1. Marco Referencial
   1. Concepto universal de auditoría.

Representa el examen de los estados financieros de una entidad, con el objeto de que el contador público independiente emita una opinión profesional respecto a si dichos estados representan la situación financiera, los resultados de la operaciones, las variaciones en el capital contable y los cambios en la situación financiera de una empresa, de acuerdo con los principios de contabilidad generalmente aceptados.

La auditoría representa el examen de los estados financieros de una entidad, con el fin de emitir una opinión sobre la razonabilidad de las cifras que de ellos emanen.

Aunque en la actualidad se realizan diversos tipos de auditoría, todos no llevan a emitir una opinión sobre algún registro, sistema, operación o actividad en particular o con fines específicos.

* 1. CONCEPTO DE AUDITORÍA EN INFORMATICA:

La Auditoría en informática se refiere a la revisión práctica que se realiza sobre los recursos informáticos con que cuenta una entidad con el fin de emitir un informe o dictamen sobre la situación en que se desarrollan y se utilizan esos recursos.

* + 1. Clasificación de la auditoría.

Tradicionalmente se consideran dos tipos de auditoría: las internas y las externas.

La auditoría interna la desarrollan personan que pueden o no depender de la entidad y actúan revisando, las más de las veces, aspectos que interesan particularmente a la administración, aunque pueden efectuar revisiones programadas sobre todos los aspectos operativos y de registro de la empresa, con el fin de emitir un informe sobre su revisión.

La auditoría externa, conocida también como auditoría independiente, la efectúan profesionistas que no dependen de la empresa, ni económicamente ni bajo cualquier otro concepto, y a los que se conoce un juicio imparcial merecedor de la confianza de terceros. El objeto de su trabajo es la emisión de un dictamen. Esta clase de auditoría es la actividad más característica del Contador Público o del Licenciado en Informática.

También existen otros tipos de auditoría como son:

* Auditoría operacional, se refiere a la revisión de la operación de una empresa y se juzga la eficiencia de la operación misma.
* Auditoría administrativa, se refiere a la organización y eficiencia de la estructura del personal con que cuenta la empresa y los procesos administrativos en que actúa dicho personal.
* Auditoría social.-se refiere a la revisión del entorno social en que se ubica y desarrolla una empresa, con el fin de valorar aspectos externos e internos que infieran en la productividad de la misma.
  + 1. IMPORTANCIA DE LA AUDITORÍA EN INFORMÁTICA.

Siempre ha existido la preocupación por parte de las organizaciones por optimizar todos los recursos con que cuenta la entidad, sin embargo por lo que respecta a la tecnología de informática, es decir, software, hardware, sistemas de información, investigación tecnológica, redes locales, bases de datos, ingeniería de software, telecomunicaciones, etc. esta representa una herramienta estratégica que representa rentabilidad y ventaja competitiva frente a sus similares en el mercado, en el ámbito de los sistemas de información y tecnología un alto porcentaje de las empresas tiene problemas en el manejo y control, tanto de los datos como de los elementos que almacena, procesa y distribuye.

El propósito de la revisión de la auditoría en informática, es el verificar que los recursos, es decir, información, energía, dinero, equipo, personal, programas de cómputo y materiales son adecuadamente coordinados y vigilados por la gerencia o por quien ellos designen.

Durante años se ha detectado el despilfarro de los recursos o uso inadecuado de los mismos, especialmente en informática, se ha mostrado interés por llegar por llegar a la meta sin importar el costo y los problemas de productividad.

* + 1. ANTECEDENTES DE LA AUDITORÍA EN INFORMATICA.

Sí bien la auditoría se ha llevado a cabo desde, que el hombre hizo su aparición, esta se llevaba de manera empírica, ha sido de gran ayuda para los pueblos conquistadores, ya que tenían que conocer y dar fe de los tributos que les rendían los pueblos conquistados, en México los “oidores” de la corona española, que con el paso del tiempo se transformarían en auditores, que vigilaban el pago de quinto real a los reyes de España.

La auditoría en informática es más reciente, se tiene como antecedente más cercano a los Estados Unidos de América. En los años cuarenta se empezaron a dar resultados relevantes en el campo de la computación, con sistemas de apoyos para estrategias militares, sin embargo, la seguridad y el control solo se limitaba a dar custodia física a los equipos y a permitir el uso de los mismos solo a personal altamente calificado.

Con el paso de los años la informática y todos los elementos tecnológicos, que la rodean han ido creando necesidades, en cada sector social y se han vuelto un requerimiento permanente para el logro de soluciones.

* + 1. Áreas a auditar en Informática

Las áreas a auditar en donde se puede realizar la auditoría en informática, puede ser:

* A toda la Entidad.
* A un departamento.
* A un área
* A una función
* A una subfunción.

Y se pueden aplicar los siguientes tipos de auditoría:

* Auditoría al ciclo de vida del desarrollo de un sistema
* Auditoría a un sistema en operación
* Auditoría a controles generales ( gestión)
* Auditoría a la administración de la función de informática.
* Auditoría a microcomputadoras aisladas
* Auditoría a redes.
  1. EL ESTANDAR COBIT
     1. HISTORIA

ISACF (Information System Audit and Control Fundation), es una asociación de profesionales, fundada en 1976 que tiene como objetivo realizar trabajos de investigación con el fin de incrementar el conocimiento y valor sobre el Control, Aseguramiento y Gobierno de la Tecnología de Información11. En 1998, se funda el Instituto de Gobierno de Tecnología de Información (IT Governance Institute), destinado a mejorar el entendimiento y promover la adopción de los principios del Gobierno de TI.

Para 1996, ISACF emite una publicación sobre Objetivos de Control para la información y tecnologías relacionas. Una segunda edición revisada y que agrega un Conjunto de Herramientas de Implementación fue liberada en 1998. COBIT (Control Objetives Information Tecnologies - Objetivo de Control para Tecnología de Información), constituye la tercera edición de los Objetivos de Control cuyo editor principal fue el Instituto de Gobierno de TI, creando así una herramienta de Gobierno de TI, que vincula la tecnología informática y prácticas de control, además consolida estándares de fuentes globales confiables en un recurso esencial para la administración (gerencia), los usuarios (profesionales de control) y los auditores.

COBIT está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

* + 1. MISIÓN

El organismo de Control y Auditoría, ISACA (Information Systems Audit And

Control Association) y el Comité Directivo de COBIT han definido la misión del estándar así: “Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores.”

