanza Chávez
JEFE DEL EQUIPO DE AUDITORÍA

De mi Consideración:

Reciba un cordial saludo a nombre de MASTER TECHNOLOGY, por medio de esta presente me permito informar que, al haber analizado la propuesta de trabajo antes presentada, ha sido ACEPTADA por el Gerente Administrativo para su inmediata ejecución.

Atentamente,

JIMENEZ TORRES RICHARD AUGUSTO
GERENTE ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

EMPRESA MASTER TECHNOLOGY
ORDEN DE TRABAJO
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

OT 1/1

N.º 001- VAA-2020

Riobamba, 31 de Julio del 2020.

Ingeniero.

JIMENEZ TORRES RICHARD AUGUSTO
GERENTE ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

De mi consideración:

Previa autorización del Proyecto de trabajo de Titulación de la Facultad de Administración de Empresas, Escuela de Contabilidad y Auditoría, permítase a la estudiante Didima Johanna Ucles Romo la realización de la "AUDITORÍA INFORMÁTICA A LA EMPRESA MASTER TECHNOLOGY, CANTÓN QUITO, PROVINCIA DE PICHINCHA, PERÍODO 2019".

Al finalizar el proyecto de titulación se emitirá las respectivas conclusiones y recomendaciones que constará de manera detallada en el informe de auditoría.

Atentamente,

Ing.: Willian Geovanny Yanza Chávez
JEFE DEL EQUIPO DE AUDITORÍA

Elaborado por:	**D.J.U. R**	**Fecha:**	**07/07/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**07/07/2020**

EMPRESA MASTER TECHNOLOGY
NOTIFICACIÓN DE INICIO DE AUDITORÍA
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

NIA 1/1

Riobamba, 03 de agosto del 2020.

Ingeniero.

JIMENEZ TORRES RICHARD AUGUSTO
GERENTE ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

Presente.

De acuerdo con la Orden de Trabajo N.º 001-VAA-2020, se le notifica que el inicio de la "AUDITORÍA INFORMÁTICA A LA EMPRESA MASTER TECHNOLOGY, CANTÓN QUITO, PROVINCIA DE PICHINCHA, PERÍODO 2019". El cual está comprendido desde el 01 de enero al 31 de diciembre del 2019 por lo que es indispensable se otorgue la información necesaria para el buen desarrollo del presente proyecto de titulación.

El equipo de auditoría está conformado de la siguiente manera:

- Ing. Willian Geovanny Yanza Chávez **Jefe de Equipo**
- Dr. Carlos Volter Buenaño Pesántez **Supervisor**
- Ing. Didima Johanna Ucles Romo **Auditora**

De antemano le agradecemos por la atención prestada a la presente.

Atentamente,

Ing.: Willian Geovanny Yanza Chávez
JEFE DEL EQUIPO DE AUDITORÍA

Elaborado por:	**D.J.U. R**	**Fecha:**	**07/07/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**07/07/2020**

3.2.2. *Archivo Corriente*

INSTITUCIÓN	MASTER TECHNOLOGY
GERENTE	JIMENEZ TORRES RICHARD AUGUSTO
RUC	17141587790001
PROVINCIA	PICHINCHA
DIRECCIÓN	SAN GREGORIO Y VERSALLES OE252
TELÉFONO	025126614/ 099-990-8072
CORREO ELECTRÓNICO	gerencia@mastertechnology.com.ec
NATURALEZA DEL TRABAJO	AUDITORÍA INFORMÁTICA
PERÍODO	2019

Elaborado por: **D.J.U. R** **Fecha:** **28/07/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **28/07/2020**

ÍNDICE	REFERENCIA.P/T
Archivo Corriente	AC 1/1
Índice del Archivo Corriente	IAC 1/1
FASE I: PLANIFICACIÓN	
Planificación Preliminar	PP 1/1
Planificación Específica	PE 1/1
Informe de visita preliminar	IVP 1/1
FASE II: EJECUCIÓN	
Análisis Situacional	AS 1/1
Cuestionarios de Control Interno	CCI 1/1
Matriz de Resumen de Cuestionarios	MRC 1/1
Hoja de Hallazgos	HH 1/1
FASE III: COMUNICACIÓN DE RESULTADOS	
Informe de Auditoría	IA 1/1

Elaborado por: **D.J.U. R** **Fecha:** **28/07/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **28/07/2020**

FASE I: PLANIFICACIÓN

3.2.3. PLAN DE AUDITORÍA INFORMÁTICA

Antecedentes: Es una institución que se dedica a la importación, distribución y asesoría respecto a equipos tecnológicos que cuenta con una intranet establecida según la Norma EIA/TIA 568 A, que entrelaza sus diversos equipos informáticos, además de una red de interconexión segura con sus sucursales.

Objetivo General

Realizar la revisión y verificación del cumplimiento de las normas mediante la Auditoria Informática a la infraestructura física de la red de la empresa Master Technology.

Objetivos Específicos

- Planificar la Auditoria que permita identificar las condiciones actuales en las que se encuentra la empresa en el área tecnológica.

- Aplicar procesos de auditoria informática mediante el modelo COSO II como herramienta de apoyo para la inspección del sistema informático, hardware, software las redes y de las seguridades de la empresa.

- Identificar las soluciones mediante planes de mejora referente al sistema informático, hardware, software, redes y a sus seguridades tanto físicas como lógicas.

Alcance y Delimitación

- Dentro de la auditoria se identificará en qué condiciones actuales se encuentra el sistema informático, hardware, software, redes y a sus seguridades tanto físicas como lógicas.

Objetivo del Alcance: Verificar el cumplimiento de las normas con la prestación de los servicios de la empresa para la optimización de los recursos informáticos.

Elaborado por:	**D.J.U. R**	**Fecha:**	**28/07/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**28/07/2020**

Puntos a Evaluar

- Cableado de Redes
- Seguridad Física
- Seguridad Lógicas
- Distribución de los recursos Informáticos
- Estrategias de mejora continua del Área Informática
- Protocolos preventivos y correctivos del área tecnológica

Metodología

Se llevará a cabo mediante los cuestionarios de control interno COSO II el cual se encuentra conformado por 8 componentes que son:

1) Ambiente Interno
2) Establecimiento de Objetivos
3) Identificación de Acontecimientos
4) Evaluación de Riesgos
5) Respuesta a los riesgos
6) Actividades de Control
7) Informacion y Comunicación
8) Supervisión

RECURSOS

Recursos Humanos

- Ing. Willian Geovanny Yanza Chávez — **Jefe de Equipo**
- Dr. Carlos Volter Buenaño Pesántez — **Supervisor**
- Ing. Didima Johanna Ucles Romo — **Auditora**

Recursos Físicos

- Archivador
- Esferos
- Hojas Papel Bond
- Carpetas
- Portaminas
- CD

Recursos Tecnológicos

- Computadora Portátil
- Memoria Flash
- Cámara
- Teléfono
- Impresora
- Scanner
- Internet

Elaborado por: D.J.U. R **Fecha:** 28/07/2020

Revisado por: W.G.Y.CH/C.V. BP **Fecha:** 28/07/2020

Presupuesto

DETALLE	VALOR
Pasajes a la Ciudad de Quito	**40,00**
Transporte dentro de la Ciudad de Quito	**20,00**
Viáticos	**30,00**
Aplicación de Encuestas	**5,00**
Saldo Móvil	**60,00**
TOTAL	**155,00**

3.2.3.1. FASE I: PLANIFICACIÓN

N.º	Procedimiento	Referencia/T	Elaborado por:	Fecha
	Planificación Preliminar			
1	Programa de Auditoria	PA 1/1	D.J.U. R	05/08/2020
2	Realizar una Visita Preliminar	VP 1/1	D.J.U. R	06/08/2020
3	Carta De Presentación	CP 1/1	D.J.U. R	06/08/2020
4	Carta De Compromiso	CP 1/1	D.J.U. R	06/08/2020
5	Memorándum De Planificación	MP 1/1	D.J.U. R	07/08/2020
6	Narrativa De La Visita Preliminar	NVP 1/1	D.J.U. R	07/08/2020
7	Entrevista al Técnico	ET 1/1	D.J.U. R	07/08/2020
8	Solicitud de Información Requerida	SEO 1/1	D.J.U. R	07/08/2020
9	Respuesta a la Solicitud de la Información Requerida	RSEO 1/1	D.J.U. R	07/08/2020
10	Áreas Criticas	AR 1/1	D.J.U. R	07/08/2020

Elaborado por: **D.J.U. R** **Fecha:** **28/07/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **28/07/2020**

VISITA A MASTER TECHNOLOGY

Fecha de Inicio: 06 /07/2020	**Hora de Inicio:** 09h00 am
Fecha de Término: 09/07/2020	**Hora de Termino:** 16h00 pm
Institución	MASTER TECHNOLOGY
Gerente	Jiménez Torres Richard Augusto
Ruc	17141587790001
Provincia	Pichincha
Dirección	San Gregorio Y Versalles Oe252
Teléfono	025126614/ 099-990-8072
Correo Electrónico	Gerencia@Mastertechnology.Com.Ec

INFORMACIÓN GENERAL

Misión

Somos una empresa enfocada en la innovación con sentido de responsabilidad con la sociedad ofertando servicios/ productos de calidad, de aparatos y equipos de comunicación incluido partes, piezas al por mayor y por menos ofreciendo a su vez servicios de consultoría a las pequeñas y medianas empresas, personas particulares tanto nacionales como extranjeras.

Visión

Ser una empresa reconocida por sus productos y servicios de calidad dentro del mercado nacional, adaptándonos día a día a las necesidades cambiantes de la sociedad y al avance tecnológico cumpliendo a cabalidad la expectativa de nuestros clientes mediante la satisfacción de sus necesidades en el ambiente tecnológico y de telecomunicación.

Valores

- ✓ Responsabilidad
- ✓ Respeto
- ✓ Confidencialidad
- ✓ Disciplina
- ✓ Solidaridad
- ✓ Trabajo en Equipo
- ✓ Compromiso
- ✓ Vocación
- ✓ Humildad
- ✓ Ética

EMPRESA MASTER TECHNOLOGY
VISITA PRELIMINAR
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

PA 1/1

DATOS EMPRESARIALES

Actividad Económica Principal

- Importación de productos Tecnológicos.

Actividad Económica Secundarias

- Prestación Personalizada de servicios informáticos.
- Consultoría y Asesoría Tributaria

Matriz: San Gregorio Y Versalles Oe252

Sucursales: Cristóbal Vaca Castro Y pedro de Mendoza
C.C Quicentro Sur, Av. Moran Valverde 1000
Av. Orellana E9-195 y Av. 6 de diciembre

Distribuidora de las Siguientes Marcas:

- Samsung
- Toshiba
- Hacer
- LG Life`s Good
- Hp
- Compac
- Sony
- Lexmark
- Lenovo
- Genius
- Intel
- Asus
- Epson
- Microsoft
- Acteck
- Cannon
- Targus
- San Disk
- APC Legendary Reliability
- NOC Eyes Value
- ViewSonic
- Linksys
- D-Link
- Kingston
- Western Digital
- Kensington

N.º de Empleados

Área	Número de empleados
Área comercial	18
Marketing	4
Área financiera	9
Área operativa	9
Servicio técnico	7
Total	47

Elaborado por: **D.J.U. R** **Fecha:** **29/07/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **29/07/2020**

EMPRESA MASTER TECHNOLOGY
CARTA DE PRESENTACIÓN
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

CP 1/1

Riobamba, 29 De Julio del 2020

Ingeniero.

JIMENEZ TORRES RICHARD AUGUSTO

GERENTE ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

Presente. –

Nos complace mencionarle nuestra propuesta de trabajo para la realización de la Auditoría Informática a la Empresa Master Technology, brindándole un servicio de calidad contando con los conocimientos necesarios para el trabajo de auditoria, nos comprometemos a demostrar trasparencia, puntualidad, responsabilidad, honestidad y ética por parte de la firma auditora, además se entregara un informe final donde se detallaran los problemas detectados con sus soluciones añadiendo conclusiones y recomendaciones que ayuden a la correcta toma de decisiones.

Nuestra firma auditora está conformada por profesionales altamente calificados con experiencia y conocimiento en el ámbito de la Auditoria Informática, dicha firma está representada por un supervisor el cual da certeza la calidad del trabajo a realizar.

A continuación, le ponemos a su consideración nuestra propuesta de trabajo, quedando a su total disposición. De manera anticipada agradecemos la atención prestada a la presente.

Atentamente,

Ing.: Willian Geovanny Yanza Chávez
JEFE DEL EQUIPO DE AUDITORÍA

Elaborado por:	**D.J.U. R**	**Fecha:**	**29/07/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**29/07/2020**

EMPRESA MASTER TECHNOLOGY
CARTA DE COMPROMISO
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

CC 1/1

Riobamba, 29 De Julio del 2020

Ingeniero.

JIMENEZ TORRES RICHARD AUGUSTO

GERENTE ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

Presente. –

Nuestro equipo de Auditoria "VALIDATE AUDITORÍA" nos comprometemos a la realización de la Auditoría Informática a la Empresa Master Technology, demostrando trasparencia, puntualidad, responsabilidad, honestidad y ética por parte de la firma auditora, además se entregará un informe final donde se detallarán los problemas detectados con sus soluciones añadiendo conclusiones y recomendaciones que ayuden a la correcta toma de decisiones.

Adicionalmente nos comprometemos a respetar los tiempos establecidos para la culminación del trabajo de auditoria en un plazo de 60 días laborables anteriormente mencionado informando los hallazgos presentados en cada fase de la auditoria.

De manera anticipada agradecemos la atención prestada a la presente.
Atentamente,

Ing. Willian Geovanny Yanza Chávez
JEFE DE EQUIPO

Dr. Carlos Volter Buenaño Pesantez
SUPERVISOR

Didima Johanna Ucles Romo
AUDITORA

Elaborado por: **D.J.U. R** **Fecha:** **30/07/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **30/07/2020**

MEMORANDÚM DE PLANIFICACIÓN

Riobamba, 29 De Julio del 2020

Institución	**MASTER TECHNOLOGY**
Gerente	Jiménez Torres Richard Augusto
Ruc	17141587790001
Provincia	Pichincha
Dirección	San Gregorio Y Versalles Oe252
Teléfono	025126614/ 099-990-8072
Correo Electrónico	Gerencia@Mastertechnology.Com.Ec

Motivo de la Auditoría

Se realizará una auditoría informática a la empresa Master Technology, cantón quito, provincia de pichincha, período 2019, para valorar la integridad, confidencialidad y disponibilidad de los recursos, equipos informáticos y su información mediante el uso de métodos, técnicas, estándares y herramientas de auditoria informática para la empresa.

Objetivos de la Auditoría

Objetivo General

Aplicar una auditoría informática a la empresa Master Technology, cantón quito, provincia de pichincha, período 2019, para valorar la integridad, confidencialidad y disponibilidad de los recursos, equipos informáticos y su información mediante el uso de métodos, técnicas, estándares y herramientas de auditoria informática para la empresa.