* + 1. ALCANCE
* Orientado al negocio (Gerencia).
* Alineado con estándares y regulaciones de hecho y de derecho.
* Basado en normas revisadas crítica y analíticamente para ser aceptadas en las tareas y actividades de TI.
* Alineado con estándares de control y auditoría (COSO, IFAC, IIA, ISACA, AICPA).
* Aplicable a las funciones de Servicios de Sistemas de Información de toda la empresa.
  + 1. OBJETIVOS
* Proporcionar a la Gerencia de normas basadas en buenas prácticas para el control de la información y la Tecnología de la Información, lo que incluye a la seguridad informática. COBIT es la herramienta de Gobierno de TI que ayude al entendimiento y a la administración de los riesgos así como de los beneficios asociados con la información y sus tecnologías relacionadas.
* Dar a los usuarios una base confiable para administrar los recursos de TI.
* Proveer a los auditores de buenos criterios para las tareas de evaluación, control y auditoría.
* Suministrar a la Gerencia, responsables de procesos de negocio y auditores, el respaldo suficiente para mejorar la administración de la T.I. COBIT está diseñado para ser utilizado por los propietarios de los procesos de negocio como una guía clara y entendible para que estos tengan total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio.
  + 1. AUDIENCIA

Particularmente, se reconoce que COBIT puede ser útil para diferentes miembros o entes dentro de una organización, así:

La Gerencia: en lo referente a la toma de decisiones de inversión en TI y control, para analizar el costo-beneficio del control en un ambiente de riesgos impredecibles.

Los Usuarios Finales: para contar con una garantía sobre la seguridad, calidad y el control de los productos de TI internos y adquiridos.

Los Auditores: para apoyar sus opiniones sobre los controles de los proyectos de TI, su injerencia en la empresa y determinar el nivel de control requerido.

* + 1. ESTRUCTURA DEL ESTANDAR COBIT

El estándar consta principalmente de 4 libros que sirven como guía para alcanzar los objetivos planteados por la Administración, Usuarios y Auditores, además de un conjunto de Herramientas y Guías para ejecutar la implementación y soportar la administración.

* Resumen Ejecutivo
* Marco de Referencia
* Objetivos de Control
* Guías de Auditoría
* Herramientas de Implementación
* Guías de Administración
  + - 1. **Resumen Ejecutivo**

Provee a la Administración del conocimiento de los principios y conceptos esenciales de COBIT17. Ya que de ello depende el optimizar el empleo de los recursos disponibles (personal, instalaciones, sistemas de aplicaciones y datos) para cumplir con esta responsabilidad y alcanzar sus objetivos. La administración debe comprender el estado de sus propios sistemas de TI y decidir el nivel de seguridad y control que deben proveer estos sistemas.

* + - 1. **Marco de Referencia**

El Marco referencial COBIT se fundamenta en que el enfoque de control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio. La información es el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información, que deben ser administrados por procesos de TI. Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como Requerimientos de Negocio para la información.

COBIT ha definido los siguientes Requerimientos del Negocio:

* REQUERIMIENTOS DE CALIDAD: Calidad, Costo, Entrega de Servicio.
* REQUERIMIENTOS FIDUCIARIOS: Efectividad y Eficiencia de Operaciones, Confiabilidad de la Información, Cumplimiento de las Leyes y Regulaciones.
* REQUERIMIENTOS DE SEGURIDAD: Confidencialidad, Integridad, Disponibilidad.

La Calidad ha sido considerada por sus características de no fallas, confiabilidad, etc. lo que implica criterios de integridad. Está dirigida al manejo apropiado de los riesgos contra las oportunidades. El aspecto de calidad está cubierto por los criterios de efectividad. Se considera que el aspecto de entrega (de servicio) de la calidad se traslapa con el aspecto de disponibilidad correspondiente a los Requerimientos de Seguridad y también en alguna medida, con la efectividad y la eficiencia. Finalmente, el costo es también considerado que queda cubierto por la Eficiencia.

Para los Requerimientos Fiduciarios, se utilizaron las definiciones de COSO (Committee of Sponsoring Organisations of the Treadway Commisssion Internal

Control-Integrated Framewor) para la efectividad y eficiencia de operaciones, confiabilidad de información y cumplimiento con leyes y regulaciones. 22

Con respecto a los aspectos de seguridad, COBIT identificó la confidencialidad, integridad y disponibilidad como los elementos clave, que son los tres elementos utilizados a nivel mundial para describir los requerimientos de seguridad.

Comenzando el análisis a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad más amplios, se extrajeron siete categorías distintas.

El Marco Referencial se clasifica en tres niveles de actividades de TI al considerar la administración de sus recursos.

En la base se encuentran las actividades y las tareas necesarias para obtener un resultado medible. Los procesos se definen en un nivel superior como una serie de actividades o tareas conjuntas con cortes de control. En el nivel más alto, los procesos son agrupados en dominios. Su agrupamiento corresponde a la responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo aplicable a los procesos de TI.

**NIVELES DEL MARCO REFERENCIAL**

Básicamente, el Marco Referencial puede ser enfocado desde tres puntos clave: Los Criterios de Información, Los Recursos de TI, y Los Procesos de TI. Lo cual, se puede distinguir en el Cubo COBIT que se muestra a continuación.

**CUBO COBIT DE PUNTOS ESTRATÉGICOS**

Con lo anterior, se puede conocer en detalle los 34 Objetivos de Control de alto nivel, definidos para cada uno de los Procesos de TI, agrupados en cuatro dominios: Planeación y Organización, Adquisición e Implementación, Entrega de Servicios y, Soporte y Monitoreo.

Las definiciones para los Dominios identificados son:

Planeación y Organización

Se refiere a las estrategias y tácticas; a la manera como la Tecnología de Información apoya al logro de los objetivos de la empresa. Se añade también la necesidad de que la visión estratégica debe ser planeada, comunicada, y administrada desde diferentes puntos de vista.

Adquisición e Implementación

Para poner en ejecución la estrategia de TI, es necesario identificar las soluciones de TI, sean éstas desarrolladas o adquiridas, además deben ser implementadas e integradas dentro del proceso del negocio. Este dominio abarca también los cambios a sistemas existentes para asegurar la continuidad de su ciclo de vida.

Entrega y Soporte

Corresponde a la distribución y entrega de los servicios requeridos, lo que va desde las actividades cotidianas hasta el entrenamiento, sin dejar de lado la seguridad de los sistemas y la continuidad de las operaciones. Este dominio abarca los procesos a los que son sometidos los datos por los sistemas de aplicación.

Monitoreo

Se refiere a la necesidad de evaluar los procesos regularmente para asegurar su calidad y suficiencia con referencia a los requerimientos de control. Toma también en cuenta la necesidad de crear procesos de control independientes, generalmente estos son llevados a cabo por auditorías internas y externas.

* + - 1. **Objetivos de Control**

Objetivos de Control son la base del conjunto de conocimientos requerido para soportar la auditoría y control de los sistemas de información.

Los Objetivos de Control de TI han sido organizados por proceso/actividad y también se han proporcionados ayudas de navegación para facilitar la entrada a partir de cualquier punto de vista estratégico y para facilitar enfoques combinados o globales, tales como instalación/implementación de un proceso, responsabilidades gerenciales globales para un proceso y utilización de recursos de TI por un proceso.

Los Objetivos de Control se enfocan sobre objetivos de control detallados y específicos asociados a cada proceso de TI. Por cada uno de los 34 procesos de TI del marco referencial, hay desde tres hasta 30 objetivos de control detallados, para un total de 318.

* + - 1. **Guías o Directrices de Auditoría**

Las Directrices de Auditoría proporcionan guías para preparar planes de auditoría que se integran al Marco Referencial de COBIT y a los Objetivos de Control detallados. Deben ser usados conjuntamente con estos dos últimos, y a partir de ahí pueden desarrollarse programas específicos de auditoría.

Sin embargo, las Directrices no son exhaustivas ni definitivas. No pueden incluir todo ni ser aplicables a todo, así que deberán ajustarse a condiciones específicas.

La preparación de estos programas está basada en:

* Adquirir conocimiento a través de entrevistas
* Considerar y evaluar la conveniencia de los controles establecidos
* Valorar la suficiencia de los procesos
* Justificar el riesgo de que los objetivos de control no se alcancen.

Las Guías de Auditoría también existen para cada uno de los 34 objetivos de control, que permitirán la revisión de los procesos de TI contra los 318 objetivos de control detallados y que aseguran a la Gerencia el cumplimiento o mejoramiento de los mismos.

* + - 1. **Guías o Directrices Gerenciales o de Administración**

Estas directrices han sido desarrolladas recientemente y su objetivo es ayudar a la Gerencia a cumplir con las necesidades y requerimientos del Gobierno de TI de una manera más efectiva.

Estas directrices son:

* Factores Críticos de Éxito.- donde se definen las directrices más importantes que deben ser tomadas en cuenta por la Administración para tener el control sobre los procesos de TI.
* Modelo de Madurez.- para controlar los procesos de TI, y así la Administración pueda ubicar a su empresa en el entorno actual, con referencia a su competencia, en la industria, y con los estándares internacionales.
* Indicadores Clave por Objetivo.- donde se definen los mecanismos de valoración, que indicarán a la Gerencia si un proceso de TI ha satisfecho los requerimientos del negocio.
* Indicadores Claves de Desempeño.- son los indicadores principales que definen el valor para conocer que tan bien se está ejecutando un proceso de TI frente al objetivo que se busca.

Las Directrices Gerenciales son consistentes con y se basan en el Marco Referencial de COBIT, los Objetivos de Control y las Directrices de Auditoría de COBIT existentes.

* 1. NORMA TIA/EIA 568-B. Estándares de Cableado para Edificios Comerciales
     1. Definición

Especifica un sistema de cableado genérico a fin de proveer un sistema de transporte de información con redes externas por un medio común y establece los requisitos de funcionamiento para dicho sistema de cableado, como lo son:

* Requisitos de componentes
* Limitaciones de distancias de cableado
* Configuraciones de tomas / conectores
* Topología

* + 1. Premisas

Con la estructuración del sistema de cableado, se busca obtener los siguientes beneficios:

* Flexibilidad
* Asegurar compatibilidad de tecnologías
* Reducción de fallas
* Traslados, adiciones y cambios rápidos.
  + 1. Esquema Planteado

En este estándar se subdivide el sistema de cableado en seis Subsistemas:

* Subsistema Área de trabajo.
* Subsistema Horizontal.
* Subsistema Vertical o “Backbone” Ascendente.
* Subsistema de Administración.
* Subsistema de Sala de Equipos.
* Subsistema de “Campus”

Esta subdivisión tal y como se ilustra en la siguiente figura, es de tipo espacial en la cual están diferenciados los requerimientos y requisitos de componentes requeridos.

* + 1. Definiciones
       1. Área de trabajo

Se extiende desde la toma hasta el equipo del usuario. Se diseña de forma tal que permita realizar los traslados, adiciones y cambios fácilmente.

Deben diseñarse como mínimo dos tomas por cada área de trabajo:

* Una toma debe ser UTP de 100 Ohmios de cuatro pares (Categoría. 5e mínimo.
* „ La otra toma debe ser:
* Cable UTP de 100 Ohmios de cuatro pares (se recomienda mínimo Cat 5e).
* El cable STP de 150 Ohmios de dos pares.
* „ Cable de fibra óptica de 50/125 um de dos fibras(Conector SC o SFF)
  + - 1. **Conexiones**

Un aspecto muy importante dentro de la especificación de un cableado estructurado, son las conexiones, éstas permiten que el flujo de información desde el cuarto de telecomunicaciones hasta el usuario sea efectuado correctamente. Para que las conexiones sean seguras y confiables, es necesario el uso de accesorios de conexión tales como: contactos de desplazamiento de aislante, tomas, conectores, regletas, patch panels, cables, etc.

Los cables de conexión deben ser fabricados de múltiples hilos y deben llenar los mismos requerimientos que el cable horizontal con excepción de la atenuación.

* + - 1. **Normativa para la fabricación del cable de conexión**
* Se establecen prácticas de Cableado UTP, para ello deben destrenzarse los pares únicamente

1/2” para el cable de la Categoría 5 y 5e

 1” para los cables de las Categorías 3 y 4

* La tensión máxima para halar debe ser de 110N (25 lbf)
* Debe eliminarse la cubierta exterior sólo hasta donde se requiera para la terminación.
* Debe proveerse el código de color marcado y documentación que se requiera por el ANSI/TIA/EIA-606
  + 1. Cableado horizontal

Se define desde el área de trabajo hasta el cuarto de telecomunicaciones.