Objetivos Específicos

- Fundamentar y estructurar el marco teórico mediante la revisión bibliográfica de diferentes autores para sustentar el presente trabajo de titulación.
- Aplicar la metodología establecida en el proceso de la auditoria informática para la determinación u obtención de evidencias y posterior elaboración del informe.
- Presentar el informe final de auditoria, con las conclusiones y recomendaciones orientadas a mejorar el uso y gestión de la información con respecto a la integridad, disponibilidad y confidencialidad de los sistemas y recursos informáticos de la empre

Alcance de la Auditoría Informática

El período dentro del cual está comprendida la Auditoria Informática es del 01 de enero al 31 de diciembre del 2019.

Plazo

El plazo estimado para la aplicación de la Auditoría Informática es de 60 días laborables.

Recursos Humanos

La firma auditora Valídate Auditoria está conformada por:

- Ing. Willian Geovanny Yanza Chávez **Jefe de Equipo**
- Dr. Carlos Volter Buenaño Pesántez **Supervisor**
- Ing. Didima Johanna Ucles Romo **Auditora**

Metodología Del Trabajo

- Observación
- Entrevista al Técnico de la Unidad de Tecnologías de la Información y Comunicación.
- Cuestionarios de Control Interno COSO II

Atentamente,

Ing. Willian Geovanny Yanza Chávez
JEFE DE EQUIPO

Dr. Carlos Volter Buenaño Pesantez
SUPERVISOR

Didima Johanna Ucles Romo
AUDITORA

Elaborado por: **D.J.U. R** **Fecha:** **31/07/2020**

Revisado por: **W.G.Y.CH/C.V.B.P** **Fecha:** **31/07/2020**

EMPRESA MASTER TECHNOLOGY
NARRATIVA DE LA VISITA PRELIMINAR
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

NVP
1/1

Lugar: Empresa Master Technology

Fecha: 04/08/2020

Hora: 10h00 am

En la visita realizada a la empresa Master Technology en el Cantón Quito, Provincia de Pichincha el día martes 04 de agosto a las 10 de la mañana se pudo observar que la entidad cuenta con una matriz y 4 sucursales ubicadas en quito norte y sur, la entidad cuenta con 47 empleados laborando de manera dependiente e independiente a la empresa, los cuales se encuentran distribuidas en las distintas áreas correspondiente al área de marketing, área financiera, servicio técnico, y ventas.

Los diferentes tipos de productos que la entidad vende al por mayor y al por menor son importados en su mayoría de china y estados unidos, al momento de llevar un registro de inventario de entrada y salida de productos no se actualiza de manera regular por lo que presenta problemas cuando la empresa tiene pedidos al por mayor, ya que la persona encargada de la actualización de inventario es un trabajador independiente a la empresa.

La empresa tiene unos horarios de labores de lunes a viernes de 09h00 am a 07h00 pm mientras que los sábados es de 10h00 a 15h00 y Enel caso de los domingos se atiende a la ciudadanía previo aviso de la necesidad ya sea de servicio técnico, asesoría, o adquisición de productos, el gerente administrativo es quien se encarga de supervisar personalmente las actividades laborales que se realizan los fines de semana

Observando minuciosamente la infraestructura, la división de las áreas, los recursos informáticos con los que cuenta cada unidad su ubicación y mala distribución, conjuntamente los problemas de seguridad física y lógica que la entidad presenta, fue evidente que nunca se ha realizado una Auditoría Informática.

Al revisar primero la matriz se pudo evidenciar que su visión y misión se encuentran claramente definidas, expuestas y socializadas al personal que labora en ese sitio, pero respecto a las sucursales el personal no tiene conocimiento ni se encuentra expuesta, como punto importante las sucursales presentan el mismo problema respecto a la falta de los recursos informáticos provocada por la mala distribución de los mismos.

Elaborado por:	**D.J.U. R**	**Fecha:**	**31/07/2020**
Revisado por:	**W.G.Y.CH/C.V.B.P**	**Fecha:**	**31/07/2020**

EMPRESA MASTER TECHNOLOGY
ENTREVISTA AL TÉCNICO
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

ET 1/1

Entrevistado: Ing. Alex Napoleón Espinoza Sánchez

¿Considera usted que los recursos designados al departamento son suficientes para el desempeño laboral?

No, porque al estar renovando e innovando a la empresa se requiere equipos y programas que en su gran mayoría tiene un valor económico elevado.

¿Por parte de su departamento han existido iniciativas para la mejora continua de los recursos informáticos?

Si existen iniciativas dirigidas el gerente de la empresa, pero no se ha obtenido respuestas ni negativas ni positivas.

¿Los puestos de trabajo existentes en la unidad cumplen con los requerimientos necesarios para cumplir a cabalidad con el trabajo a realizar?

No necesariamente en mi caso cumplo con el perfil, pero mi auxiliar no, ya que los conocimientos que el tiene es de lo que yo le voy enseñando en el lugar de trabajo.

¿Como calificaría su nivel de satisfacción (malo, bueno, regular) con las herramientas informáticas de las que dispone?

Regular, a pesar de las herramientas proporcionadas a veces es necesario traer herramientas de uno mismo para poder desempeñarse bien.

¿Como evaluaría usted la prevención y solución de posibles problemas que podrían presentar los equipos informáticos?

Bueno, aunque algunas ocasiones es necesaria la inversión económica para poder prevenir o solucionar los problemas que presentan los equipos informáticos por cuestión de optimizar el tiempo y realizar el trabajo más rápidamente.

¿Desde su punto de vista que nivel de conciencia considera usted que tiene el personal de la empresa con respecto al bueno manejo de los equipos informáticos?

Es bajo ya que muchos empleados no toman en cuenta que son equipos delicados que pueden averiarse con relativa facilidad.

Elaborado por:	**D.J.U. R**	**Fecha:**	**07/08/2020**
Revisado por:	**W.G.Y.CH/C.V.B.P**	**Fecha:**	**07/08/2020**

EMPRESA MASTER TECHNOLOGY
SOLICITUD DE REQUERIMIENTO
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

ET 1/1

Riobamba, 07 De agosto del 2020

Ingeniero.

JIMENEZ TORRES RICHARD AUGUSTO

GERENTE ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

Presente. –

La firma auditora "VALIDATE AUDITORÍA", al dar inicio al trabajo de auditoria nos acercamos a usted por este medio para la petición de la estructura organizacional de la empresa Master Technology tras no haber sido posible visualizarlo en su página web, matriz o sucursales por lo que decidimos realizar la presente para que nos pueda entregar dicha información necesaria para el avance del trabajo de auditoria. Cabe recalcar que la información solicitada será tratada exclusivamente para fines de ejecución del trabajo.

De antemano le agradecemos por la atención prestada a la presente.

Atentamente,

Ing. Willian Geovanny Yanza Chávez
JEFE DE EQUIPO

Dr. Carlos Volter Buenaño Pesantez
SUPERVISOR

Didima Johanna Ucles Romo
AUDITORA

Elaborado por: **D.J.U. R** **Fecha:** **07/08/2020**

Revisado por: **W.G.Y.CH/C.V.B.P** **Fecha:** **07/08/2020**

Centro Comercial Quitus Local 351-352 San Gregorio s/n y Versalles
Teléfonos: 512 6614/ 512 6615/ 0999 908 072 / 0999 630 070
Información: ventas@solve361.com E-mail gerencia@mastertechnology.com.ec
Quito-Ecuador

Riobamba, 08 de agosto del 2020.

Ingeniero

Willian Geovanny Yanza Chávez

DIRECTOR DEL PROYECTO DE INVESTIGACIÓN

De mi Consideración:

Reciba un cordial saludo a nombre de MASTER TECHNOLOGY, por medio de esta presente me permito informar de acuerdo a la petición de la entrega del documento donde se plasme la estructura organizacional, la entidad no cuenta con esta información por lo que no se ha establecido una estructura desde la creación de la empresa hasta la actualidad.

Atentamente,

JIMENEZ TORRES RICHARD AUGUSTO

GERENTE ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

EMPRESA MASTER TECHNOLOGY
DETERMINACIÓN DE ÁREAS CRÍTICAS
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

DAC
1/1

Institución	**MASTER TECHNOLOGY**
Gerente	Jiménez Torres Richard Augusto
Ruc	17141587790001
Provincia	Pichincha
Dirección	San Gregorio Y Versalles Oe252
Teléfono	025126614/ 099-990-8072
Correo Electrónico	Gerencia@Mastertechnology.Com.Ec

Prioridad	**Área o Actividad Crítica**	**Razones**
1	Área Administrativa	Ausencia de gestión de estrategias para mejorar el área informática de la empresa.
2	Área Informática	Falta de estrategias y protocolos para el control de la seguridad informática de la empresa.
3	Área Financiera	No existe una conciencia de manejo adecuado de los equipos informáticos. Existe insuficiencia de equipos por la mala distribución existente en la empresa para cada una de las áreas. Ausencia de perfiles de usuario específicos.
4	Área Comercial	Inexistencia de responsables por el uso de los equipos informáticos. El software utilizado es insuficiente para la protección de los equipos ocasionando procesos lentos y riesgo constante de virus. Equipos Deteriorado ocupando espacios físicos.
5	Área Técnica	Insuficiencia de Fondos para la adquisición de herramientas informáticas. Los perfiles de puestos no cumplen con los requerimientos para el puesto de trabajo.

Elaborado por: **D.J.U. R** **Fecha:** **07/08/2020**

Revisado por: **W.G.Y.CH/C.V.B.P** **Fecha:** **07/08/2020**

FASE II: EJECUCIÓN

3.2.3.2. FASE II: EJECUCICIÓN

N.º	PROCEDIMIENTO	REFERENCIA	ELABORADO POR	FECHA
1	Programa de auditoria.	PA 1/1	D.J.U. R	08/08/2020
2	Análisis Situacional FODA	AS 1/1	D.J.U. R	09/08/2020
3	Matriz de Correlación FO	MCFO 1/1	D.J.U. R	10/08/2020
4	Matriz de Correlación DA	MCDA 1/1	D.J.U. R	10/08/2020
6	Perfil Estratégico Interno	PEI 1/1	D.J.U. R	11/08/2020
7	Perfil Estratégico Externo	PEE 1/1	D.J.U. R	11/08/2020
8	Cuestionario de Control Interno COSO II	CCI 1/1	D.J.U. R	12/08/2020
9	Matriz Resumen de los Cuestionarios de Control Interno COSO II	MRCCI	D.J.U. R	13/08/2020
10	Hoja de Hallazgos	HH1/1	D.J.U. R	14/08/2020
9	Hoja de Indicadores	HI 1/1	D.J.U. R	07/08/2020

Elaborado por: **D.J.U. R** **Fecha:** **08/08/2020**

Revisado por: **W.G.Y.CH/C.V.B.P** **Fecha:** **08/08/2020**

EMPRESA MASTER TECHNOLOGY
ANÁLISIS SITUACIONAL
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

AS 1/1

ANÁLISIS INTERNO

	FORTALEZAS		DEBILIDADES
F1	Alta demanda de productos	D1	Saturación del sistema de mensajería en línea
F2	Capacidad de adaptación	D2	Deficiente asignación de recursos
F3	Excelente trabajo en equipo	D3	Equipamiento tecnológico desactualizado
F4	Variedad de productos, costos y marcas	D4	Personal con deficiente capacitación informática
F5	Conocimientos de los equipos informáticos disponibles	D5	Insuficiencia en presupuesto asignado a seguridad de redes
F6	Ubicación Geográfica	D6	Deficiencia de Personal
F7		D7	Ataques Informáticos
		D8	Ausencia de prevención en caso de pérdidas de información
		D9	

ANÁLISIS EXTERNO

	OPORTUNIDADES		AMENAZAS
O1	Crecimiento constante de la empresa	A1	Hurto de publicidad
O2	Contactos directos con distribuidores internacionales.	A2	Ingresos de nuevos competidores
O3	Productos Garantizados Internacionalmente	A3	Competencia Desleal
O4		A4	Eventos catastróficos
O5		A5	Gran dependencia de proveedores internacionales
O6		A6	Pandemia

Elaborado por: **D.J.U. R** **Fecha:** **09/08/2020**

Revisado por: **W.G.Y.CH/C.V.B.P** **Fecha:** **09/08/2020**

EMPRESA MASTER TECHNOLOGY
MATRIZ DE CORRELACIÓN FO
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

MCFO 1/1

	FO	O1 Crecimiento constante de la empresa	O2 Contactos directos con distribuidores internacionales.	O3 Productos Garantizados Internacionalmente	TOTAL	
F1	Alta demanda de productos	5	5	5	**15**	**21%**
F2	Capacidad de adaptación	5	3	1	**9**	**13%**
F3	Excelente trabajo en equipo	5	3	1	**9**	**13%**
F4	Variedad de productos, costos y marcas	5	5	5	**15**	**21%**
F5	Conocimientos de los equipos informáticos disponibles	5	5	5	**15**	**21%**
F6	Ubicación Geográfica	5	1	1	**7**	**11%**
	TOTAL	**30** **43%**	**22** **31%**	**18** **26%**	**70**	**100%**

Forma de Ponderación:

- Si tienen una relación directa se le valorará con = 5
- Si tienen una relación indirecta se le valorará con = 3
- Si no tiene ningún tipo de relación su valor será = 1

Análisis: Se demuestra un porcentaje del 21% en fortaleza debido a su alta demanda de productos, a la variación de sus costos y de marcas, además de tener un adecuado conocimiento de los equipos informáticos con los que cuenta la empresa. Mientras tanto con un porcentaje del 43% se refleja en el crecimiento de la empresa dentro del mercado convirtiéndose de esta manera la empresa Master Technology mediante sus productos logra un desarrollo óptimo.

Elaborado por: **D.J.U. R** **Fecha:** **10/08/2020**

Revisado por: **W.G.Y.CH/C.V.B.P** **Fecha:** **10/08/2020**

EMPRESA MASTER TECHNOLOGY
MATRIZ DE CORRELACIÓN DA
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

MCDA 1/1

		A1	A2	A3	A4	A5	A6		
	DA	Hurto de publicidad	Nuevos competidores	Competencia Desleal	Eventos catastróficos	Dependencia de proveedores	Pandemia	**TOTAL**	
D1	Saturación del sistema de mensajería en línea	1	1	1	1	1	5	**10**	**13%**
D2	Deficiente asignación de recursos	1	3	1	3	1	3	**12**	**16%**
D3	Equipamiento tecnológico desactualizado	1	1	1	1	1	1	**6**	**8%**
D4	Personal con deficiente capacitación informática	1	3	1	3	1	3	**12**	**16%**
D5	Insuficiencia en presupuesto asignado a seguridad de redes	1	1	1	3	1	3	**10**	**13%**
D6	Deficiencia de Personal	1	1	1	1	1	3	**8**	**11%**
D7	Ataques Informáticos	1	1	1	3	1	3	**10**	**13%**
D8	Ausencia de prevención en caso de pérdidas de información	1	1	1	3	1	1	**8**	**10%**
	TOTAL	**8**	**12**	**8**	**18**	**8**	**22**	**76**	
		10%	**16%**	**10%**	**24%**	**10%**	**30%**		**100 %**

Forma de Ponderación:

- Si tienen una relación directa se le valorará con = 5
- Si tienen una relación indirecta se le valorará con = 3
- Si no tiene ningún tipo de relación su valor será = 1

Análisis: Se demuestra un porcentaje del 16% en Debilidades respectos a la deficiencia de asignación de recursos y a la deficiente capacitación en el área de informática al personal de la empresa mientras que la amenaza más alta es de 30% correspondiente a la situación actual debido a la pandemia ocasionada por covid 19.