Incluye las tomas de información y los medios de transmisión tales como el cable, los accesorios de conexión y “Cross Connects”. Debe poseer las siguientes características:

* Debe ser topología estrella.
* Los componentes eléctricos específicos de aplicación, no deben ser instalados como parte del cableado horizontal. Si es necesario, deben estar expuestos.
*  Se permite un punto de transición en el cableado horizontal
*  Cable para uso bajo alfombra.
*  Punto de consolidación en oficina abierta
*  Cables aceptados en este tipo de cableado:
*  Cuatro pares, trenzado en pares, sin blindaje, 100 Ohmios (UTP)
*  Dos pares, trenzado en pares, blindado, 150 Ohmios (STP)
*  Cables de fibra óptica de 62.5/125 um de dos fibras.
  + 1. Cableado Vertical

Se define como la interconexión entre cuartos de cableado, áreas de trabajo, y acometidas. También incluye el cableado entre edificios.

Los cables aprobados en este tipo de cableado son:

* Cable multipar UTP de 100 Ohmios
* Cable STP de 150 Ohmios
* Cable de fibra óptica de 62.5/125um
* Cable de fibra Óptica Monomodo

 Las distancias máximas:

* UTP; 800 metros (para transmisión de voz solamente)
* STP; 700 metros (para transmisión de voz solamente)
* Fibra óptica multimodo: 2000 metros
* Fibra óptica Monomodo: 3000 metros

1. Situación Actual
   1. Descripción General de la Empresa

La empresa XX  es una empresa con sede en la ciudad de Asunción, con sucursales en la ciudad de Encarnación y en Hohenau, dedicada a la venta de ropa, franquiciada de la marca Hering.

La empresa ofrece una variedad de productos diferenciados cuyos consumidores meta son las personas que estén entra la edad de 1 a 35 años. La marca Hering es una marca reconocida a nivel internacional por su calidad y por sus colecciones en sintonía con las tendencias actuales, manteniendo su identidad y tradición.

* 1. Misión

Desarrollar marcas, crear y vender productos y servicios de ropa con valor percibido y atención al cliente.

* 1. Visión

Ser reconocida como la más rentable y mejor gestión de las marcas de ropa.

* 1. Descripción Organizacional

Para el departamento de Itapúa la organización cuenta con una Coordinación Regional, que coordina y supervisa las sucursales del departamento.

La sucursal a ser auditada cuenta con una gerencia, un salón de ventas y un depósito.

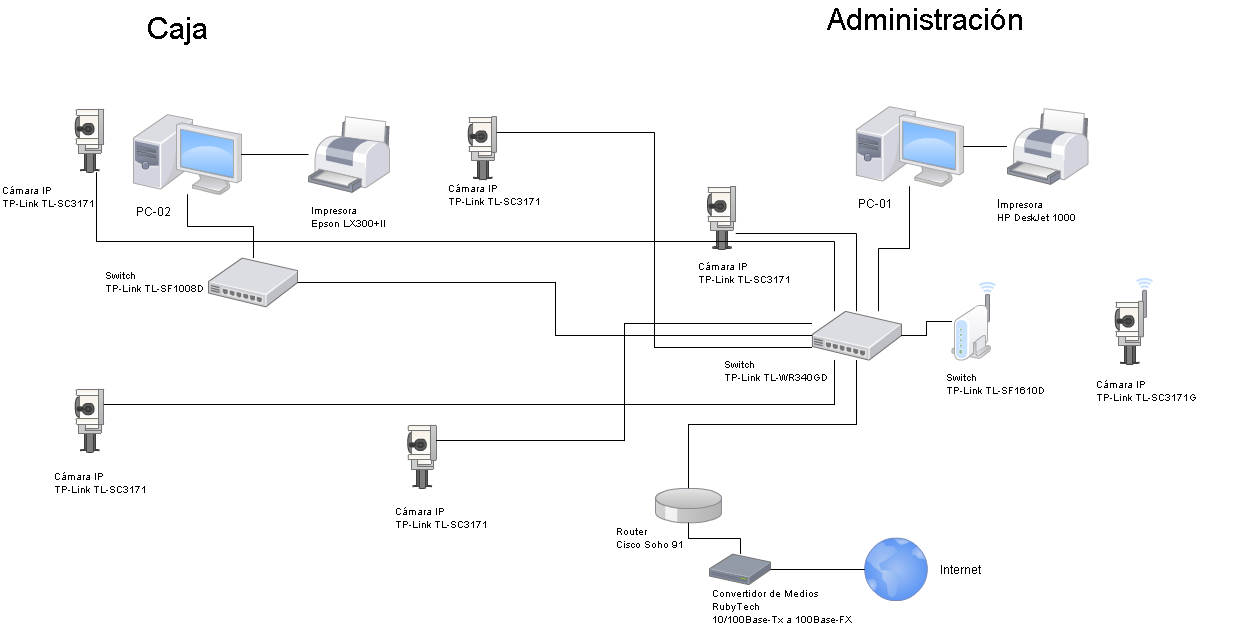
A continuación se presenta el Organigrama de la sucursal:

El plantel de empleados está compuesto de la siguiente manera:

* 1 (Una) Coordinadora Regional
* 1 (Una) Gerente
* 6 (Seis) Vendedoras
* 1 (Un) Depositero
* 1 (Un) Limpiadora

1. Infraestructura de la Red
   1. Inventario de hardware y software

* 1 (Un) Convertidor de Medios RubyTech. Caract.: 10/100 Base-TX a 100 Base-FX
* 1 (Un) Router Cisco Soho 91. Caract.: 4 Puertos.
* 1 (Un) Switch TP-Link TL-SF1610D. Caract.: 16 puertos.
* 1 (Un) Switch WIFI TP-Link TL-WR340GD. Caract.: 4 puertos.
* 1 (Una) PC (PC-1). Caract.: Pentium DualCore E5700 3.00 GHz 1.96 GB de RAM. S.O.: Microsoft Windows XP Professional 2002-Service Pack 3. Antivirus: Kaspersky 2013 Internet Security.
* 1 (Una) PC (PC-2). Caract.: Pentium DualCore E5800 3.2GHz 4GB de RAM. S.O.: Microsoft Windows 7 Professional 2009-Service Pack 1. Antivirus: Kaspersky 2013 Internet Security.
* 1 (Una) Impresora HP DeskJet 1000.
* 1 (Una) Impresora Epson LX300+II.
* 5 (Cinco) Cámaras de vigilancia IP TP-Link TL-SC3171.
* 1 (Una) Cámara de vigilancia IP inalámbrica TP-Link TL-SC3171G.
  1. Diagrama de la Red



1. Análisis de Riesgos
   1. Definición

El análisis de Riesgos trata sobre como minimizar los efectos de un problema de seguridad; para esto se debe tener identificado claramente qué es lo se quiere proteger, contra qué, y cómo se lo va a proteger.