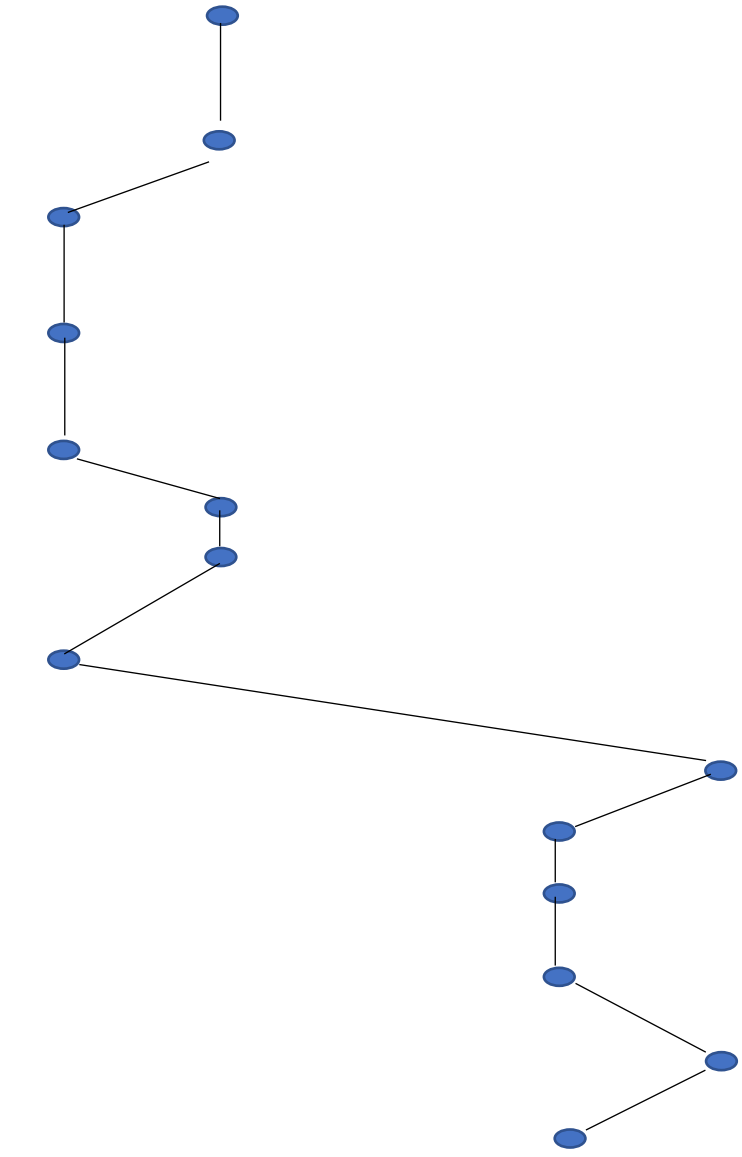
Elaborado por: **D.J.U. R** **Fecha:** **10/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **10/08/2020**

EMPRESA MASTER TECHNOLOGY
PERFIL ESTRATÉGICO INTERNO
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

PEI 1/1

	ASPECTOS INTERNOS	CLASIFICACIÓN DE IMPACTO				
		DEBILIDAD			FORTALEZA	
		Gran Debilidad	Debilidad	EQUILIBRIO	Fortaleza	Gran Fortaleza
	DEBILIDADES					
D1	Saturación del sistema de mensajería en línea					
D2	Deficiente asignación de recursos					
D3	Equipamiento tecnológico desactualizado					
D4	Personal con deficiente capacitación informática					
D5	Insuficiencia en presupuesto asignado a seguridad de redes					
D6	Deficiencia de Personal					
D7	Ataques Informáticos					
D8	Ausencia de prevención en caso de pérdidas de información					
	FORTALEZAS					
F1	Alta demanda de productos					
F2	Capacidad de adaptación					
F3	Excelente trabajo en equipo					
F4	Variedad de productos, costos y marcas					
F5	Conocimientos de los equipos informáticos disponibles					
F6	Ubicación Geográfica					
	TOTAL	**4**	**4**		**4**	**2**
	PORCENTAJE	**50%**	**50%**		**67%**	**33%**



Elaborado por: **D.J.U. R** **Fecha:** **11/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **11/08/2020**

EMPRESA MASTER TECHNOLOGY
PERFIL ESTRATÉGICO EXTERNO
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

PEE 1/1

CLASIFICACIÓN DE IMPACTO

ASPECTOS INTERNOS		**AMENAZAS**			**OPORTUNIDAD**	
		Gran Amenaza	Amenaza	EQUILIBRIO	Oportunidad	Gran Oportunidad
	AMENAZAS					
A1	Hurto de publicidad					
A2	Ingresos de nuevos competidores					
A3	Competencia Desleal					
A4	Eventos catastróficos					
A5	Gran dependencia de proveedores internacionales					
A6	Pandemia					
	OPORTUNIDAD					
O1	Crecimiento constante de la empresa					
O2	Contactos directos con distribuidores internacionales.					
O3	Productos Garantizados Internacionalmente					
	TOTAL	**3**	**3**		**0**	**3**
	PORCENTAJE	**50%**	**50%**		**0%**	**100%**

Elaborado por: **D.J.U. R** **Fecha:** **11/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **11/08/2020**

EMPRESA MASTER TECHNOLOGY
CUESTIONARIO DE CONTROL INTERNO COSO II
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

CCIAC 1/2

COMPONENTE I: AMBIENTE DE CONTROL

N.º	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿Existe un reglamento o normativa definida para el manejo de los recursos informáticos de la empresa?		X		
2	¿En la estructura orgánica de la empresa se encuentran definidas los niveles de apoyo y asesoría que brinda la Unidad de Tecnología de Información y Comunicación?		X		
3	¿La empresa cuenta con planes de desarrollo informáticos?		X		
4	¿Se conocen y se aplican las normas establecidos por parte de la Unidad de Tecnología de Información y Comunicación para el manejo de los recursos informáticos?		X		
5	¿Se encuentran claramente definidos las funciones y responsabilidades del personal de la Unidad de Tecnología de Información y Comunicación?		X		
6	¿El personal que labora en la Unidad de Tecnologías de Información y Comunicación cumple con los perfiles para el puesto de trabajo?		X		
7	¿La entidad Cuenta con planes de capacitación para la Unidad de Tecnología de Información y Comunicación?		X		
8	¿La Unidad de Tecnología de Información y Comunicación Cuenta con un manual de políticas para la gestión?		X		
9	¿Existe un manual de procesos y procedimientos que se encuentren debidamente actualizados?		X		
	TOTAL	**0**	**9**	**0**	

Elaborado por: **D.J.U. R** **Fecha:** **12/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **12/08/2020**

NIVEL DE CONFIANZA		
Alto	**Moderado**	**Bajo**
95% - 76%	*75% - 51%*	*50% - 15%*
5% - 24%	*25% - 49%*	*50% - 85%*
Bajo	**Moderado**	**Alto**
NIVEL DE RIESGO		

Nivel de Confianza (NC) $= \frac{Respuestas\ Positivas}{PTRespuestas\ Negativas} * 100\%$

Nivel de Confianza (NC) $= \frac{0}{9} * 100\%$

$= 0{,}0$

$=$ **0%**

Nivel de Riesgo (NR)= 100% - Nivel de Confianza (NC)

= 100% - 0%

= **100%**

ANÁLISIS:

El primer componente correspondiente al COSO II el Ambiente de Control arrojo como resultado que el nivel de confianza es de 0% tras 0 respuestas positivas de 9 preguntas realizadas; mientras que el nivel de riesgo siendo de 100 % tras 9 respuestas negativas se lo considera alto, con un impacto altamente significativo que perjudica a la empresa en su totalidad.

Elaborado por: **D.J.U. R** **Fecha:** **12/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **12/08/2020**

COMPONENTE II: ESTABLECIMIENTO DE OBJETIVOS

N.º	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿Los recursos informáticos solventan a cabalidad las necesidades de la empresa?		X		
2	¿Existe procedimientos a seguir para la resolución de problemas con los equipos informáticos de cada área?		X		
3	¿La información correspondiente a las labores de la empresa proporcionada a las áreas de trabajo esta verificada?	X			
4	¿El daño o perdida de un equipo informático representa retrasos significativos en las actividades laborales?	X			.
5	¿Cuentan con estrategias establecidas para la mejora continua de los recursos informáticos?		X		❖ No se ha contemplado una estructura adecuada.
	TOTAL	**2**	**3**	**0**	

NIVEL DE CONFIANZA		
Alto	**Moderado**	**Bajo**
95% - 76%	*75% - 51%*	*50% - 15%*
5% - 24%	*25% - 49%*	*50% - 85%*
Bajo	**Moderado**	**Alto**
NIVEL DE RIESGO		

Nivel de Confianza (NC) $= \frac{Respuestas\ Positivas}{PTRespuestas\ Negativas} * 100\%$

Nivel de Confianza (NC) $= \frac{2}{5} * 100\% = 0{,}4 =$ **40%**

Nivel de Riesgo (NR)= 100% - Nivel de Confianza (NC)

= 100% - 40% = **60%**

ANÁLISIS:

El 2do componente correspondiente al COSO II el establecimiento de objetivos arrojo como resultado que tanto el nivel de confianza es de 40% considerado un nivel bajo, mientras que el nivel de riesgo es de 60% considerado un nivel alto y con un impacto negativo altamente significativo.

Elaborado por: **D.J.U. R** **Fecha:** **12/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **12/08/2020**

COMPONENTE III: IDENTIFICACIÓN DE ACONTECIMIENTOS

N.º	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿El espacio físico donde se encuentran los equipos informáticos cuenta con las seguridades necesarias?		X		❖ Solo en determinadas áreas.
2	¿Existe un responsable del mantenimiento adecuado de los equipos informáticos?		X		❖ El problema es resuelto por la persona encargada del equipo.
3	¿Cuentan con un inventario de los recursos informáticos de su matriz y sucursales?		X		❖ Solo de los productos destinados a la venta.
4	¿Cuentan con señalética en las áreas donde se encuentran los recursos informáticos?		X		❖ El lugar pasa cerrado bajo llave.
5	¿El acceso a los perfiles de usuario cuentan con claves de ingreso al sistema?	X			
6	¿El ingreso al sistema cuenta con tiempo límite para su utilización?	X			
	TOTAL	**2**	**4**	**0**	

NIVEL DE CONFIANZA		
Alto	**Moderado**	**Bajo**
95% - 76%	*75% - 51%*	*50% - 15%*
5% - 24%	*25% - 49%*	*50% - 85%*
Bajo	**Moderado**	**Alto**
NIVEL DE RIESGO		

Nivel de Confianza (NC) $= \frac{Respuestas\ Positivas}{PTRespuestas\ Negativas} * 100\%$

Nivel de Confianza (NC) $= \frac{2}{6} * 100\% = 0{,}333 =$ **33%**

Nivel de Riesgo (NR)= 100% - Nivel de Confianza (NC)

= 100% - 33% = **67%**

ANÁLISIS:

El 3er componente correspondiente al COSO II identificación de acontecimientos arrojo como resultado que el nivel de confianza es de 33% considerado como bajo lo que representa un riesgo para la empresa considerando que el nivel de riesgo es de 67% por lo que significaría un riesgo muy alto y su impacto viene hacer significativo a largo plazo.

Elaborado por: **D.J.U. R** **Fecha:** **12/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **12/08/2020**

COMPONENTE IV: EVALUACIÓN DEL RIESGO

N.º	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿El gerente administrativo cuenta con un plan de contingencia en caso de que los equipos informáticos estén en riesgo?		X		❖ El problema se resuelve en el momento en que se presenta.
2	¿La empresa cuenta con respaldos de información de los equipos informáticos?		X		❖ No se ha considerado la opción de respaldar
3	¿El personal de la empresa identifican los posibles riesgos que pueden ocasionar el desconocimiento de la seguridad física?	X			
4	¿Los integrantes de la empresa saben cómo actuar en caso de presentarse una situación de riesgo que comprometa los recursos informáticos?		X		❖ No se a presentado la situación que ponga a prueba su habilidad.
	TOTAL	**1**	**3**	**0**	

NIVEL DE CONFIANZA		
Alto	**Moderado**	**Bajo**
95% - 76%	*75% - 51%*	*50% - 15%*
5% - 24%	*25% - 49%*	*50% - 85%*
Bajo	**Moderado**	**Alto**
NIVEL DE RIESGO		

Nivel de Confianza (NC) $= \frac{Respuestas\ Positivas}{PTRespuestas\ Negativas} * 100\%$

Nivel de Confianza (NC) $= \frac{1}{4} * 100\% = 0{,}25 =$ **25%**

Nivel de Riesgo (NR)= 100% - Nivel de Confianza (NC)

= 100% - 25% = **75%**

ANÁLISIS:

El 4to componente correspondiente al COSO II evaluación del riesgo arrojo como resultado que el nivel de confianza es de apenas 25 % considerándose un nivel bajo tras 1 respuesta positiva de 4 preguntas realizadas; considerado dentro del nivel bajo; mientras que el nivel de riesgo siendo de 75 % tras 3 respuestas negativas se lo considera alto. Por lo tanto, el impacto que tiene la entidad es significativa por el nivel de riesgo alto lo que conllevaría problemas en cualquier momento de dar solución inmediata.

Elaborado por: **D.J.U. R** **Fecha:** **12/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **12/08/2020**

EMPRESA MASTER TECHNOLOGY
CUESTIONARIO DE CONTROL INTERNO COSO II
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

CCIRR 1/1

COMPONENTE V: RESPUESTA AL RIESGO

N.º	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿El gerente administrativo tiene conocimientos para actuar ante posibles riesgos de perdida de información?	X			
2	¿En caso de no tener conocimiento de algún tema de seguridad física y lógica se asesoran con un especialista en el área?	X			
3	¿Existen medidas preventivas cuando se detecta a tiempo un peligro que involucre los equipos informáticos?	X			
4	¿Se a socializado las medidas a todo el personal para conocimiento del mismo?	X			
	TOTAL	**4**	**0**	**0**	

NIVEL DE CONFIANZA		
Alto	**Moderado**	**Bajo**
95% - 76%	*75% - 51%*	*50% - 15%*
5% - 24%	*25% - 49%*	*50% - 85%*
Bajo	**Moderado**	**Alto**
NIVEL DE RIESGO		

Nivel de Confianza (NC) $= \frac{Respuestas\ Positivas}{PTRespuestas\ Negativas} * 100\%$

Nivel de Confianza (NC) $= \frac{4}{4} * 100\% = 1 =$ **100%**

Nivel de Riesgo (NR)= 100% - Nivel de Confianza (NC)

= 100% - 100% = **0%**

ANÁLISIS:

El 5to componente correspondiente al COSO II respuesta al riesgo arrojo como resultado que el nivel de confianza es 100% considerándose un nivel alto, es decir, satisfactorio tras haber dado positivo todas las preguntas realizas por lo que no existe respuestas negativas.

Elaborado por: **D.J.U. R** **Fecha:** **12/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **12/08/2020**

EMPRESA MASTER TECHNOLOGY
CUESTIONARIO DE CONTROL INTERNO COSO II
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

CCIAC 1/4

COMPONENTE VI: ACTIVIDADES DE CONTROL

N.º	PREGUNTA	SI	NO	N/A	OBSERVACIONES
	Seguridad Física				
1	¿El acceso al centro de datos cuenta con restricción para personal que no esté autorizado?		X		❖ El personal interno de la empresa accede de forma normal al área sin autorización
2	¿Los equipos informáticos cuenta con una adecuada estructura de red para comunicarse?		X		❖ Cuenta con una red establecida y funcional pero no se ha hecho mejorar para una buena comunicación.
3	¿La empresa cuenta con el equipo de vigilancia necesaria para salvaguardar la seguridad de los recursos informáticos?		X		❖ Solo existen cámaras de seguridad en las salidas y entradas de la empresa.
4	¿Se mantiene un control de actividades de cada usuario de los distintos equipos informáticos?		X		❖ Porque no existe perfiles de usuario específicos.
5	¿Los equipos informáticos cuentan con pólizas de seguros como respaldo?		X		❖ No se asignaron fondos para pólizas de equipos.
6	¿El centro de datos se encuentra correctamente ventilado es decir cuenta con regulación de temperatura?	X			
7	¿El cableado eléctrico de la estructura cuenta con conexión a tierra?	X			
8	¿Existe planos de la red de conexión de los equipos informáticos?		X		❖ La red no cumple con estándares de documentación.
9	¿La empresa cuenta con equipos UPS (fuente de poder ininterrumpida)?		X		❖ No se le da la debida importancia
10	¿La empresa cuenta con racks (estructura metálica donde se coloca los equipos informáticos)?	X			
11	¿Existen políticas de adquisición de equipos informáticos?	X			
12	¿La entidad cuenta con protocolos de manejo de equipos obsoletos?		X		❖ Los equipos son desechados.
	TOTAL	**4**	**8**	**0**	

Elaborado por: **D.J.U. R** **Fecha:** **12/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **12/08/2020**

N.º	PREGUNTA	SI	NO	N/A	OBSERVACIONES
	Seguridad Lógica				
13	¿La entidad realiza respaldos de información?		X		❖ La empresa no tiene como habito respaldar información.
14	¿La empresa cuenta con un software especializado para la protección de su sistema?	X			❖ Software gratuito
15	¿El software con el que cuenta la empresa protege la información contra todo tipo de ataque informático?		X		❖ El software gratuito no cuenta con todas las seguridades.
16	¿La organización cuenta con políticas que establece la creación de contraseñas seguras para el acceso al sistema informático?		X		❖ La entidad está incursionando en el manejo adecuado de la seguridad de la información
17	¿La empresa cuenta con servicios Cloud en los cuales pueda almacenar información de forma segura?		X		❖ Se está iniciando la implementación de este servicio
18	¿La empresa cuenta con una red privada o intranet para el manejo de la información?	X			
19	¿Las políticas de seguridad lógica de la empresa incluyen procesos de control de acceso lógico?	X			
	TOTAL	**7**	**12**	**0**	

Elaborado por: D.J.U. R **Fecha:** 12/08/2020

Revisado por: W.G.Y.CH/C.V. BP **Fecha:** 12/08/2020

NIVEL DE CONFIANZA		
Alto	**Moderado**	**Bajo**
95% - 76%	*75% - 51%*	*50% - 15%*
5% - 24%	*25% - 49%*	*50% - 85%*
Bajo	**Moderado**	**Alto**
NIVEL DE RIESGO		

Nivel de Confianza (NC) $= \frac{Respuestas\ Positivas}{PTRespuestas\ Negativas} * 100\%$

Nivel de Confianza (NC) $= \frac{7}{19} * 100\% = 0{,}3684 =$ **37%**

Nivel de Riesgo (NR)= 100% - Nivel de Confianza (NC)

= 100% - 37% = **63%**

ANÁLISIS:

El sexto componente correspondiente al COSO II Actividades de Control relacionadas a seguridad física y lógica arrojo como resultado que el nivel de confianza es de 37% tras 7 respuestas positivas de 19 preguntas realizadas; considerado dentro del nivel bajo por estar ubicado en el rango de 50% - 15%; mientras que el nivel de riesgo siendo de 63 % tras 12 respuestas negativas se lo considera alto por estar en el rango de 50% - 85%. Por lo tanto, el impacto que tiene la entidad es significativa lo cual puede ocasionar problemas en cualquier momento si no se da una solución inmediata a los problemas encontrados.

Elaborado por: **D.J.U. R** **Fecha:** **12/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **12/08/2020**

EMPRESA MASTER TECHNOLOGY
CUESTIONARIO DE CONTROL INTERNO COSO II
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

CCIAC 4/4

COMPONENTE VII: INFORMACIÓN Y COMUNICACIÓN

N.º	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿El gerente administrativo comunica oportunamente al personal información relacionada con la entidad?	X			
2	¿Se comunica al personal el procedimiento a seguir en caso de que la seguridad de la información sea vulnerada?	X			
3	¿Los sistemas informáticos garantizan la integridad y confiabilidad de la información?		X		❖ Las redes no han sido actualizadas en varios años.
4	¿Se tienen establecidos canales de comunicación dentro de la empresa?	X			
5	¿La comunicación interna permite interactuar entre las distintas unidades administrativas de la empresa y el departamento de tecnología para la asesoría técnica oportuna?		X		
6	¿Los sistemas informáticos garantizan la disponibilidad, accesibilidad y oportunidad de la información?	X			
	TOTAL	**4**	**2**	**0**	

NIVEL DE CONFIANZA		
Alto	**Moderado**	**Bajo**
95% - 76%	*75% - 51%*	*50% - 15%*
5% - 24%	*25% - 49%*	*50% - 85%*
Bajo	**Moderado**	**Alto**
NIVEL DE RIESGO		

Nivel de Confianza (NC) $= \frac{Respuestas\ Positivas}{PTRespuestas\ Negativas} * 100\%$

Nivel de Confianza (NC) $= \frac{4}{6} * 100\% = 0{,}6666 =$ **67%**

Nivel de Riesgo (NR)= 100% - Nivel de Confianza (NC)

= 100% - 67% = **33%**

ANÁLISIS:

El 7mo componente correspondiente al COSO II Información y Comunicación arrojo como resultado que el nivel de confianza es de 67% considerado como moderado, mientras que el nivel de riesgo es de 33% por lo que representa un riesgo moderado y representa un impacto poco significativo para la empresa.

Elaborado por: **D.J.U. R** **Fecha:** **12/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **12/08/2020**

COMPONENTE VIII: SUPERVISIÓN

N.º	PREGUNTA	SI	NO	N/A	OBSERVACIONES
1	¿Se cuenta con un cronograma de inspección para verificar la integridad de las bases de datos de los sistemas informáticos?		X		
2	¿Se realizan informes para mantener registros de los estados de los equipos informáticos?	X			
3	¿Los usuarios de los equipos informáticos de la empresa son definidos como responsables directos del estado de los mismos?		X		❖ No existe perfiles de usuario específicos.
4	¿Se controla el buen funcionamiento de los puntos de red y de las instalaciones eléctricas?	X			
5	¿Existe personal designado para supervisar las actividades realizadas por los miembros de cada unidad de la empresa?	X			
	TOTAL	**3**	**2**	**0**	

NIVEL DE CONFIANZA		
Alto	**Moderado**	**Bajo**
95% - 76%	*75% - 51%*	*50% - 15%*
5% - 24%	*25% - 49%*	*50% - 85%*
Bajo	**Moderado**	**Alto**
NIVEL DE RIESGO		

Nivel de Confianza (NC) $= \frac{Respuestas\ Positivas}{PTRespuestas\ Negativas} * 100\%$

Nivel de Confianza (NC) $= \frac{3}{5} * 100\% = 0{,}6 =$ **60%**

Nivel de Riesgo (NR)= 100% - Nivel de Confianza (NC)

= 100% - 60% = **40%**

ANÁLISIS:

El 8Vo componente correspondiente al COSO II Supervisión arrojo como resultado que el nivel de confianza es de 60% considerado como moderado, mientras que el nivel de riesgo es de 40% por lo que representa un riesgo moderado y representa un impacto parcial para la empresa

Elaborado por: **D.J.U. R** **Fecha:** **12/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **12/08/2020**

EMPRESA MASTER TECHNOLOGY
MATRIZ RESUMEN CUESTIONARIO DE CONTROL INTERNO COSO II
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

MRCCI
1/1

MATRIZ RESUMEN DE LOS CUESTIONARIOS DE CONTROL INTERNO COSO II

N.º	Componente	Referencia. Pt	% De Confianza	Nivel De Confianza	% De Riesgo	Nivel De Riesgo
1	Ambiente Interno	CCAI	0%	Nulo	100%	Alto
2	Establecimiento de Objetivos	CCIEO	40%	Bajo	60%	Moderado
3	Identificación de Acontecimientos	CCIIA	33%	Bajo	67%	Alto
4	Evaluación de Riesgo	CCIER	25%	Bajo	75%	Alto
5	Respuesta al Riesgo	CCIRR	100%	Alto	0%	Nulo
6	Actividades de control	CCIAC	37%	Bajo	63%	Alto
7	Información y Comunicación	CCIIC	67%	Moderado	33%	Moderado
8	Supervisión	CCIS	60%	Moderado	40%	Moderado
	TOTAL		**362**	**Moderado**	**438**	
	PROMEDIO		**45,25%**	**BAJO**	**54,75%**	**MODERADO**

ANÁLISIS:

Al enfocarnos en el promedio se puede observar que el nivel de confianza es de 45,25 % considerado un nivel bajo, mientras que el nivel de riesgo que se encuentra dentro del rango moderado es de 54,75%. Por lo tanto, el único componente que muestra un nivel 100% satisfactorio es la respuesta al riesgo por lo que en el resto de componentes deberán ser prestadas atención ya que 2 tienen un nivel moderado de 67% en Información y Comunicación, 60% en Supervisión y 4 muestran un nivel bajo, afectando significativamente a las actividades de la empresa.

Elaborado por: **D.J.U. R** **Fecha:** **13/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **13/08/2020**

CONDICIÓN

La entidad no cuenta con un reglamento o normativa definida para el manejo de los recursos informáticos de la empresa.

CRITERIO

Según la norma 410-04 de la Contraloría General del Estado donde se menciona las políticas y procedimientos en la cual nos dice que el gerente de una empresa aprobara políticas y procedimientos donde se puedan definir claramente los procedimientos a seguir para la regulación y control de actividades. Por lo tanto, la entidad deberá contar con un documento de respaldo donde se plasme el reglamento o normativa aprobado y difundido por gerencia que la entidad necesita para el buen manejo de los recursos informáticos

CAUSA

La entidad no ha considerado la necesidad de la creación de reglamentos para el manejo de los recursos informáticos.

EFECTO

El personal de la empresa no tiene un respaldo donde se indique el manejo de los recursos informáticos por lo que dicho manejo lo realizan a su criterio

CONCLUSIÓN

La empresa al no contar con un reglamento o normativa afecta a la estabilidad tanto de la misma como la de su personal al permitir que se tengan dudas respecto al manejo debido de los recursos informáticos ocasionando problemas a corto, mediano y largo plazo, existiendo la incertidumbre del impacto que tendrá la ausencia de dicho reglamento para la entidad.

RECOMENDACIÓN

Se debe contar con un reglamento o normativa donde se describa de manera clara y concreta como se deben manejar los recursos informáticos de la empresa para que el personal tenga un documento de respaldo en el cual puedan despejar sus dudas sobre el manejo, lo que se les permite hacer y lo que no pueden hacer sin necesidad de recurrir a preguntar a un trabajador, jefe o gerente, incluso evitando recordar lo que podían o no hacer, así la entidad tendrá donde basarse evitando problemas innecesarios.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

No se encuentran definidos los niveles de apoyo ni de asesoría que brinda la Unidad de Tecnología de información y Comunicación.

CRITERIO

Según la norma 410-01 de a Contraloría General del Estado donde nos menciona acerca de la Organización Informática nos dique que la Unidad de Tecnología de la información deberá constar en la estructura organizacional, tener definidos los niveles de apoyo como de asesoría para garantizar la cobertura de sus servicios y así llegar a todas las áreas de la empresa.

CAUSA

La empresa no ha estructurado un organigrama donde se pueda definir los niveles de apoyo y asesoría que brindaría la creación de una Unidad de Tecnología de Información y Comunicación.

EFECTO

La ausencia de niveles de apoyo y asesoría de la Unidad de Tecnología de Información y Comunicación provoca que las unidades pertenecientes a la empresa no tengan una ayuda ni una asesoría en el desarrollo y buen manejo de la tecnología en sus áreas de trabajo.

CONCLUSIÓN

El personal al no contar con una Unidad de Tecnología de Información y Comunicación se crea un ineficiente desempeño en sus actividades diarias dentro de la empresa provocando que actúan conforme a lo que tienen de conocimiento o acudiendo a una asesoría externa que no sepa en su totalidad la situación real de la empresa, actuando conforme a la falta de conocimiento y experiencia.

RECOMENDACIÓN

Se deberá definir líneas de apoyo y asesoría el cual deberá ser socializado con todo el personal de la empresa evitando de esta manera que se generen dudas y acudan de manera inmediata a la Unidad de Tecnología de Información y Comunicación para la resolución eficiente y eficaz de dicha unidad y así el personal estará 100% apto y seguro de la labor a desempeñar.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

La empresa no cuenta con planes de desarrollo informático.