Se conocen dos alternativas para responder a estas inquietudes, una cuantitativa y otra cualitativa.

La cuantitativa se basa en cálculos complejos que implica la probabilidad de que un suceso ocurra y una estimación a las pérdidas en caso de que éste se de; el llamado “Coste Anual Estimado”, se obtiene del productos de estos términos, (EAC, Estimated Annual Cost), sin embargo, la inexactitud en el cálculo, a menudo hace difícil que esta alternativa sea tomada en cuenta.

El segundo método de análisis de riesgos es el cualitativo, últimamente muy difundido por las llamadas “consultoras de seguridad”, que se especializan en seguridad lógica, cortafuegos, tests de infiltración y similares. Este método toma en consideración realizar estimaciones de pérdidas potenciales, para lo cual relacionan cuatro puntos importantes:

* Las amenazas
* Las vulnerabilidades
* El impacto asociado a una amenaza
* Los controles o salvaguardas.

Con estos cuatro elementos se puede obtener un indicador cualitativo del nivel de riesgo asociado a un activo determinado dentro de la organización, visto como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

* 1. Evaluación de riesgos de la gestión de seguridad en la red

COBIT se sustenta en varias fuentes para la definición de su estándar, tales como normas, estándares y programas que cuentan con auspicio del gobierno de los Estados Unidos, entre ellos el Instituto de Estándares y Tecnología (NIST), del cual se tomará uno de los documentos emitidos como base para la realización del Análisis de Riesgos.

* 1. Metodología NIST800-30 para la Administración de Riesgos

“La Administración de Riesgos es el proceso de identificar, evaluar y ejecutar acciones para reducir el riesgo a un nivel aceptable”.

El Instituto de Estándares y Tecnología (NIST) liberó su publicación especial 800- 30 con recomendaciones para la administración de riesgo para los sistemas de información del cual se tomará los nueve pasos sugeridos para una correcta evaluación de riesgos. Estos son:

* Paso 1. Caracterización del Sistema.
* Paso 2. Identificación de la Amenaza.
* Paso 3. Identificación de Vulnerabilidad.
* Paso 4. Análisis del Control.
* Paso 5. Determinación de Probabilidad.
* Paso 6. Análisis del Impacto.
* Paso 7. Determinación del Riesgo.
* Paso 8. Recomendaciones de los Controles.
* Paso 9. Documentación de los Resultados.
  1. Identificación de Amenazas y Vulnerabilidades

Luego de identificados los recursos a proteger se deben identificar las vulnerabilidades y amenazas a que están expuestos. Una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

Las amenazas se catalogan en diferentes grupos según su impacto sobre los sistemas informáticos y la forma como se producen:

* + 1. Desastres del entorno

Se refieren a problemas relacionados con la ubicación del entorno de trabajo informático o de la propia organización, así como con las personas que de una u otra forma están relacionadas con el mismo. Se toman en cuenta desastres naturales (terremotos, inundaciones, etc.), desastres producidos por elementos cercanos, como los cortes de fluido eléctrico, y peligros relacionados con operadores, programadores o usuarios del sistema.

* + 1. Amenazas en el sistema

Se refieren a todas las vulnerabilidades de los equipos y su software que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, medidas de protección que éste ofrece, fallos en los programas, copias de seguridad, etc.

* + 1. Amenazas en la red

Se debe tener en cuenta los aspectos relativos al cifrado de los datos que son sujetos de transmisión, protección de una red local de la Internet, sistemas de autenticación de usuarios remotos que accedan a ciertos recursos de la red interna.

Cabe anotar que para el análisis de las amenazas no solo se deben tomar en cuenta a los posibles atacantes externos (piratas informáticos, crakers) a la organización, sino que en la mayoría de los casos los potenciales ataques vienen desde el interior de la organización, debido principalmente a los pocos conocimientos sobre sistemas informáticos, seguridades y el trabajo en red básicamente.

Por otro lado, están también los actos accidentales, producidos por los mismos usuarios como pueden ser los borrados accidentales, fallas de programación, desconexión de cables de energía, etc.

* 1. Identificación de Amenazas

Previamente, se tendrán claramente definidos los conceptos de:

Amenaza: Posibilidad de ejercer de forma accidental o intencional una vulnerabilidad.

Vulnerabilidad: Debilidad que puede ser accidental o intencionalmente explotada.

Así, las posibles amenazas identificadas dentro de la red de datos de la empresa auditada son:

* + 1. Amenazas naturales
* Tormentas eléctricas.
  + 1. Amenazas humanas
* Acciones no intencionales como: Ingreso inadvertido de datos, mal uso de recursos.
* Acciones deliberadas como: ataques a la red, acceso no autorizado a información confidencial.
  + 1. Amenazas Medioambientales
* Falla en el Servicio de Energía.
* Falla en el Sistema de Comunicaciones.
* Falla de equipos y aplicaciones.
  1. Identificación de Vulnerabilidades
* No existe un documento específico de políticas de seguridad de TI.
* No existe un acuerdo de confidencialidad entre la empresa y el servicio técnico.
* No existe un plan de clasificación de información o en su lugar una pauta que tome parte en la determinación de cómo la información debe ser manipulada y protegida.
* No existe una acuerdo de confidencialidad o de no revelación de la información como parte de los términos y condiciones iniciales del empleo para el personal.
* No existe un procedimiento para verificar todos los boletines de advertencia e informativos con respecto al uso de software malicioso.
* No existe un procedimiento formal para reportar los incidentes que puedan presentarse en la red por los canales de administración apropiados tan pronto como sea posible.
* Los medios de respaldo y los procedimientos para su restauración no están guardados en un lugar seguro y lejos del sitio actual.
* No existe un procedimiento para el monitoreo y control del uso de los recursos de TI por parte los empleados.
* No existe un plan de contingencia establecido en caso de falla de equipos críticos para las operaciones del negocio.
* No existe un documento formal para el registro de la entrega o retiro de recursos de TI al personal.
* No hay respaldo para el fallo de equipos críticos.
* La BD no se encuentra almacenada en un sector restringido de la empresa.
* Los archivos de la empresa no se encuentran protegidos por contraseña.
* El firewall se encuentra desactivado.
* La licencia del antivirus ha caducado.
* El SO de unos de los terminales ya no cuenta con soporte ni actualizaciones.
* Existe una sobrecarga de conexiones en un solo tomacorrientes
* No existe un procedimiento de revisión periódica de archivos logs de los equipos.
* Las conexiones físicas de la red local no se encuentran adecuadamente estructuradas.
* Los usuarios no guardan confidencialidad de sus cuentas y passwords.
  1. Probabilidad de Impacto de la Amenaza

Para la definición de la probabilidad que una amenaza afecte a una vulnerabilidad se tomó como referencia la tabla de la NIST.