CRITERIO

Según la norma 410-03 de la Contraloría General del Estado menciona del plan informático estratégico de la tecnología, nos dice la Unidad de Tecnologías de la Informacion deberá elaborar para posteriormente implementar un plan estratégico informático en el cual se detallarán su forma de contribuir con los objetivos, misión y visión de la empresa considerando que esta deberá contar con planes de mejora donde participaran todas y cada una de las áreas pertenecientes a la empresa.

CAUSA

La entidad no le ha dado la debida importancia de crear planes de desarrollo informático desde la creación de la empresa hasta la actualidad.

EFECTO

La ausencia de un plan de desarrollo informático hace que la empresa no pueda proveer como solucionar o como mejorar la empresa corriendo el riesgo de tener equipos obsoletos sin tener un respaldo de qué hacer con ellos para darle un uso adecuado sin que ocupen espacios físicos, dependencia constante de empresas ajenas para la solución de errores generando un gasto innecesario a la empresa.

CONCLUSIÓN

Al no contar con los planes de desarrollo informáticos y al no darle la debida importancia a las beneficios y desventajas de dichos planes la empresa se expone a un riesgo potencial, gastos innecesarios, vulnerabilidad de los recursos informáticos en cada una de las áreas de la empresa y que el personal no cuenta con un respaldo o guía para actuar correctamente en el caso de presentar inconvenientes.

RECOMENDACIÓN

Si la entidad considera la creación un buen plan de desarrollo se puede independizar de empresas externas para el manejo de información o resolución de problemas de equipos informáticos, teniendo la posibilidad de que un futuro se añada este tipo de servicio a otras empresas incrementando sus ingresos económicos, más estabilidad dentro de mercado y oportunidad de crecimiento rápido.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

No se conocen ni se aplican las normas establecidos por parte de la Unidad de Tecnologías de la Informacion y Comunicación para el manejo de los recursos informáticos.

CRITERIO

Según la norma 410-04 de la Contraloría General del Estado donde se menciona las políticas y procedimientos en la cual nos dice que el gerente de una empresa aprobara políticas y procedimientos donde se puedan definir claramente los procedimientos a seguir para la regulación y control de actividades. Por lo tanto, la entidad deberá contar con un documento de respaldo donde se plasme el reglamento o normativa aprobado y difundido por gerencia que la entidad necesita para el buen manejo de los recursos informáticos

CAUSA

Al no contar con una Unidad de Tecnologías de la Informacion y Comunicación la empresa no puede dar a conocer ni aplicar las normas que generalmente esta unidad establece para todas las áreas que integran a una empresa

EFECTO

Al no tener primeramente una Unidad de Tecnologías de la Informacion y Comunicación la entidad no podrá implementar normas para el manejo de los recursos informáticos y las demás áreas que integran a la empresa no tienen ni respaldo de asesoría adecuada para actuar conforme a los establecido por esta unidad.

CONCLUSIÓN

El personal al no contar con una Unidad de Tecnología de Información y Comunicación se crea un ineficiente desempeño en sus actividades diarias dentro de la empresa provocando que actúan conforme a lo que tienen de conocimiento o acudiendo a una asesoría externa que no sepa en su totalidad la situación real de la empresa, actuando conforme a la falta de conocimiento y experiencia.

RECOMENDACIÓN

La entidad deberá crear una Unidad de Tecnologías de la Informacion y Comunicación para posteriormente implementar normas para el uso adecuado de los recursos informáticos que conforme a la norma 410-04 esta sea aprobada y socializada por el gerente y de esta manera se puede contar con un respaldo y llevar un control correcto de dichos recursos informáticos.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

No se encuentran definidas las funciones y responsabilidades del personal de la Unidad de Tecnologías de la Informacion y Comunicación.

CRITERIO

Según la norma 410-02 de la Contraloría General del Estado donde nos menciona acerca de la Segregación de funciones, nos dice que las funciones y responsabilidades deberán estar definidas y socializadas para que así no pueda haber duplicación de funciones dentro de la empresa y así llevar a cabo un control del rendimiento de personal y evaluación de los perfiles de puesto de trabajo que puedan cubrirse conforme a la necesidad de cada organización.

CAUSA

Las funciones y responsabilidades del personal de Master Technology no están definidas por la Unidad de Tecnologías de la Informacion y Comunicación por la ausencia de la misma por lo que gerencia no realización su debida creación.

EFECTO

Al no tener definidas las funciones y responsabilidades el personal realiza una duplicidad dentro de cada una de las áreas ocasionando confusión y atascamiento de procesos y procedimientos en las labores diarias de la entidad.

CONCLUSIÓN

La entidad al no contar con sus funciones y responsabilidades con los que debe contar cada trabajador de la empresa, se expone a que su personal al no contar claramente definidos sus perfiles de trabajo actuara conforme les parezca correcto y conveniente para ellos provocando que exista tiempo ocio, improductividad, atrasos e incumplimiento de metas tanto personales como institucionales.

RECOMENDACIÓN

Deberán definir las funciones y responsabilidades en todas las áreas que integran la empresa y comunicarlo formalmente a cada área para prevenir posibles problemas a corto, mediano y largo plazo. Y así poder controlar las actividades que realizar cada trabajador, teniendo un respaldo de lo que cada uno de ellos debe hacer en su puesto de trabajo.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

No se cumple con los perfiles del puesto de trabajo para el personal de la Unidad de Tecnologías de la Informacion y Comunicación.

CRITERIO

Según la norma 410-02 de la Contraloría General del Estado donde nos menciona acerca de la Segregación de funciones, nos dice que las funciones y responsabilidades deberán estar definidas y socializadas para que así no pueda haber duplicación de funciones dentro de la empresa y así llevar a cabo un control del rendimiento de personal y evaluación de los perfiles de puesto de trabajo que puedan cubrirse conforme a la necesidad de cada organización.

CAUSA

Los perfiles del puesto de trabajo para el personal de la Unidad de Tecnologías de la Informacion y Comunicación de Master Technology no están definidas por la misma ante la ausencia de la misma por lo que gerencia no realización su debida creación.

EFECTO

Al no tener definidas los perfiles del puesto de trabajo para el personal de la Unidad de Tecnologías de la Informacion y Comunicación de Master Technology el personal realiza una duplicidad dentro de cada una de las áreas ocasionando confusión y atascamiento de procesos y procedimientos en las labores diarias de la entidad.

CONCLUSIÓN

La entidad al no contar los perfiles del puesto de trabajo con los que debe contar cada trabajador de la empresa, se expone a que su personal al no contar claramente definidos sus perfiles de trabajo actuara conforme les parezca correcto y conveniente para ellos provocando que exista tiempo ocio, improductividad, atrasos e incumplimiento de metas tanto personales como institucionales.

RECOMENDACIÓN

Deberán definir los perfiles del puesto de trabajo en todas las áreas que integran la empresa y comunicarlo formalmente a cada área para prevenir posibles problemas a corto, mediano y largo plazo. Y así poder controlar las actividades que realizar cada trabajador, teniendo un respaldo de lo que cada uno de ellos debe hacer en su puesto de trabajo.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

No se cuenta con planes de capacitación para la Unidad de Tecnologías de la Información y Comunicación.

CRITERIO

Según la norma 410-15 de la Contraloría General del Estado donde nos menciona acerca de la Capacitación Informática, nos dice que están dirigidas ya sea para personal de la Unidad de Tecnologías de la Información y Comunicación como para los usuarios, orientadas a los puestos de trabajo y a la necesidad de adquirir o actualizar los conocimientos de cada una de las áreas.

CAUSA

La empresa Master Technology no cuenta con planes de capacitación para la Unidad de Tecnologías de la Información y Comunicación ya que sus capacitaciones son de manera general a todo el personal de la entidad.

EFECTO

Al no contar con planes de capacitación para el personal de la Unidad de Tecnologías de la Información y Comunicación de Master Technology el personal no actualiza sus conocimientos para desempeñarse eficaz y eficientemente dentro de las áreas.

CONCLUSIÓN

La ausencia de planes de capacitación provoca una desactualización de conocimientos lo que significa que el personal de la unidad no podrá desempeñarse bien en sus puestos de trabajo como no podrá hacer uso correcto de los recursos informáticos por falta de capacitaciones.

RECOMENDACIÓN

La entidad debe realizar planes de capacitación para el personal de la Unidad de Tecnologías de la Información y Comunicación y del resto de sus áreas para mantenerse actualizado de los nuevos avances tecnológicos, sus herramientas y formas de adaptación a los cambios constantes que las empresas enfrentan día con día para satisfacer con las necesidades de sus clientes.

Elaborado por: D.J.U. R **Fecha:** 14/08/2020

Revisado por: W.G.Y.CH/C.V. BP **Fecha:** 14/08/2020

CONDICIÓN

La Unidad de Tecnologías de la Información y Comunicación no cuenta con un manual de políticas de gestión.

CRITERIO

Según la norma 410-04 de la Contraloría General del Estado donde se menciona las políticas y procedimientos en la cual nos dice que el gerente de una empresa aprobara políticas y procedimientos donde se puedan definir claramente los procedimientos a seguir para la regulación y control de actividades. Por lo tanto, la entidad deberá contar con un documento de respaldo donde se plasme el reglamento o normativa aprobado y difundido por gerencia que la entidad necesita para el buen manejo de los recursos informáticos

CAUSA

Al no contar con una Unidad de Tecnologías de la Información y Comunicación la empresa no puede dar a conocer ni aplicar un manual de políticas de gestión que la empresa no cuenta para ninguna de sus áreas.

EFECTO

Al no tener primeramente una Unidad de Tecnologías de la Información y Comunicación la entidad no podrá implementar un manual de políticas de gestión por lo que las demás áreas que integran a la empresa no cuentan con dichos manuales para actuar conforme a los establecido por esta unidad.

CONCLUSIÓN

La ausencia de la Unidad de Tecnología de Información y Comunicación crea un ineficiente desempeño en sus actividades diarias dentro de la empresa por la falta de una manual de políticas de gestión provocando que actúan conforme a lo que tienen de conocimiento o acudiendo a una asesoría externa que no sepa en su totalidad la situación real de la empresa

RECOMENDACIÓN

La entidad deberá crear una Unidad de Tecnologías de la Información y Comunicación para posteriormente crear e implementar un manual de políticas de gestión que ayuden al buen rendimiento de todas las áreas que conforman la empresa

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

No existe un manual de procesos y procedimientos que se encuentren debidamente actualizados

CRITERIO

Según la norma 410-04 de la Contraloría General del Estado donde se menciona las políticas y procedimientos en la cual nos dice que el gerente de una empresa aprobara políticas y procedimientos donde se puedan definir claramente los procedimientos a seguir para la regulación y control de actividades. Por lo tanto, la entidad deberá contar con un documento de respaldo donde se plasme el reglamento o normativa aprobado y difundido por gerencia que la entidad necesita para el buen manejo de los recursos informáticos

CAUSA

La inexistencia de un manual de procesos y procedimientos hace que no se puedan actualizar los mismos por lo que la entidad se ha descuidado de la creación de dichos manuales.

EFECTO

El personal de la empresa no tiene conocimientos de los debidos procesos y procedimientos que se deben seguir para una eficiente labor Enel desempeño de sus actividades tanto con los recursos informáticos como con los usuarios.

CONCLUSIÓN

El riesgo que corre la empresa es significativo al no tener un manual de procesos y procedimientos que respalden sus acciones dentro de cada una de las áreas de la entidad, ocasionando una falta de control total respecto a la decisión de cada trabajador sobre cómo hacer su trabajo.

RECOMENDACIÓN

La empresa Master Technology debe crear e implementar un manual de procesos y procedimientos para beneficio propio ya que de esta manera podrá controlas las acciones que realiza cada trabajador de la empresa en cada uno de sus puestos de trabajo considerando que tendrán un respaldo como es el manual en caso de incumplimiento para su debida sanción.

Elaborado por: D.J.U. R **Fecha:** 14/08/2020

Revisado por: W.G.Y.CH/C.V. BP **Fecha:** 14/08/2020

CONDICIÓN

Los recursos informáticos disponibles en la empresa no solventan a cabalidad las necesidades de la empresa.

CRITERIO

Según la norma 410-12 de la Contraloría General del Estado donde se menciona la Administración de Soporte De Tecnologia de Informacion en su inciso 1 donde nos dice que se deberán realizar revisiones de manera periódica para constatar si los recursos informáticos son suficientes para poder cubrir las necesidades. Por lo tanto, para poder cumplir con esta norma se deberá tener previamente un inventario en el cual puedan basarse para su constatación y toma de decisiones.

CAUSA

Los recursos informáticos disponibles en la empresa no solventan a cabalidad las necesidades de la empresa debido a la mala distribución de la misma en cada una de sus áreas.

EFECTO

La falta de recursos informáticos en la empresa al no solventar a cabalidad las necesidades de la empresa debido a la mala distribución de la misma en cada una de sus áreas produce un retraso en sus actividades y el no cumplimiento de los objetivos ya establecidos por la empresa.

CONCLUSIÓN

La falta de supervisión de los recursos informáticos que disponen cada una de las áreas que integran la empresa ocasiona que la misma no tenga conocimiento de lo que se necesita para su buen funcionamiento, como tampoco se sabe que recursos ya no son útiles y en que nomás se debería invertir.

RECOMENDACIÓN

La entidad deberá supervisar de manera regular para llevar un control de todos los recursos disponibles que tiene y verificar cada de las áreas para la constatación física de lo que se necesita en cada una de ella, de lo que ya no debería constar en el inventario y de posibles nuevas adquisiciones que ayuden al buen funcionamiento de la empresa.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

No existen procedimientos a seguir para la resolución de problemas de los equipos informáticos.

CRITERIO

Según la norma 410-04 de la Contraloría General del Estado donde se menciona las políticas y procedimientos en la cual nos dice que el gerente de una empresa aprobara políticas y procedimientos donde se puedan definir claramente los procedimientos a seguir para la regulación y control de actividades. Por lo tanto, la entidad deberá contar con un documento de respaldo donde se plasme el reglamento o normativa aprobado y difundido por gerencia que la entidad necesita para el buen manejo de los recursos informáticos

CAUSA

La inexistencia de procedimientos a seguir para la resolución de problemas de los equipos informáticos es causa de que la gerencia no se ha preocupado de la creación de dichos procedimientos ya que se encuentran en manos de los técnicos a cargo.

EFECTO

Hace que todas las áreas dependan en su totalidad de los técnicos con los que cuenta la empresa, y en caso de la ausencia de ellos el personal no sabe qué acciones tomar.

CONCLUSIÓN

Al depender 100% de sus técnicos sin un documento de respaldo donde se detalle de manera clara que hacer cuando se presentan problemas con los equipos informáticos, hace que la empresa no avance internamente y sea inestable en sus procesos por lo que puede ocasionar inconvenientes con sus clientes o usuarios al momento de presentarse este problema en un momento inadecuado.

RECOMENDACIÓN

Es recomendable que la empresa tenga un documento de respaldo para que cada área que integra la empresa sea independiente de manera parcial de los técnicos y sepan que acciones deben tomar en caso de presentarse problemas con cada uno de sus equipos informáticos y acudir a ellos siempre y cuando el problema requiera de un técnico.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

No cuentan con estrategias establecidas para la mejora continua de los recursos informáticos.

CRITERIO

Según la norma 410-04 de la Contraloría General del Estado donde se menciona las políticas y procedimientos en la cual nos dice que el gerente de una empresa aprobara políticas y procedimientos donde se puedan definir claramente los procedimientos a seguir para la regulación y control de actividades. Por lo tanto, la entidad deberá contar con un documento de respaldo donde se plasme el reglamento o normativa aprobado y difundido por gerencia que la entidad necesita para el buen manejo de los recursos informáticos

CAUSA

La inexistencia de estrategias establecidas para la mejora continua de los recursos informáticos es causa de que la gerencia no se ha preocupado de la creación de dichas estrategias.

EFECTO

Hace que todas las áreas ante la falta de estrategias no se tome ninguna acción respecto a la mejora continua, es decir, si la gerencia no presenta estrategias nadie lo hará.

CONCLUSIÓN

Cuando no existe estrategias para la mejora continua, hace que la empresa no avance internamente y sea inestable en sus procesos por lo que puede ocasionar inconvenientes innecesarios por lo que el personal actuara de manera individual y ejecutara la estrategia que el crea conveniente.

RECOMENDACIÓN

Es recomendable que la empresa tenga un documento de respaldo para que cada área que integra la empresa sepa de las estrategias que ayudaran a la mejora continua para el proceso rápido de sus actividades en cada área de trabajo beneficiando también a los recursos informáticos que la empresa dispone y pueda disponer de acuerdo a las necesidades que vayan surgiendo para cumplir con los objetivos establecidos por la empresa.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

El espacio físico donde se encuentran los equipos informáticos no cuenta con las seguridades necesarias.

CRITERIO

Según la norma 410-10 de la Contraloría General del Estado donde se menciona la Seguridad de Tecnologia de información en su inciso 6 nos dice que, las instalaciones físicas donde se encuentren los equipos informáticos deberán ser adecuadas para monitorear y controlar su estado, así como su temperatura, la humedad, energía que estas necesitan para su buen funcionamiento.

CAUSA

Los espacios físicos donde se encuentran los equipos informáticos no cuentan con las seguridades que estas necesitan debido a la falta de inversión para salvaguardar dichos equipos.

EFECTO

Al no contar con la seguridad necesaria en los espacios físicos donde se encuentran los equipos informáticos, estos corren riesgos de sufrir un daño considerable que afecta de manera económica a la empresa.

CONCLUSIÓN

La entidad no percibe los posibles riesgos que corre al no destinar fondos para invertir en la seguridad del espacio físico de sus equipos informáticos, estos daños pueden ser desde leve hasta permanente incluso dejar obsoleto algunos de sus equipos por la falta de prevención.

RECOMENDACIÓN

Se debe enviar fondos destinados exclusivamente a la seguridad de sus espacios físicos ya que la actividad económica de la empresa depende de su equipamiento tecnológico, por ende, esta se verá afecta si no salvaguardan sus equipos, recurso informático primordial para el buen desempeño del personal y funcionamiento de la entidad.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

No existe un responsable del mantenimiento adecuado de los equipos informáticos.

CRITERIO

Según la norma 410-09 de la Contraloría General del Estado donde se menciona el Mantenimiento y control de la infraestructura tecnológica en su inciso 6 en la cual nos dice se deberá elaborar un plan donde conste el mantenimiento tanto preventivo como correctivo, plasmando revisiones periódicas, control de las áreas críticas y la evaluación de sus vulnerabilidades relacionadas con los hardware y software.

CAUSA

Los equipos informáticos no cuentan con un responsable directo de su mantenimiento debido a que estas necesitan de una inversión para salvaguardar dichos equipos.

EFECTO

La entidad no percibe los posibles riesgos que corre al no destinar fondos para invertir en la Enel mantenimiento de sus equipos informáticos, estos daños pueden ser desde leve hasta permanente incluso dejar obsoleto algunos de sus equipos por la falta de prevención.

CONCLUSIÓN

El riesgo que corre la empresa es significativo al no tener un manual de procesos y procedimientos que respalden sus acciones dentro de cada una de las áreas de la entidad, ocasionando una falta de control total respecto a la decisión de cada trabajador sobre cómo hacer su trabajo.

RECOMENDACIÓN

Se debe designar un responsable del mantenimiento de los equipos informáticos para llevar un control de quien está a cargo de su correcto funcionamiento ya que la actividad económica de la empresa depende de su equipamiento tecnológico, por ende, esta se verá afecta si no salvaguardan sus equipos, recurso informático primordial para el buen desempeño del personal y funcionamiento de la entidad

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

La entidad no cuenta con un inventario de los recursos informáticos de su matriz y sucursales.

CRITERIO

Según la norma 410-08 de la Contraloría General del Estado donde se menciona adquisiciones de infraestructura tecnológica en su inciso 2 nos dice que la Unidad de Tecnologías de la Informacion y Comunicación es el encargado de la planificación tecnológica adquisición y vida útil de los recursos informáticos de acuerdo a los requerimientos de cada área de trabajo.

CAUSA

La persona encargada del inventario es trabajador independiente de la empresa por lo que solo se realiza inventario cada que recibe una autorización expresa del gerente administrativo.

EFECTO

Al no contar con un inventario permanente y actualizado el personal no tiene conocimiento de cuanta existencia hay, por lo que su conocimiento es pobre en cuestión de productos disponibles para la venta.

CONCLUSIÓN

Si no se cuenta con un inventario permanente y actualizado regularmente se corre los riesgos que la empresa ya a enfrentado respecto a que se ofrece un producto que no se tenía conocimiento que ya no había por la falta de dicho inventario y quedan como empresa ante la falta de seriedad delante de sus clientes causando una mala reputación de la misma.

RECOMENDACIÓN

Contar con un inventario que se encuentre actualizado para conocimiento de cuantos productos se venden, cuantos son entregados a bodega, los que tenga algún tipo de imperfección con los detalles claros y concisos del producto para que al momento de que sean solicitados el personal tenga conocimiento de hasta cuantos puede vender acorde a su disponibilidad.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

No existe señaléticas en las áreas donde se encuentran los recursos informáticos.

CRITERIO

Según la norma 410-08 de la Contraloría General del Estado donde se menciona adquisiciones de infraestructura tecnológica en su inciso 2 nos dice que la Unidad de Tecnologías de la Informacion y Comunicación es el encargado de la planificación tecnológica adquisición y vida útil de los recursos informáticos de acuerdo a los requerimientos de cada área de trabajo.

CAUSA

No se considera la debida importancia al uso de señaléticas en el área donde se encuentran los equipos informáticos basándose únicamente en la conciencia del personal.

EFECTO

Aunque el personal tenga conocimiento básico del tipo de señaléticas que puedan haber, la empresa corre riesgo de que sus equipos informáticos sufran daños por parte del personal al no tener una orden visual que les permite percibir el riesgo que corre un equipo informático por alguna imprudencia de los trabajadores.

CONCLUSIÓN

Las señaléticas son algo indispensable que debe tener una empresa para prevenir posibles riesgos de sus equipos informáticos por la imprudencia de su personal, al no tener señalética los trabajadores dejan a su criterio los posibles riesgos que corre un equipo informático al momento de realizar sus actividades diarias como por ejemplo pensar tomar líquidos encima de dichos equipos creyendo que no pasara nada.

RECOMENDACIÓN

Colocar señaléticas en las áreas donde se encuentren los recursos informáticos para prevenir posibles riesgos de dichos equipos por la imprudencia de su personal, que sean visibles y colocados en lugares estratégicos establecidos por la gerencia, tanto en su matriz como en sus sucursales evitando generar dudas respectos a los riesgos que pueden ocurrir dentro de la empresa por la ausencia de señalética.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

El gerente administrativo no cuenta con un plan de contingencia en caso de que los equipos informáticos estén en riesgo.

CRITERIO

Según la norma 410-11 de la Contraloría General del Estado donde se menciona Los Planes de Contingencia en su inciso 1 en la cual nos dice que esto es correspondiente de la Unidad de Tecnologías de la Informacion y Comunicación para que pueda tomar acciones a través de un plan de respuesta al riesgo la cual deberá incluir los posibles escenarios, designación de responsables para salvaguardar la seguridad física, la seguridad de su información en lo posible al 100% de su totalidad.

CAUSA

La ausencia de un plan de contingencia no a sido considerada por el gerente administrativo ya que no se contempla la opción de que sus equipos puedan estar en riesgo.

EFECTO

Los equipos informáticos corren verdadero riesgo ante la falta de un plan de contingencia para prevenir dichos riesgos pasando de un problema leve a un problema grave que afecte a toda la entidad.

CONCLUSIÓN

La falta de conocimiento con respecto a un plan de contingencia pone en vulnerabilidad a los equipos informáticos, siendo riesgoso para cada una de las áreas de la empresa, ocasionando pérdidas económicas, pérdida total de sus equipos por no saber que acciones se deben tomar ante los posibles escenarios que puedan presentarse.

RECOMENDACIÓN

La realización de un plan de contingencia es indispensable ante la necesidad de poder proveer los riesgos que puedan afectar los equipos informáticos, con un plan se podrá enfrentar ante los escenarios de riesgos de manera oportuna, fortaleciendo a la empresa y a sus trabajadores brindándoles una herramienta con que enfrentar las situaciones.

Elaborado por: D.J.U. R **Fecha:** 14/08/2020

Revisado por: W.G.Y.CH/C.V. BP **Fecha:** 14/08/2020

CONDICIÓN

La empresa no cuenta con respaldos de información de los equipos informáticos.

CRITERIO

Según la norma 410-10 de la Contraloría General del Estado donde se menciona la Seguridad de Tecnologia de información en su inciso 4 nos dice que, se debe guardar información critica o sensible en lugares externos a la empresa, la misma debe contar con un lugar de almacenamiento o un sitio que sea seguro para los respaldos de información de los equipos informáticos.

CAUSA

Existe mucha confianza en mantener el respaldo de la información en una sola persona o en un solo equipo de la empresa.

EFECTO

La entidad puede perjudicarse gravemente ante la falta de respaldos de información quedando en cero tras perder información confidencial y única para la misma.

CONCLUSIÓN

La empresa al haber experimentado la perdida de información por la falta de respaldos su posición fue critica por haber perdido toda la información indispensable para entidad ocasionando problemas en cada una de sus áreas, por lo que previo a la perdida aun no se han podido recupera en su totalidad información guardado por años.

RECOMENDACIÓN

Conforme a lo que establece la norma 410-10 Seguridad de Tecnologia de información en su inciso 4. L empresa deberá tener almacenado, respaldado su información en lugares externos considerados seguros para la entidad para evitar problemas graves a la empresa, además es recomendable tener respaldos en más de un dispositivo y en más de un lugar.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

Los integrantes de la empresa no saben cómo actuar en caso de presentarse una situación de riesgo que comprometa los recursos informáticos.

CRITERIO

Según la norma 410-11 de la Contraloría General del Estado donde se menciona Los Planes de Contingencia en su inciso 1 en la cual nos dice que esto es correspondiente de la Unidad de Tecnologías de la Informacion y Comunicación para que pueda tomar acciones a través de un plan de respuesta al riesgo la cual deberá incluir los posibles escenarios, designación de responsables para salvaguardar la seguridad física, la seguridad de su información en lo posible al 100% de su totalidad.

CAUSA

La ausencia de un plan de contingencia no ha sido considerada por el gerente administrativo ya que no se contempla la opción de que sus equipos puedan estar en riesgo.

EFECTO

Los recursos informáticos al ser indispensables para el buen funcionamiento de la entidad al no saber cómo actuar ante un riesgo, la empresa se enfrenta desde pérdidas económicas hasta una paralización temporal de sus actividades.

CONCLUSIÓN

La falta de conocimiento con respecto a un plan de contingencia pone en vulnerabilidad a los recursos informáticos, siendo riesgoso para cada una de las áreas de la empresa, ocasionando pérdidas económicas, pérdida total de sus recursos por no saber que acciones se deben tomar ante los posibles escenarios que puedan presentarse.

RECOMENDACIÓN

La realización de un plan de contingencia es indispensable ante la necesidad de poder proveer los riesgos que puedan afectar los recursos informáticos, con un plan se podrá enfrentar ante los escenarios de riesgos de manera oportuna, fortaleciendo a la empresa y a sus trabajadores brindándoles una herramienta con que enfrentar las situaciones.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

El acceso al centro de datos no cuenta con una restricción para personal no autorizado.

CRITERIO

Según la norma 410-10 de la Contraloría General del Estado donde se menciona la Seguridad de Tecnologia de información en su inciso 1 nos dice que, el acceso deberá ser controlado con el fin de salvaguardar la ubicación donde se encuentran los equipos y recursos informático.

CAUSA

La falta de control con la restricción de personal no autorizada es a causa de que todo el personal de la empresa puede ingresar y salir sin ningún tipo de registro.

EFECTO

Surgimiento de problemas al no saber quién nomas tuvo acceso al centro de datos por la falta de control de personal no autorizado.

CONCLUSIÓN

No se tiene conocimiento, ni registro ni ningún tipo de control por lo que no se puede señalar responsables en caso de llegar a presentarse problema en el centro de datos, perdida de recursos o equipos informáticos ni límite de tiempo en su permanencia.

RECOMENDACIÓN

Es necesario llevar un control para el personal no autorizado que impida su acceso al centro de datos para evitar inconvenientes que lleguen a perjudicar al área incluso hasta la entidad.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

Los equipos informáticos no cuentan con una adecuada estructura de red para comunicarse.

CRITERIO

Según la norma 410-01 de la Contraloría General del Estado donde nos menciona acerca de la Organización Informática nos dique que la Unidad de Tecnología de la información deberá constar en la estructura organizacional, tener definidos los niveles de apoyo como de asesoría para garantizar la cobertura de sus servicios y así llegar a todas las áreas de la empresa.

CAUSA

Falta de fondos para invertir en una adecuada estructura de red que permita una óptima comunicación de los equipos informáticos.

EFECTO

Existe una mala comunicación con todas las áreas de la empresa por la falta de una buena estructura de red que les permita un envió de información optimo y sin problemas.

CONCLUSIÓN

Considerando la actividad de la empresa en donde los recursos y equipos informáticos son su principal herramienta que no exista una buena comunicación por la falta de una estructura de red adecuada hace que la empresa se quede atascada y no progrese de manera eficiente impidiendo prestar un buen servicio a la ciudadanía.

RECOMENDACIÓN

Establecer fondos que puedan ser invertidos en una adecuada estructura de red la cual permita que sus equipos informáticos tengan una buena comunicación dentro del área y todas las unidades que integran a la empresa.

CONDICIÓN

La empresa no cuenta con el equipo de vigilancia necesaria para salvaguardar la seguridad de los recursos informáticos.