* + 1. DEFINICION DE PROBABILIDADES

|  |  |  |
| --- | --- | --- |
| **Nivel de Probabilidad** | **Ponderación** | **Definición** |
| Alto | 3 | El origen de amenaza es altamente motivado y suficientemente capaz, y los controles para prevenir que se ejerza la vulnerabilidad son ineficaces. |
| Medio | 2 | El origen de amenaza es motivado y capaz, pero los controles presentes pueden impedir que se ejerza con éxito la vulnerabilidad. |
| Bajo | 1 | El origen de amenaza carece de motivación o capacidad, existen controles para prevenir o por lo menos para impedir significativamente que se ejerza la vulnerabilidad. |

De igual manera para la definición del impacto se consideró la tabla proporcionada por la NIST que define la magnitud del impacto en niveles alto, medio y bajo. Cabe notar que para la definición de estos niveles se toma en cuenta los siguientes criterios de seguridad: integridad, disponibilidad y confidencialidad.

* + 1. Definición de la magnitud del impacto

|  |  |  |
| --- | --- | --- |
| **Magnitud del Impacto** | **Ponderación** | **Definición** |
| Alto | 3 | (1) puede producir la pérdida costosa de recursos; |
|  |  | (2) puede dañar significativamente o impedir una misión de organización, su reputación o intereses; o |
|  |  | (3) puede resultar muerte o la lesión seria del personal. |
| Medio | 2 | (1) puede producir la pérdida costosa de activos tangibles o recursos; |
|  |  | (2) puede dañar, o puede impedir la misión de la organización, su reputación o intereses; o |
|  |  | (3) puede resultar en lesión del personal. |
| Bajo | 1 | (1) puede producir la pérdida de algunos recursos tangibles o recursos o |
|  |  | (2) puede afectar notablemente la misión de la organización, su reputación, o intereses. |

* 1. Determinación del Riesgo

La siguiente matriz se obtiene del producto entre los niveles de Probabilidad e Impacto definidos anteriormente, para conocer el riesgo que se aplica a la amenaza:

* + 1. MATRIZ DE PONDERACION DE RIESGOS

|  |  |  |  |
| --- | --- | --- | --- |
| Probabilidad de la Amenaza | Impacto de la Amenaza | | |
| Bajo (1) | Medio (2) | Alto (3) |
| Alto (3) | BAJO : 3 x 1 = 3 | MEDIO : 3 x 2 = 6 | ALTO : 3 x 3 = 9 |
| Medio (2) | BAJO : 2 x 1 = 2 | MEDIO : 2 x 2 = 4 | MEDIO : 2 x 3 = 6 |
| Bajo (1) | BAJO : 1 x 1 = 1 | BAJO : 1 x 2 = 2 | BAJO : 1 x 3 = 3 |

* 1. Resultado de la Evaluación del Riesgo

A continuación se presenta la Matriz de Evaluación de Riesgos, en donde se analizan cada uno de los recursos identificados considerados críticos, para cada uno de ellos se reconocen amenazas y vulnerabilidades, el control existente, su posible impacto y probabilidad de ocurrencia se reconoce a partir de la entrevista con el encargado de la sucursal y del checklist aplicado, el nivel de riesgo se obtiene de la aplicación de la matriz de ponderación anterior y finalmente se proponen las recomendaciones necesarias para alcanzar un control considerable.