CRITERIO

Según la norma 410-10 de la Contraloría General del Estado donde se menciona la Seguridad de Tecnologia de información en su inciso 6 nos dice que, las instalaciones físicas donde se encuentren los equipos informáticos deberán ser adecuadas para monitorear y controlar su estado, así como su temperatura, la humedad, energía que estas necesitan para su buen funcionamiento.

CAUSA

Al no contar con el equipo de vigilancia necesaria para salvaguardar la seguridad de los recursos informáticos no cuentan con las seguridades que estas necesitan debido a la falta de inversión de dichos equipos.

EFECTO

Al no contar con la seguridad necesaria del equipo de vigilancia para salvaguardar la seguridad donde se encuentran los recursos informáticos, estos corren riesgos de sufrir un daño considerable que afecta de manera económica a la empresa sin saber que o quien lo ocasiono.

CONCLUSIÓN

La entidad no percibe los posibles riesgos que corre al no destinar fondos para invertir en la seguridad necesaria del equipo de vigilancia que son útiles para salvaguardar la seguridad de los mismos.

RECOMENDACIÓN

Se debe enviar fondos destinados exclusivamente a la seguridad de equipo de vigilancia necesaria para salvaguardar la seguridad de los recursos informáticos ya que la actividad económica de la empresa depende de su equipamiento tecnológico, por ende, esta se verá afecta si no salvaguardan sus equipos, recurso informático primordial para el buen desempeño del personal y funcionamiento de la entidad.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

No se mantiene un control de actividades de cada usuario de los distintos equipos informáticos.

CRITERIO

Según la norma 410-04 de la Contraloría General del Estado donde se menciona las políticas y procedimientos en la cual nos dice que el gerente de una empresa aprobara políticas y procedimientos donde se puedan definir claramente los procedimientos a seguir para la regulación y control de actividades. Por lo tanto, la entidad deberá contar con un documento de respaldo donde se plasme el reglamento o normativa aprobado y difundido por gerencia que la entidad necesita para el buen manejo de los recursos informáticos

CAUSA

La inexistencia de un control de actividades de cada usuario de los equipos informáticos se de a que no existe usuarios específicos que indica que persona fue la ocupo dicho equipo.

EFECTO

El personal de la empresa no tiene conocimientos de los debidos procesos y procedimientos que se deben seguir para una eficiente labor. En el desempeño de sus actividades tanto con los recursos informáticos como con los usuarios.

CONCLUSIÓN

El riesgo que corre la empresa es significativo al no tener un control de actividades de cada usuario que respalden sus acciones en cada uno de los equipos informáticos, ocasionando una falta de control total respecto a la decisión de cada trabajador sobre cómo hacer su trabajo.

RECOMENDACIÓN

Llevar un control de las actividades de cada usuario en los distintos equipos informáticos para saber en todo momento quien nomas uso el equipo, el tiempo que lo utilizo, la actividad que realizo y si el nombre del usuario corresponde a la Identidad de usuario que le correspondía para que la entidad tenga detalles en caso de surgir algún problema con los equipos y designar un responsable para su respectiva sanción.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

Los equipos informáticos no cuentan con una póliza de seguros como respaldo.

CRITERIO

Según la norma 410-10 de la Contraloría General del Estado donde se menciona la Seguridad de Tecnologia de información en su inciso 4 nos dice que, se debe guardar información crítica o sensible en lugares externos a la empresa, la misma debe contar con un lugar de almacenamiento o un sitio que sea seguro para los respaldos de información de los equipos informáticos.

CAUSA

La gerencia no ha considerado por motivos económicos póliza de seguros como respaldo para sus equipos informáticos.

EFECTO

La entidad puede perjudicarse gravemente ante la falta de respaldos de sus equipos informáticos.

CONCLUSIÓN

La empresa al haber experimentado la perdida de equipos informáticos por la falta de respaldos como lo son las pólizas de seguros su posición fue critica por haber perdido toda la información indispensable para entidad ocasionando problemas en cada una de sus áreas, por lo que previo a la perdida aún no se han podido recupera en su totalidad información guardado por años.

RECOMENDACIÓN

Conforme a lo que establece la norma 410-10 Seguridad de Tecnologia de información en su inciso 4. L empresa deberá tener almacenado, respaldado sus equipos informáticos mediante pólizas de seguros para evitar problemas graves a la empresa, además es recomendable tener respaldos en más de un dispositivo.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

No existen planos de la red de conexión de los equipos informáticos.

CRITERIO

Según la norma 410-10 de la Contraloría General del Estado donde se menciona la Seguridad de Tecnologia de información en su inciso 6 nos dice que, las instalaciones físicas donde se encuentren los equipos informáticos deberán ser adecuadas para monitorear y controlar su estado, así como su temperatura, la humedad, energía que estas necesitan para su buen funcionamiento.

CAUSA

Se debe a la época con la que fue creada la empresa porque no se tenía gran conciencia a la importancia de documentar este tipo de aspectos.

EFECTO

No poder determinar en qué punto exacto se dio una brecha de seguridad por la falta de planos de red de conexión de los equipos informáticos.

CONCLUSIÓN

Es un gran riesgo ya que en el momento que se genere una falla no se va a poder determinar a qué escala afecta esta falla a la empresa porque no se tiene conocimiento de a qué y cuantos equipos se encuentran conectados lo que conlleva en el no poder determinar con exactitud que equipos fueron afectados, que seguridades fueron violadas o que sistemas pueden generar problemas a futuro a raíz de la falla que se pudo generar.

RECOMENDACIÓN

Realizar un mapeo de toda la red para determinar conexione innecesarias, conexiones faltantes, posibles riesgos y darle solución lo más pronto posible a dichas fallas.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

El software con el que cuenta la empresa no protégela información contra ataques informáticos.

CRITERIO

Según la norma 410-10 de la Contraloría General del Estado donde se menciona la Seguridad de Tecnologia de información en su inciso 5 nos dice que, se deberán implementar seguridades respecto a software y hardware, y sus seguridades de manera periódica con acciones preventivas y correctivas a las que se encuentran vulnerables como lo son ataques informáticos.

CAUSA

La empresa prefiere por motivos económicos adquirir un software gratuito que se adquiere vía internet sin tomar en cuenta el riesgo que esto implica.

EFECTO

El sistema se encuentra siempre en constante vulnerabilidad por lo que el software gratuito no protege en su totalidad de los ataques informáticos que se encuentran en la red.

CONCLUSIÓN

El no considerar un software pagado que protege de todos los ataques informáticos a los que exponen En el internet corre riesgo de vulnerabilidad de su información y de sus equipos informáticos por la facilidad que se tiene de acceso a su sistema debido a su software.

RECOMENDACIÓN

Cambiar el software que tienen gratuito e invertir en un software pagado que proteja de mejor manera contra los ataques informáticos y disminuir el riesgo de vulnerabilidad al sistema de la empresa Master Technology disminuyendo de esa manera también el riesgo de sus equipos informáticos.

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

CONDICIÓN

La organización no cuenta con políticas que establece la creación de contraseñas seguras para el acceso al sistema informático.

CRITERIO

Según la norma 410-04 de la Contraloría General del Estado donde se menciona las políticas y procedimientos en la cual nos dice que el gerente de una empresa aprobara políticas y procedimientos donde se puedan definir claramente los procedimientos a seguir para la regulación y control de actividades. Por lo tanto, la entidad deberá contar con un documento de respaldo donde se plasme políticas con respecto al uso de contraseñas seguras para el acceso al sistema informático.

CAUSA

La falta de políticas para la creación de contraseñas seguras para el acceso al sistema informático se debe a la utilización de una sola contraseña para el acceso al sistema.

EFECTO

Por la falta de control y de políticas con la creación de contraseñas la empresa corre riesgo que en un descuido del personal la contraseña llegue a manos ajenas e ingrese a información confidencial de la empresa.

CONCLUSIÓN

La necesidad de crear políticas de contraseñas seguras para el acceso al sistema informático es indispensable para la seguridad tanto de la información como la de sus equipos porque al manejar una contraseña única para toda la información se hace vulnerable y en un descuido la información queda expuesta a persona ajenas de la entidad.

RECOMENDACIÓN

Crear e implementar políticas de contraseñas seguras para el acceso al sistema informático para de esta manera llevar un control del número de personas que pueden acceder a un equipo y a su información

Elaborado por:	**D.J.U. R**	**Fecha:**	**14/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**14/08/2020**

3.2.3.3. Comunicación de Resultados

Objetivo General

Aplicar una auditoría informática a la empresa Master Technology, cantón quito, provincia de pichincha, período 2019, para valorar la integridad, confidencialidad y disponibilidad de los recursos, equipos informáticos y su información mediante el uso de métodos, técnicas, estándares y herramientas de auditoria informática para la empresa.

Objetivo Específico

- Presentar el informe final de auditoria, con las conclusiones y recomendaciones orientadas a mejorar el uso y gestión de la información con respecto a la integridad, disponibilidad y confidencialidad de los sistemas y recursos informáticos de la empresa.

N.º	Procedimiento	Referencia/T	Elaborado por:	Fecha
1	Programa de Auditoria	PA 1/1	D.J.U. R	15/08/2020
2	Notificación de Culminación del Trabajo	NCT 1/1	D.J.U. R	16/08/2020
3	Convocatoria para lectura del informe	CLI 1/1	D.J.U. R	17/08/2020
4	Informe de Auditoría	IA 1/1	D.J.U. R	18/08/2020

Elaborado por: **D.J.U. R** **Fecha:** **15/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **15/08/2020**

EMPRESA MASTER TECHNOLOGY
NOTIFICACION DE CULMINACION DE ACTIVIDADES
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

NCA 1/1

Riobamba, 16 de agosto del 2020

Ingeniero.

JIMENEZ TORRES RICHARD AUGUSTO

GERENTE ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

Presente. –

La razón de esta presente es para informarle que el equipo de trabajo de auditoria "VALIDATE AUDITORÍA", ha culminado con éxito sus actividades dentro de la empresa Master Technology respecto a la Auditoria Informática que se ha venido realizando e informado en cada una de sus etapas.

Agradecemos su colaboración, paciencia y seguimiento en cada de nuestras actividades, le deseamos el mayor de los éxitos en las actividades de su empresa.

Atentamente,

Ing.: Willian Geovanny Yanza Chávez
DIRECTOR DEL PROYECTO DE TITULACIÓN

Elaborado por:	**D.J.U. R**	**Fecha:**	**16/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**16/08/2020**

EMPRESA MASTER TECHNOLOGY
CONVOCATORIA PARA LECTURA DEL INFORME
DEL 01 DE ENERO AL 31 DEDICIEMBRE DEL 2019

CLI 1/1

Riobamba, 17 de agosto del 2020

Ingeniero.

JIMENEZ TORRES RICHARD AUGUSTO

GERENTE ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

Presente. –

Una vez finalizado el trabajo de Auditoria Informática, convocamos a una reunión para la respectiva lectura del Informe de Auditoria, el cual se llevará cabo el día 28 de Agosto del 2020 a las 10h00 am en las instalaciones de la matriz de la Empresa Master Technology

Nuevamente anticipamos nuestros más sinceros agradecimientos por su colaboración, paciencia y seguimiento en cada de nuestras actividades, le deseamos el mayor de los éxitos en las actividades de su empresa.

Atentamente,

Ing.: Willian Geovanny Yanza Chávez
DIRECTOR DEL PROYECTO DE TITULACIÓN

Elaborado por:	**D.J.U. R**	**Fecha:**	**17/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**17/08/2020**

Riobamba, 28 de agosto del 2020

Ingeniero.

JIMENEZ TORRES RICHARD AUGUSTO

GERENTE ADMINISTRATIVO DE LA EMPRESA MASTER TECHNOLOGY

Presente. –

De mi Consideración

Al término de la Auditoria Informática, aplicada a la empresa Master Technology, del Cantón Quito, Provincia de Pichincha, Periodo 2019, con total responsabilidad me tomo la atribución de expresarme acerca de la integridad, confidencialidad y disponibilidad de los recursos, equipos informáticos y su información mediante el uso de métodos, técnicas, estándares y herramientas de auditoria informática para la empresa, objetivo de la auditoria, y si los mismo cumplen con lo establecido en la norma 410-10 de la Contraloría General del Estado respecto a la tecnología de la información en una opinión clara y concreta.

La Auditoria Informática que se realizo fue en base a los 8 componente que conforman el método COSO II, cuyos elementos han sido de gran utilidad permitiendo una objetiva evaluación en relación a la situación en la que se encontraba la entidad, para poder detectar los posibles problemas que dan paso a que su seguridad física, lógica y de los recursos informáticos no sea confiable ni para la entidad ni para sus usuarios.

En mi opinión, la Empresa Master Technology abarcando tanto matriz como sus sucursales ubicadas en la Ciudad de Quito, no cumple a cabalidad con las normas de control interno COSO II y las normas de la Contraloría General del Estado 410-10 Tecnologías de la Informacion demostrando claramente desde el punto de la observación hasta la obtención de evidencias que la empresa no acata con lo ya establecido perjudicando su estabilidad, seguridad y desarrollo empresarial.

Elaborado por: **D.J.U. R** **Fecha:** **18/08/2020**

Revisado por: **W.G.Y.CH/C.V. BP** **Fecha:** **18/08/2020**

A continuación, se detallarán los hallazgos más relevantes encontrados durante el proceso de auditoria, los cuales se encontrarán de manera resumida.

C1: La Empresa Master Technology ha venido trabajando hasta la actualidad sin el apoyo y asesoría que brinda una Unidad de Tecnologías de la Informacion y Comunicación.

R1: Se debe crear de manera inmediata una Unidad de Tecnologías de la Informacion y Comunicación para que así cada una de las áreas que integran la empresa puedan contar con su apoyo y asesoría cuando sea requerida y ayude a los procesos y procedimientos a ser más eficientes y eficaces.

C2: Jamás se han creado normas, reglamentos que puedan facilitar el buen manejo de los recursos informáticos de la empresa, siendo esto una herramienta principal acorde a la actividad de la empresa.

R2: Crear normas y reglamentos que sirvan como documentación de respaldo para el personal de la empresa y buen uso de los recursos informáticos para una óptima utilización y buen desempeño de la entidad.

C3: No se ha considerado respaldar sus equipos informáticos mediante pólizas de seguros para hacer frente a posibles riesgos que afecten directamente a dichos equipos.

R3: Salvaguardar los equipos informáticos a través de pólizas de seguros evitando el riesgo de perdidas parciales o totales de sus equipos, herramientas fundamentales para el funcionamiento adecuado de la entidad.

C4: La empresa desde su creación no ha implementado respaldos de la información de sus equipos informáticos como seguridad ante escenarios que pongan en riesgo su seguridad.