* + 1. MATRIZ DE EVALUACION DE RIESGOS

| **Recurso** | **Amenaza** | **Vulnerabilidad** | **Control Existente** | **Impacto** | **Probabilidad** | **Nivel de Riesgo** | **Recomendación** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Equipos de conexión de Red y PC | Mal uso de recursos | No existe un documento específico de políticas de seguridad de TI. | Ninguno | Alto | Media | Medio | Definir un documento de políticas de seguridad para TI. |
| Equipos de conexión de Red y PC | Acceso no autorizado a información confidencial. | No existe un documento específico de políticas de seguridad de TI. | Ninguno | Medio | Media | Medio | Definir un documento de políticas de seguridad para TI. |
| Equipos de conexión de Red y PC | Acceso no autorizado | No existe un documento específico de políticas de seguridad de TI. | Ninguno | Alto | Media | Medio | Definir un documento de políticas de seguridad para TI. |
| Aplicaciones de red (Sistema) | Ingreso inadvertido o mal intencionado a datos | Las cuentas utilizadas en este sistema son creadas por área no por usuario. | Ninguno | Alto | Alta | Alto | Definir que la creación de cuentas y sus perfiles sea por empleado. |
| Aplicaciones de red (Sistema) | Acceso no autorizado a información confidencial | Los usuarios no guardan confidencialidad de sus cuentas y passwords. | Los usuarios conocen su responsabilidad sobre la no divulgación de sus cuentas. | Alto | Baja | Bajo | Reforzar la conciencia de responsabilidad de los usuarios sobre el uso de sus cuentas. |
| Aplicaciones de red (Sistema) | Ingreso inadvertido de datos | Definición o asignación errónea de perfiles de usuario. | Ninguno | Alto | Baja | Bajo | Revisión periódica de las cuentas existentes y sus perfiles. |
| Equipos de conexión de Red y PC | Acceso no autorizado a información confidencial | No existe una política de requerimientos de seguridad en contratos con terceros. | Ninguno | Alto | Media | Medio | Añadir cláusulas de confidencialidad de la información en los contratos establecidos con compañías externas. |
| Equipos de Circuito Cerrado | Acceso no autorizado a información confidencial | No existe una política de requerimientos de seguridad en contratos con terceros. | Ninguno | Alto | Media | Medio | Añadir cláusulas de confidencialidad de la información en los contratos establecidos con compañías externas. |
| Aplicaciones de red (Sistema) | Mal uso de recursos y acceso no autorizado | No existe un plan de clasificación de información o una pauta que tome parte en la determinación de cómo la información debe ser manipulada y protegida. | La información considerada clave para un usuario es almacenada en una PC, sin controles de acceso restringido. | Alto | Media | Medio | Elaborar el plan de clasificación de la información y dar a conocer a los involucrados. |
| Aplicaciones de red (Sistema) | Mal uso de recursos y acceso no autorizado | No existe una acuerdo de confidencialidad o de no revelación de la información como parte de los términos y condiciones iniciales del empleo para el personal. | Ninguno | Medio | Alta | Medio | Elaborar un acuerdo de confidencialidad que sea parte de contrato de empleo. |
| Servidor (Pen drive) | Ataque a la red | No existe un procedimiento formal para reportar los incidentes de seguridad por los canales de administración apropiados tan pronto como sea posible. | Reportes informales | Alto | Media | Medio | Establecer un procedimiento de formal para reportar incidentes de seguridad. |
| Servidor (Pen drive) | Mal uso de recursos | No existe un servidor dedicado donde sea almacenado el sistema principal | Almacenado en una unidad extraíble (pen drive) | Alto | Alta | Alto | Adquirir un equipo destinado al almacenamiento del sistema. |
| Servidor (Circuito Cerrado) | Mal uso de recursos | No existe un servidor especifico donde sea almacenado el sistema principal | Almacenado en una PC de uso diario | Alto | Alta | Alto | Adquirir un equipo destinado al almacenamiento de las grabaciones del circuito cerrado. |
| Servidor (Pen drive) | Acceso no autorizado a información confidencial | No existe un procedimiento formal para reportar los incidentes de seguridad por los canales de administración apropiados tan pronto como sea posible. | Reportes informales | Alto | Media | Medio | Establecer un procedimiento de formal para reportar incidentes de seguridad. |
| Equipos de conexión de Red | Ataque a la red y mal uso de recursos | No existe un procedimiento formal para reportar los incidentes de seguridad por los canales de administración apropiados tan pronto como sea posible. | Reportes informales | Alto | Media | Medio | Establecer un procedimiento de formal para reportar incidentes de seguridad. |
| PC | Carga de software malicioso | La licencia del antivirus ha caducado. | Ninguno | Medio | Media | Medio | Adquirir licencias para cada equipo. |
| PC | Carga de software malicioso | El firewall se encuentra desactivado. | Ninguno | Medio | Media | Medio | Activar el firewall de cada equipo y realizar actualizaciones periódicas. |
| Servidor (Pen drive, Circuito Cerrado) y PC | Mal uso de recursos | Los medios de respaldo y los procedimientos para su restauración no están guardados en un lugar seguro y lejos del sitio actual. | Algunos respaldos existen pero se guardan dentro de la oficina. No existen procedimientos de restauración. | Alto | Media | Medio | Almacenar los respaldos en un lugar externo a la empresa. Establecer procedimientos de restauración de datos. |
| PC | Mal uso de recursos | No existe un procedimiento para el monitoreo y control del uso de los recursos de TI por parte los empleados. | Ninguno | Medio | Alta | Medio | Definir un documento para monitorear el uso de los recursos de TI. |
| Servicio de Internet | Mal uso de recursos | No existe un procedimiento para el monitoreo y control del uso de los recursos de TI por parte los empleados. | Ninguno | Medio | Alta | Medio | Definir un documento para monitorear el uso de los recursos de TI. |
| Servidor, PC, Servicio de Internet, Equipos de Conexión de Red, Equipos de Circuito Cerrado | Tormentas Eléctricas | No existe un plan de contingencia. | Ninguno | Alto | Alta | Alto | Establecer un plan de contingencia que contemple amenazas naturales. |
| Servidor, Equipos de Conexión de Red, Equipos de Circuito Cerrado | Ataque a la red | No existe un plan de contingencia. | Ninguno | Alto | Alta | Alto | Establecer un plan de contingencia que contemple este tipo de amenazas. |
| Aplicaciones en red | Ataque a la red | No existe un plan de contingencia. | Ninguno | Alto | Alta | Alto | Establecer un plan de contingencia que contemple este tipo de amenazas. |
| Sistema de UPS | Falla en servicio de energía. | No existe un plan de contingencia. | El sistema de UPS actual es casi obsoleto. | Alto | Media | Medio | Crear un plan de contingencia para cubrir este tipo de amenazas. Adquirir nuevos equipos. |
| Servicio de Internet | Falla en el sistema de comunicaciones. | No existe un plan de contingencia. | Ninguno | Alto | Media | Medio | Establecer un plan de contingencia que contemple este tipo de amenazas. |
| PC, Equipos de conexión de Red y Equipos de Circuito Cerrado | Mal uso de recursos. | No existe un documento formal para el registro de la entrega o retiro de recursos de TI al personal o terceros. | Ninguno | Bajo | Baja | Bajo | Elaborar un documento de entrega y recepción de recursos. |
| Servidor, PC, Equipos de Conexión de Red, Equipos de Circuito Cerrado | Falla de equipos y aplicaciones. | No hay respaldo para el fallo de equipos críticos. | Ninguno | Alto | Media | Medio | Adquirir equipos de respaldo. |
| Servidor | Ataque a la red, mal uso de recursos y carga de software malicioso. | No existe un procedimiento de revisión periódica de archivos logs de los equipos. | Ninguno | Bajo | Baja | Bajo | Definir un procedimiento para la revisión periódica de los logs. |
| Servidor (Pendrive) | Mal uso de recursos. | La BD no se encuentra en un lugar restringido de la empresa. | La BD está almacenada en un equipo con acceso a funcionarios | Alto | Alta | Alto | Almacenar la BD en un lugar restringido con acceso solo a personal autorizado. |
| PC, Equipos de conexión de Red | Mal uso de recursos. | Los archivos de la empresa no se encuentran protegidos por contraseña. | Ninguno | Alto | Media | Medio | Definir políticas para la creación de contraseñas seguras de los archivos de la empresa. |
| Correo Electrónico | Mal uso de recursos. | No existe un procedimiento formal para el monitoreo y control del uso del recurso. | Ninguno | Medio | Alta | Medio | Definir políticas sobre uso de correo, negar envío de cadenas, de información no laboral, posible fuente de virus y pérdida de datos. |
| Servicio de Internet | Mal uso de recursos. | No existe un procedimiento formal para el monitoreo y control del uso del recurso. | Ninguno | Medio | Alta | Medio | Definir nuevas políticas sobre uso de internet, restringir el acceso, posible fuente de virus y pérdida de datos. |
| PC | Mal uso de recursos. | El SO de uno de los terminales ya no cuenta con soporte ni actualizaciones. | Ninguno | Medio | Media | Medio | Actualizar el SO de los equipos y adquirir las licencias correspondientes. |
| PC, Equipos de conexión de Red | Mal uso de recursos. | Existe una sobrecarga de conexiones en un solo tomacorrientes | Ninguno | Alto | Media | Medio | Realizar un reordenamiento de las conexiones eléctricas. |
| PC, Equipos de conexión de Red | Mal uso de recursos. | Las conexiones físicas de la red local no se encuentran adecuadamente estructuradas. | Ninguno | Alto | Media | Medio | Reestructurar el cableado de la red local, canaletear y adquirir un Rack para los equipos de conexión de red. |

1. Plan de Auditoría Informática
   1. Alcance de la Auditoría

La presente auditoría aplicará COBIT 4.1 como metodología para la evaluación y análisis de los diferentes procesos y controles que se aplican en el área de la tecnología de la información.

A pesar de que COBIT es una herramienta que trabaja conjuntamente con los objetivos principales de la organización, la auditoría se centrara en:

* Análisis de la estructura física y lógica de la red y;
* Los métodos de respaldo de la información (backups) de la empresa.
  1. Objetivos
* Verificar la existencia de controles de confiabilidad, protección y disponibilidad de la información, basados en los siguientes objetivos de control de COBIT: DS4.9, DS11.3, DS11.
* Evaluar el estado del cableado de la red interna, basado en los estándares TIA/EIA 568-B.
* Verificar el uso de técnicas de seguridad en la red, basado en el objetivo de control de COBIT DS5.10 y el capítulo 13 del estándar ISO 27002
  1. Justificación

La empresa diariamente genera, maneja y distribuye información de vital importancia para la continuidad de las operaciones del negocio. Así mismo maneja informaciones confidenciales como información personal de los clientes, informaciones proveídas por la empresa franquiciadora e informaciones relevantes a costos, proveedores y datos bancarios propios de la empresa entre otras.

Dada la relevancia de la disponibilidad, confiabilidad y protección de la información y de los canales de distribución surge la necesidad de realizar esta auditoría a los equipos pertenecientes a la red interna de la sucursal para minimizar los riesgos de pérdida, fuga o adulteración de la información.

* 1. Recursos

Donde se identifican todos los recursos cuya integridad pueda ser amenazada de cualquier forma:

* Hardware: Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, computadores, personales, impresoras, unidades de disco, líneas de comunicación, servidores, routers.
* Software: Códigos fuente y objeto de aplicaciones, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicación, aplicaciones cliente-servidor.
* Información: En ejecución, almacenada en línea, almacenada fuera de línea, en comunicación, bases de datos.
* Personas: Usuarios, operadores, administradores.
* Accesorios: Papel, cintas, tóners, CD´s.

A continuación los recursos que serán utilizados para la realización de la presente auditoría:

* Recursos Humanos: El equipo de auditoría estará conformado por dos personas
* Hardware: Dos Notebooks, smartphones, impresora, cámara fotográfica.
* Accesorios: Cuaderno de Anotaciones, Bolígrafo.
* Software: Microsoft Office, Web cacoo.com
* Información: Estándar COBIT 4.1, EIA/TIA 568-B, ISO 27002
  1. Plan de Trabajo

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Etapa | Tarea | Documentos y/o herramientas utilizadas | Responsables | Periodo |
| Estudio Preliminar | Visita a la sucursal para recabar informaciones iniciales y presentación de los auditores | Cámara Fotográfica, Agenda y bolígrafo | Rubén Bordón  Roque Ocampo | 31-03 al |
| Elaboración del cuestionario para la primera entrevista | MS Word 2007 y Modelos de cuestionarios | Roque Ocampo |  |
| Entrevista a la Coordinadora Regional y a la Gerente | Agenda y bolígrafo | Rubén Bordón |  |
| Elaboración del Acuerdo de Confidencialidad | MS Word 2007 y Modelos de Acuerdos de Confidencialidad | Rubén Bordón  Roque Ocampo |  |
| Visita para recopilar informaciones acerca de la estructura de la empresa, cargos, funciones y responsabilidades de los empleados del área a ser auditada |  | Rubén Bordón  Roque Ocampo |  |
| Elaboración del Proyecto | Definición del alcance y los objetivos |  | Rubén Bordón  Roque Ocampo |  |
|  | Redacción del Marco Referencial |  | Roque Ocampo |  |
|  | Redacción de la Descripción de la Empresa |  | Rubén Bordón |  |
|  | Determinación de los Recursos para la realización de la auditoría informática |  | Rubén Bordón  Roque Ocampo |  |
|  | Elaboración del Análisis de Riesgo |  | Rubén Bordón  Roque Ocampo |  |
|  |  |  |  |  |
|  |  |  |  |  |
| * + Redacción del Análisis de Riesgos * Desarrollo de la Auditoria   + Relevamiento de datos * Entrevistas y Encuestas   + Entrevista a Patrick Godefroid (Gerente de la empresa)   + Encuesta y entrevista informal a Carolina Godefroid (Usuario del sistema y Encargada de la sucursal)   + Encuesta y entrevista informal a Graciela Maidana(Usuario del sistema y Secretaria)   + Análisis de las evidencias obtenidas en las encuestas   + Evaluación del proceso de datos y de los equipos de cómputos   + Seguridad de los datos   + Control de operación   + Seguridad física   + Procedimientos de respaldo.   + Diseñar casos de prueba para aplicar a las tablas de ventas de la BD   + Ejecución de las pruebas sobre el modulo de ventas de la BD   + Prueba de duplicados de los números de las facturas.   + Comparación de montos totales de los talonarios con el rango correspondiente en la base de datos   + Correlatividad de las fechas   + Correlatividad de los números de facturas   + Importe total negativo   + Números de facturas faltantes (gap) * Revisión e informe * Determinación del diagnostico e implicancias * Elaboración de la carta de gerencia * Elaboración del borrador del informe * Elaboración final del informe * Presentación del informe final |  |  |  |  |