R4: Respaldar y almacenar la información considerada confidencial e importante, convirtiéndose indispensable para beneficio propio de la entidad por lo que es recomendable su respaldo en más de un equipo, en periodos máximos de 2 semanas y en más de sitio seguro como medida prevención.

C5: El software que dispone la empresa adquirido de forma gratuita, no protege ni la información ni sus equipos contra ataques potencialmente peligrosos que coloca en posición de vulnerabilidad a la entidad.

R5: Se recomienda que se busque un software especializado que cumpla con las necesidades de protección de software de la empresa teniendo en cuenta cada uno de los aspectos principales respecto a seguridad lógica y física.

Elaborado por:	**D.J.U. R**	**Fecha:**	**18/08/2020**
Revisado por:	**W.G.Y.CH/C.V. BP**	**Fecha:**	**18/08/2020**

CONCLUSIONES

- Se realizo una auditoría informática a la empresa Master Technology valorando en el proceso la integridad, confidencialidad y disponibilidad de los recursos, equipos informáticos y su información mediante el uso de métodos, técnicas, estándares y herramientas de auditoria informática para la empresa, obteniendo como resultado la determinación del estado actual de la entidad.

- La revisión previa de diferentes autores que tratan sobre la Auditoria Informática, así como documentos de proyectos previos realizados a otras entidades, permitieron documentar, fundamentar y sustentar adecuadamente el proceso que se realizó durante el presente trabajo de titulación.

- El método Deductivo que parte de lo general a lo especifico permitió generar un criterio propio en base a la obtención de la información de la empresa tanto en su funcionamiento general como en el funcionamiento especifico de cada una de sus áreas.

- Considerando que la empresa desde su creación no ha sido sometida a una Auditoria Informática, desde el punto de vista de un profesional que observe, analice, detalle e interprete los datos de la entidad por lo que, durante el proceso de auditoria, se han encontrado varias deficiencias con los cuales se determinaron hallazgos significativos que ayudaron a convertir sus debilidades en fortalezas mediante la aplicación del método deductivo.

- El informe de auditoría dirigido al gerente administrativo de la empresa Master Technology detalla de manera clara y concisa los aspectos más relevantes encontrados durante el proceso de la Auditoria informática, dando a conocer sus respectivas recomendaciones a dichos aspectos considerados prioritarios, con el único fin de mejorar el estado actual de la entidad.

RECOMENDACIÓNES

- Es recomendable una inspección general de la empresa antes del proceso de auditoria para conocimiento del manejo de los recursos, informáticos, así como la información y datos que manejan, el cual se lo puede llevar a cabo con visitas regulares a la entidad.

- Para el desarrollo del trabajo de titulación se recomienda debe considerar la revisión extensa de los documentos de proyectos similares, así como el contraste con los conceptos extraídos de los libros de los diferentes autores citados o relacionados con el proyecto que se desea realizar, para el enriquecimiento del documento.

- Es recomendable la realización de una Auditoria Informática cada cierto periodo de tiempo para conocimiento del estado de la entidad, desde una perspectiva profesional, que ayude a la identificación de áreas críticas, fallas y posibles riesgos que ponga en vulnerabilidad la estabilidad de la empresa para que así se puedan presentar propuestas que incrementen su nivel de seguridad en todos sus ámbitos, su nivel de eficiencia y eficacia en sus procesos y procedimientos.

- Se sugiere considerar los aspectos más relevantes encontrados durante el proceso de Auditoria Informática**,** así como a sus recomendaciones detalladas en el Informe dirigido al gerente administrativo de la empresa Master Technology quedando a su entera disposición lo que más le beneficie a la entidad

GLOSARIO

A

Ataque de Fuerza Buta

Interprétese como la ejecución de un programa que realizará comprobaciones finitas a un sistema de acceso una por una hasta conseguir la clave o el acceso al sistema, la efectividad de este ataque dependerá de la potencia del equipo utilizado o del número de atacantes.

B

Base de datos

Es un repositorio o un almacén que permite guardar cantidades grandes de información de forma ordenada y que sea de fácil acceso.

D

Dispositivo

Es un mecanismo complejo creado para desarrollar una determinada función, los dispositivos tienen que ser físicos como: un teléfono celular, computadoras, tablets, flash memory.

E

Encriptar

Significa ocultar información usando una clave para que no pueda ser entendido por los que no tienen dicha clave.

Enrutar

Que te dirige o define el destino.

H

Hallazgo

Son todas las anomalías, debilidades, problemas que afectan a las actividades realizadas por una entidad, las cuales pueden presentarse en toda empresa ocasionando que la misma no pueda tener un adecuado desempeño.

N

Nodos

Entiéndase como dispositivos o puntos relevantes dentro de una red o puntos de conexión.

P

Phishing

Es estafar usando técnicas de ingeniería social haciéndose pasas por empresa o personas que portan una aparente comunicación oficial.

R

Recursos informáticos

Es cualquier software, aplicación, herramienta, componente o dispositivo que se puede agregar o combinar con una computadora o sistema.

S

Sistemas informáticos

Es un sistema que permite almacenar, procesar y gestionar la información para la cual hace uso de un conjunto de elementos relacionados entre sí como por ejemplo el hardware, software y profesionales informáticos.,

Software

Es el conjunto de programas o rutinas que brinda soporte lógico a un sistema informático para que pueda realizar tareas específicas.

Spyware

Programa malicioso espía que reúne información de un dispositivo informático y la transmite a otro dispositivo externo sin autorización del dueño.

V

Virus

Programa malicioso diseñado para propagarse dentro de un software oficial y causar daños tanto a software como a hardware.

BIBLIOGRAFÍA

Bonilla, M. F. (2015). *Auditoría Sistemas Informáticos Compañía Hidalgo Broncano Coso Ii Control Interno Toma De Decisiones, De La Ciudad De Riobamba, Provincia De Chimborazo, Periodo, 2012*. (Tesis De Pregrado, Escuela Superior Politécnica De Chimborazo), Obtenido De http://dspace.espoch.edu.ec/handle/123456789/13448

Calder, A. (2017). *Iso27001/Iso27002: Una Guía De Bolsillo.* It Governance Ltd.

Cando Nataly, M. C. (2019). *Auditoría Informática A Metrisa Metropolitana Riobamba Clínica De Servicios Médicos Especializados S.A., De La Ciudad De Riobamba, Provincia De Chimborazo, Período 2018.* (Tesis De Pregrado, Escuela Superior Politécnica De Chimborazo), Obtenido De http://dspace.espoch.edu.ec/handle/123456789/13448

De Luis Gargallo, E. (2018). *La Seguridad Para Los Menores En Internet.* Editorial UOC.

Dordoigne, J., & Atelin, P. (2016). *Redes Informáticas.* ENI.

Gaitán, R. E. (2015). *Administración De Riesgos ERM Y La Auditoría Interna.* ECOE Ediciones.

Cárdenas H., C. Y., Soto, D. Y. E. H., & Efrén, D. Y. (2016). *Diseño De Un Sistema Integrado Gestión Basado En Las Normas Iso 9001: 2015 E Iso 27001: 2013 Para La Empresa La Casa Del Ingeniero Lci.* Escuela Colombian De Ingeniería Julio Garavito.

Luna, Y. B. (2015). *Auditoría Integral: Normas Y Procedimientos.* ECOE Ediciones.

Muñoz Razo, C. (2002). *Auditoría En Sistemas Computacionales.* México: Pearson Educación.

Infante-Moro, A., Infante-Moro, J. C., Martínez-López, F. J., García-Ordaz, M., & Gallardo - Fernández, M. (2017). *La Auditoría Informática En Las Grandes Empresas Españolas.* XIX Seminário Luso-Espanhol (SLE) De Economía Empresarial.

Proaño Escalante, R. A., Saguay Chafla, C. N., Jácome Canchig, S. B., & Sandoval Zambrano, F. (2017). *Sistemas Basados En Conocimiento Como Herramienta De Ayuda En La Auditoría De Sistemas De Información.* Enfoque UTE, 8, 148-159

Pulgarín Álvarez, A. P. (2016). *Auditoría Informática A La Empresa Ecua-Mails.* (Bachelor's Tesis, Quito: Universidad Israel, 2016).

Sánchez Gómez A. R. (2005, octubre 7). *Definición Genérica De Auditoría Y Sus Etapas.* Recuperado De: Http://www.Gestiopolis.Com/Definicion-Generica-Auditoria-Etapas/

Razo, C. M. (2002). *Auditoría en sistemas computacionales. Pearson Educación.:* Guía Para Su Implantación En Empresas Públicas Y Privadas. Ediciones De La U.

Redes Norma 568A (2012). *Redes Norma 568A.* Recuperado De: https://cableadoestrycturado.weebly.com/norma-eiatia-568a.html

Solarte, F. N. S., Rosero, E. R. E., & Del Carmen Benavides, M. (2015). *Metodología De Análisis Y Evaluación De Riesgos Aplicados A La Seguridad Informática Y De Información Bajo La Norma ISO/IEC 27001.* Revista Tecnológica-ESPOL, 28(5).

Soldevilla Paredes, J. (2014). *Auditoria I: Contabilidad Para Todos*, Aplicación Editorial Imprenta Unión De La Universidad Peruana Unión, Km19 Carretera Central, Ñaña, Lima-Perú. Recuperado De: Https://Drive.Google.Com/File/D/1fnpqbyujfgjzwzopfthtury6an3gtahe/View

Soto, M. D. C. S., Millán, N. D. C. O., Caro, M. S., & Garfias, J. I. M. (2018). *La Auditoría Informática En Las Organizaciones.* Revista Electrónica Sobre Cuerpos Académicos Y Grupos De Investigación, 4*(8).*

Speth, C. (2016). *El Análisis DAFO: Los Secretos Para Fortalecer Su Negocio.* 50minutos. Es.

Urbina, G. B. (2016). *Introducción A La Seguridad Informática.* Grupo Editorial Patria.

Valdiviezo, S. (2014). *Auditoría De Seguridad Física Y Lógica De Los Sistemas Informáticos A La Empresa Sumatex, De La Ciudad De Riobamba, Provincia De Chimborazo Por El Periodo 2012.* (Tesis De Pregrado, Escuela Superior Politécnica De Chimborazo), Obtenido De Http://Dspace.Espoch.Edu.Ec/Handle/123456789/5110

Valencia-Duque, F. J., & Orozco-Alzate, M. (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 Tecnologías De Información, (22), 73-88.

Veloz Chunata, J. M. (2015). *Auditoría Informática Al Gobierno Autónomo Descentralizado Municipal Del Cantón Penipe, Provincia De Chimborazo* (Tesis Inédita De Licenciatura) Politécnica Nacional De Chimborazo, Chimborazo, Ecuador.

Velthuis, M. G. P. (2008). *Auditoría De Tecnologías Y Sistemas De Información.* Grupo Editorial Ra-Ma.

Vieites, Á. G. (2013). *Tipos De Ataques E Intrusos En Las Redes Informáticas.* Línea]. Obtenido En: Http://Www. Edisa. Com/Wp-Content/Uploads/2014/08/Ponencia_-_Tipos_De_Ataques_Y_De_Intrusos_En_Las_Redes_Informaticas. Pdf. [Accedido: 09-Ago-2017].

Villena, J. C. (2019). *Auditoría Informática A La Unidad De Gestión Tecnológica Del Gobierno Autónomo Descentralizado Municipal Del Cantón San Pedro De Pelileo, Periodo, 2016* (Tesis De Pregrado, Escuela Superior Politécnica De Chimborazo), Obtenido De Http://Dspace.Espoch.Edu.Ec/Handle/123456789/9971

ANEXOS

Anexo A: Encuesta Aplicada al Personal Técnico de la Empresa Master Technology

ENCUESTA

Dirigida al personal técnico de la Empresa Master Technology

1. **¿El acceso al lugar donde se ubica servidor está restringido para el personal no autorizado?**

   SI_____

   NO_____

2. **El área de informática cuenta con las seguridades internas y externas.**

   SI_____

   POCO_____

   MUY POCO_____

   NINGUNA_____

3. **¿En caso de fallo de los sistemas informáticos la empresa cuenta con medidas de seguridad y respaldo de la información?**

   SI _____

   NO _____

   Cuales_____

4. **¿El servidor dispone de aire acondicionado para regular la temperatura?**

   SI_____

   NO_____

5. **¿El lugar donde se encuentra el Data Center cuenta con sensores de humo?**

   SI_____

   NO_____

6. **¿Los dispositivos electrónicos que se conectan a la red informática (celulares, computadores) de la empresa cuentan con programas de protección para evitar riesgos informáticos?**

   SI_____

   NO_____

Anexo B: Encuesta Aplicada al Personal Administrativo de la Empresa Master Technology

ENCUESTA

Dirigida al personal administrativo de la Empresa Master Technology

1. **¿El área informática cuenta con una salida de emergencia?**

   SI _____

   NO _____

2. **¿La señalética del área de informática es suficiente y se encuentra visible?**

   Si_____

   Poco_____

   Ninguna_____

3. **¿Usted ha participado en las capacitaciones institucionales relacionadas al área de informática?**

   SI _____

   NO _____

Anexo C: Encuesta Aplicada al Gerente Administrativo de la Empresa Master Technology

ENCUESTA

Dirigida al Gerente Administrativo de la Empresa Master Technology

1) **¿Los usuarios que ingresan al sistema cuentan con claves de acceso personal?**

SI_____

NO_____

2) **¿Se cuenta con los recursos informáticos necesarios para el buen funcionamiento del negocio?**

SI _____

NO _____

Desconozco_____

3) **¿La empresa cuenta con un plan estratégico establecido para la actualización de software de sus sistemas informáticos?**

SI _____

NO _____

En qué tiempo_____

4) **¿La empresa cuenta con un plan estratégico establecido para la actualización de sus sistemas informáticos físicos?**

SI _____

NO _____

En qué tiempo_____

5) **¿Se están destinando los recursos informáticos en las cantidades necesarias para cada área del negocio o empresa?**

SI _____

NO _____

Desconozco_____

6) **¿En caso de contar con un plan estratégico para la actualización de sus equipos informáticos, dentro de que periodo de tiempo de ejecutaría el mismo?**

a) De 1 a 3 años_____
b) De 3 a 5 años_____
c) De 5 a 7 años_____
d) De 7 a 10 años_____

7) **¿Los recursos informáticos pertenecientes a la empresa cuentan con póliza de seguros?**

SI _____
NO _____

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS PARA EL APRENDIZAJE Y LA INVESTIGACIÓN

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 20 / 11 / 2020

INFORMACIÓN DE LA AUTORA
Nombres – Apellidos: DIDIMA JOHANNA UCLES ROMO
INFORMACIÓN INSTITUCIONAL
Facultad: ADMINISTRACIÓN DE EMPRESAS
Carrera: INGENIERÍA CONTABILIDAD Y AUDITORÍA
Título a optar: INGENIERA EN CONTABILIDAD Y AUDITORÍA C.P.A
f. Analista de Biblioteca responsable: