

**UNIVERSIDAD POLITÉCNICA DE NICARAGUA**

**“Sirviendo a la comunidad”**



**ESCUELA DE ADMINISTRACIÓN, COMERCIO Y FINANZAS**

**Maestría en Auditoría Integral Versión V**

**TESIS DE MAESTRIA**

**Tema: Diagnóstico del Desempeño del Sistema de Facturación en la Distribuidora Tropical del Pacífico S.A, en el primer trimestre del año 2013.**

**Autor:**

**Ing. Katherine Yunieth Orozco Sánchez**

**Tutor:**

**Msc. Sandra Sanchez Vilchez**

**Managua, Septiembre 2014**

## DEDICATORIA

Agradezco primero a Dios, “Porque Dios da la sabiduría, y de su boca viene el conocimiento y la inteligencia.” (Proverbios 2:6).

A mi madre que me ha apoyado en cada instante de mi vida, que se ha esforzado junto a mí en el logro de esta meta, que ha sido la muestra fiel de que con perseverancia, trabajo y esfuerzo se puede lograr cualquier cosa en la vida y que junto a mi abuela me enseñó los valores más importantes de la vida, se los dedico a ustedes que son el motor de mi vida. Son mi ejemplo a seguir.

A mis hijos que amo con todo mi ser, Derek Jeshua y Sarah Kathleen González Orozco.

## AGRADECIMIENTOS

Le agradezco en primer lugar a Dios, que me ha protegido y siempre ha estado presente en todos los momentos de mi vida. Gracias mi Dios por ayudarme a lograr esta meta.

A mi madre que siempre está conmigo apoyándome, aconsejándome e impulsándome a seguir siempre adelante.

A mi tutora Msc. Sandra Sánchez Vílchez por darle minucioso seguimiento a la elaboración de la presente tesis.

Al profesor Phd. Israel Benavidez por su valioso asesoramiento en el desarrollo inicial de esta tesis.

A mi esposo el Ing. Virgilio González por haber emprendido y culminado a mi lado esta etapa de nuestra vida.

## RESUMEN EJECUTIVO

La presente tesis consiste en desarrollar un diagnóstico del desempeño del Sistema de Facturación en la Distribuidora Tropical del Pacífico, S.A, en el primer trimestre del año 2013, por medio de un análisis técnico, utilizando como base Normas internacionales de seguridad de sistemas para evaluar su arquitectura y sus componentes de seguridad, con el objetivo de identificar la confiabilidad, integridad y disponibilidad de la información que se procesa, intercambia, reproduce y conserva, mediante el uso del Sistema en referencia y determinar si es factible su conexión a otros puntos de ventas u optar por la adquisición de un nuevo software que cumpla con las necesidades de ampliarse a nivel de red corporativa.

La Distribuidora Tropical del Pacífico, S.A, en los aspectos organizativos evaluados, tiene identificada como fortalezas, una Estructura orgánica y Marco normativo esencial, formalmente establecido, posee un alto componente de posicionamiento en el mercado por casi 18 años y está fundada en valores de servicio al cliente con honestidad, calidad y mejora continua.

Como parte del Diagnóstico al Sistema de Facturación, se analizó su arquitectura informática, fue desarrollada en la herramienta de Visual Basic 6.0 y Ms Access como gestor de base de datos, y se concluyó que no es posible que el Sistema en estudio, pueda conectarse a otros puestos de comercialización porque solo opera a nivel de red local, siendo necesario la compra o desarrollo de un nuevo software dinámico, moderno, flexible, seguro y robusto.

En lo que respecta al análisis de la seguridad del Sistema, se identificó una frágil estructura de seguridad, no existen bitácoras y pistas de auditoría informática, siendo una limitante de alta importancia, porque muy difícilmente se podría identificar un posible crimen cibernético. Por tal razón, se recomendó el diseño de pistas de auditoría de eventos de monitoreo, esenciales para prevenir o identificar fraudes por el sistema de facturación analizado.

Como parte del análisis de riesgos, se identificó 20 escenarios de riesgos, de los cuales 11 tienen mayor exposición al riesgo. Las causas identificadas fueron: Fallas en controles internos; Errores humanos (mala digitación, omisión o falta de capacitación); Acciones fraudulentas y Amenazas externas a la Distribuidora (colusión para robos).

La premisa subyacente en la gestión de riesgos, es que todas las organizaciones enfrentan esta incertidumbre y la Distribuidora analizada, no es ajena a esta situación, siendo importante valorar la vulnerabilidad identificada a fin de fortalecer los aspectos que son sensibles para su mitigación.

Como parte del valor agregado a la presente tesis, se elaboró una Estrategia para fortalecer su gestión y continuidad, como resultado se presentó Perfil de Proyecto del Sistema Integrado de Facturación e Inventario, cuyos requisitos técnicos son los siguientes: Esquemas de seguridad que protejan los datos almacenados en la base de datos de las tres interfaces PC, Móvil PDA y Web; Acceso a la información a través de usuarios, claves y permisos sobre las opciones asignadas a cada usuario; Activación de pistas de auditoría que registren quien realizó cada operación y cuando; Adaptabilidad al cambio por modificaciones requeridas a corto o mediano plazo.

Finalmente, se diseñó un Plan de Continuidad del Negocio, mediante la identificación de aspectos débiles de la infraestructura que son susceptibles de sufrir un incidente y afectar la continuidad del negocio, para lo cual se proponen acciones y medidas a emprender en caso de ocurrir un incidente que afecte el negocio.

## Índice General

Introducción .....	9
CAPITULO I: PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACION.....	11
1.1.    Antecedentes .....	11
1.2.    Planteamiento del Problema: .....	12
1.3.    Formulación del Problema.....	12
1.4.    Justificación del Problema:.....	12
1.5.    Objetivos de la Investigación .....	14
Objetivo General:.....	14
Objetivos Específicos .....	14
CAPÍTULO II: MARCO TEÓRICO .....	15
2.1.    Concepto de diagnóstico .....	15
2.2.    Definición de control interno .....	15
2.3.    Definición de Arquitectura del software .....	15
2.4.    Manual técnico .....	15
2.5.    Diseño lógico .....	15
2.6.    Definición de ERP .....	16
2.7.    Definición de ingeniería de software.....	16
2.8.    Concepto de seguridad informática .....	16
2.9.    Definición de pista de auditoría .....	17
2.10.   Registro de auditoría de seguridad.....	17
2.11.   Control interno informático .....	17
2.12.   Conceptos de riesgos informáticos.....	17
2.13.   Existen 3 tipos de riesgos informáticos: .....	17
2.14.   Mapas de riesgos .....	18
2.15.   Concepto de plan de continuidad del negocio .....	18
Capítulo III: ESTRATEGIA METODOLÓGICA .....	19
3.1    Tipo de investigación.....	20
3.2    Enfoque de la investigación.....	20

3.3	Instrumento utilizado para la recolección de información: Entrevista no estructurada .....	21
3.4	Criterios para escoger a los entrevistados .....	21
3.5	Otras fuentes de investigación utilizadas .....	22
Capítulo IV: Informe final .....		23
4.1	Aspectos organizativos.....	23
4.2	Análisis de la arquitectura del sistema de facturación .....	27
4.3	Evaluación de la seguridad del sistema de facturación .....	33
4.4	Acceso lógico del sistema de facturación.....	34
4.5	Seguridad electrónica.....	34
4.6	Seguridad en el personal.....	35
4.7	Seguridad Física.....	36
4.8	Seguimiento de problemas y pistas de Auditoria.....	38
4.9	Evaluación de Riesgos operacionales y tecnológicos .....	40
4.9.1	Metodología utilizada.....	40
4.9.2	Parámetros de calificación.....	41
4.10	Riesgos potenciales identificados.....	42
4.11	Mapeo de escenarios de riesgos.....	54
4.12	Identificación de causas .....	55
4.13	Tratamientos de Riesgos Identificados.....	57
4.14	Requerimientos para el fortalecimiento de la Distribuidora .....	57
4.15	Nivel de seguridad del sistema de facturación .....	59
4.16	Estrategia para fortalecer el sistema de facturación.....	60
4.17	Parámetros de requerimientos técnicos del perfil del Sistema .....	61
4.18	Plan de continuidad del negocio.....	69
Capítulo V: CONCLUSIONES Y RECOMENDACIONES.....		70
5.1	Conclusiones.....	70
5.2	Recomendaciones.....	72
ANEXOS .....		73
CUESTIONARIO SOBRE SEGURIDAD DE LA INFORMACIÓN .....		74
CUESTIONARIO DE CONTROL INTERNO .....		77

Seguridad de la Información ISO 27001 .....	81
Normas Jurídicas de Nicaragua .....	84
Plan de Continuidad del Negocio .....	91
Referencias Bibliográficas.....	110



## **Introducción**

En estos tiempos, las necesidades de las empresas son definidas por el entorno global en que coexisten, este ambiente es muy competitivo; es indudable que el gran número de empresas existentes y la gran competitividad existente entre ellas; ya sea por materias primas, optimización de sus recursos, ingresar a nuevos mercados, entre otros; exige a las organizaciones de nuestro tiempo a un óptimo funcionamiento, esto con el propósito de lograr una ventaja competitiva a fin de mantenerse en el mercado.

Por lo anteriormente expuesto, es importante mencionar que la toma de decisiones que se lleva a cabo dentro de las organizaciones debe cumplir con ciertas características como son: rapidez, oportunidad y fundamentadas en disponer información concreta, que permita tomar decisiones eficientes, efectivas y con un bajo costo para la empresa; pues de ello dependerá el éxito o fracaso.

Debido a que la Junta Directiva de la Distribuidora Tropical del Pacífico S.A., requiere mejorar sus ventas de jugos Tropicales, necesita de un diagnóstico técnico del Sistema de Facturación para determinar si puede ampliar su mercado, o bien, tomar decisiones de inversión de un software que pueda satisfacer su necesidad.

Por lo antes expuesto se ha elaborado, la presente tesis denominada: “Diagnóstico del desempeño del Sistema de Facturación en la Distribuidora Tropical del Pacífico S.A., en el primer trimestre del año 2013”, en el que se pretende analizar los riesgos tecnológicos y control interno, entre otras alternativas de mejoras para que la empresa continúe creciendo en el mercado nacional.

De acuerdo al estudio realizado, se concluye que la Distribuidora Tropical del Pacífico S.A; que en adelante se denominará La Distribuidora, debe tomar la decisión de contratar una firma desarrolladora de software para que diseñe un Sistema Integrado de Facturación con los requerimientos de seguridad y lógica que están contenidos en este Diagnóstico.

El presente documento está estructurado por el Capítulo I: Planteamiento del Problema, Capítulo II: Marco Teórico, Capítulo III: Estrategia Metodológica, Capítulo IV: Informe final y Capítulo V: Conclusiones y Recomendaciones.

# **CAPITULO I: PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACION**

## **1.1. Antecedentes**

La Distribuidora Tropical del Pacífico S.A, tiene 14 años de trabajar en Nicaragua de forma ininterrumpida en la distribución de productos alimenticios. Comercializan varias líneas de productos, estos son: Riviana Pozuelo con todas sus galletas, Ducal con sus jugos, salsa de tomates, sopas instantáneas y Café Tigre, estos últimos dos productos son procesados en Nicaragua.

Actualmente la distribuidora objeto de análisis cuenta con dos almacenes de despacho de productos éstos, están organizados de forma independiente así como su sistema de facturación, es decir no existe una base de datos única que registre los ingresos y salidas del inventario y efectivo, lo que limita el control de productos, las ventas globales y su rentabilidad.

Adicionalmente, la empresa ha crecido en volúmenes de venta y como consecuencia pretende crear nuevos almacenes en las distintas regiones del país, razón por la cual el sistema de Facturación actual fue desarrollado en Visual Basic 6.0, lo cual no permite que sea integrado con el resto de almacenes, una de las limitaciones que actualmente enfrenta la Distribuidora es que los saldo de inventarios de productos no se descargan en línea con el sistema contable habiendo descuadre en saldos que actualiza hasta el día siguiente.

Dada la alta demanda de ventas, se requiere que el sistema de facturación, esté integrado con el sistema contable, este último fue desarrollado con la herramienta Fortran el cual no se puede integrar al sistema de Facturación.

El equipo de ejecutivos y ventas realizan grandes esfuerzos para responder a las necesidades de la empresa y esto ocasiona altos costos de horas extras y mayor cansancio en los trabajadores para dejar conciliados los saldos de ventas con la contabilización, duplicándose los esfuerzos en los cierres de mes.

La Junta Directiva de la Distribuidora, conscientes de las limitaciones que actualmente tienen decidió que se estudiara el sistema de Facturación para determinar la contratación de una empresa desarrolladora de software a fin de diseñar un sistema que cumpla con sus necesidades. Por tal motivo la presente tesis servirá de insumo para determinar si técnicamente el sistema de facturación puede ser modificarse de lo contrario se podría optar por la compra de un nuevo sistema integrado que cumpla las expectativas del negocio.

### **1.2. Planteamiento del Problema:**

El Sistema de Facturación actualmente es independiente en cada almacén lo que limita hacer auditorías internas efectivas, además cuando se creó este sistema no fue contemplada la expansión de la Distribuidora y controles necesarios asociados para evitar pérdidas de mercadería por su vencimiento.

### **1.3. Formulación del Problema**

¿En qué afecta a la Distribuidora la independencia del Sistema de Facturación en cada almacén?

¿Permite el Sistema de Facturación hacer consultas entre los distintos almacenes?

¿El sistema de Facturación posee niveles de seguridad que indiquen alertas del personal no autorizado?

### **1.4. Justificación del Problema:**

Los sistemas creados para procesar y difundir resultados o información elaborada pueden producir resultados erróneos si dichos datos son, a su vez, erróneos.

Es por eso que se hace necesario la efectuar un diagnóstico para identificar si el Sistema de Facturación posee la seguridad informática suficiente que minimice los riesgos en el procesamiento de la información o en validar los datos en aquel posible caso que se ingrese de forma incorrecta.

Es importante conocer además, cómo está segregado el control interno y la responsabilidad inherente a los puestos de trabajo para determinar si los ejecutivos tienen acceso a nivel de supervisión y en el caso del personal de caja

no pueda realizar acciones que pongan en grave peligro a la empresa al acceder al sistema de Facturación para: Autorizar o modificar mercaderías, porque se podría correr el peligro de que exposición de fraudes de mercadería. Para ello se analizará el Sistema de Facturación para determinar si cuenta con los controles pertinentes y además puede integrarse a todos los almacenes o bien es necesario el diseño y desarrollo de otro Sistema que cumpla con las expectativas de la Junta Directiva.

Los resultados del presente Diagnóstico serán de gran importancia por lo siguiente:

- a) Beneficiará a la Distribuidora porque con este estudio se ahorrará el pago de este dictamen técnico que ha sido desarrollado sobre Normas Internacionales de Seguridad de Información ISO/IEC 27002, entre otras. Por otra parte se obtendrá perfil de sistema que servirá de base para el requerimiento técnico a presentar a la firma desarrolladora de software a fin de que diseñe, desarrolle e implemente un Sistema Integrado de Facturación con características de ingeniería de software modernas y que las bases de datos puedan ser compartidas para agilizar el registro con eficiencia y calidad. Que pueda además generar reportes financieros por almacenes y corporativos para medir el impacto de la posición financiera integral y por almacén.
- b) Académicamente servirá de referencia para estudios posteriores relacionados con Diagnósticos y auditorías de sistemas automatizadas con enfoque de riesgos.
- c) En lo personal la suscrita fortalecerá a las bases de los conocimientos adquiridos en la Maestría de Auditoría Integral y además indagar sobre seguridad informática, estándares internacionales de tecnología de la información y leyes que regulen los sistemas, para que pueda aplicarlos en el ejercicio de mi carrera como Ingeniera de Sistemas y en la especialidad de Auditoría informática.

## **1.5. Objetivos de la Investigación**

### **Objetivo General:**

Desarrollar un estudio actual del funcionamiento del Sistema de Facturación de la Distribuidora Tropical del Pacífico S.A y proponer diseño de sistema flexible que sea adaptable al crecimiento de la empresa.

### **Objetivos Específicos:**

1. Analizar los aspectos organizativos y control interno de los procesos relacionados a la facturación.
2. Evaluar la arquitectura del sistema de Facturación y mecanismos de seguridad informática implementados.
3. Identificar las amenazas y estimaciones de los riesgos del proceso de facturación y conexos.
4. Proponer estrategias para el fortalecimiento de la Distribuidora a fin de eliminar vulnerabilidades existentes.

## **CAPÍTULO II: MARCO TEÓRICO**

### **2.1. Concepto de diagnóstico**

Raquel Amaya Martínez González (1993) analiza el diagnóstico definiéndolo como: “Una labor eminentemente práctica, exploratoria, encaminada al conocimiento de la naturaleza de una situación en una categoría de clasificación que permita establecer si presenta carencias o no, para, partir de ahí, elaborar un pronóstico sobre su desarrollo” (p.20).

### **2.2. Definición de control interno**

Coopers & Lybrand (1997) define el control interno como: “un proceso, efectuado por el personal de una entidad, diseñado para conseguir unos objetivos específicos. Una de las metas es evaluar el marco de control interno tomando como base el marco normativo interno y leyes asociadas” (p.15).

### **2.3. Definición de Arquitectura del software**

Antoni Olive Ramón & Ernest Teniente López (2004) señalan que: “la arquitectura del software es una descripción de los subsistemas y componentes (computacionales) de un sistema y las relaciones entre ellos” (p.11).

### **2.4. Manual técnico**

Roberto Cortes Morales (2010) se refiere al manual técnico como: “el código fuente y documentado del sistema, además de las especificaciones del lenguaje y librerías usadas para su creación, además de los requerimientos necesarios para su correcta ejecución” (p. 54).

### **2.5. Diseño lógico**

C. J. Date &, Sergio Luis & María Ruiz Faudón (2001) exponen el diseño lógico como “el proceso de construir un esquema de la información que utiliza la empresa, basándose en un modelo de base de datos específico, independiente

del Sistema de Gestión de Bases de Datos (SGBD) concreto que se vaya a utilizar y de cualquier otra consideración física” (p.327).

## **2.6. Definición de ERP**

Kenneth E. Kendall & Julie E. Kendall (2005) proponen la definición de ERP o sistemas planificación de recursos empresariales como: “sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía” (p.32).

## **2.7. Definición de ingeniería de software**

Door Ian Sommerville (2006) define la Ingeniería de software como: “la disciplina o área de la Ingeniería que ofrece métodos y técnicas para desarrollar y mantenimiento del software después que se utiliza” (p.6).

## **2.8. Concepto de seguridad informática**

Purificación Aguilera López (2010) define la seguridad informática en los siguientes términos: “es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable” (p.9).



## **2.9. Definición de pista de auditoría**

Leonor Galán Quiroz (1996) explica las pistas de auditoría como: “datos e informaciones históricas que están disponibles para su examen, con objeto de probar la corrección e integridad con la cual los procedimientos convenidos de seguridad, relativos a una clave o transacción(es), han sido seguidos” (p. 114).

## **2.10. Registro de auditoría de seguridad**

Javier Areitio Bertolín, (2008) se refiere a los registros de auditoría de seguridad como: “Proceso que proporciona un mecanismo de análisis y valoración de la seguridad, información relevante sobre la seguridad de un sistema de información” (p.321).

## **2.11. Control interno informático**

Leonor Galán Quiroz, (1996) refiere el control interno informático como: “la acción de controlar diariamente las actividades de los sistemas, cumpliendo los procedimientos, estándares y normas fijados por la Dirección de la organización y/o Dirección de Informática, así como los requerimientos legales. (p.116).

## **2.12. Conceptos de riesgos informáticos**

Leonor Galán Quiroz (1996) define el riesgo como: “la probabilidad de que un suceso adverso ocurra” (p.52).

## **2.13. Existen 3 tipos de riesgos informáticos:**

Leonor Galán Quiroz (1996) hace referencia a los tipos de riesgos:

Riesgo inherente: Se refiere al riesgo de que se presenten errores importantes en las actividades de la organización.

Riesgos de control: Se refiere al riesgo de que el sistema de control interno del cliente no prevea ni corregirá tales errores.

Riesgo de detección: Se refiere al riesgo de que cualesquier otro errores de importancia no puedan ser detectado por el auditor. (p.52).

#### **2.14. Mapas de riesgos**

Rubí Consuelo Mejía Quijano (2006) se refirió a los mapas de riesgos en los siguientes términos:

Es una herramienta que permite organizar la información sobre los riesgos de las empresas y visualizar su magnitud, con el fin de establecer las estrategias adecuadas para su manejo.

Los mapas de riesgos pueden presentarse con gráficos o datos. Los gráficos corresponden a la calificación de los riesgos con sus respectivas variables y a su evaluación de acuerdo con el método utilizado en cada empresa. Los datos pueden agruparse en tablas, con información referente a los riesgos; a su calificación, evaluación, controles y procesos, con respecto a los riesgos que la pueden afectar y las medidas de tratamiento implementadas. (p.39-40).

#### **2.15. Concepto de plan de continuidad del negocio**

Juan Gaspar Martínez (2004) define el plan de continuidad del negocio como:

Plan de continuidad del negocio es un proceso de dirección que identifica los impactos potenciales que amenazan a la organización y proporcionan el marco adecuado para construir y reforzar la capacidad de dar respuesta efectiva que salvaguarde los intereses, la imagen y el valor de las actividades realizadas por la misma (p.12).

### **Capítulo III: ESTRATEGIA METODOLÓGICA**

El presente diagnóstico se realizó utilizando la metodología cualitativa ya que se basa únicamente en conocer los hechos mediante el análisis de la información y entrevistas de las personas que llevan el proceso de facturación y aquellos procesos vinculados de la Distribuidora. Marcelo M. Gómez (2006) menciona que: “Los resultados de un estudio cualitativo son descripciones detalladas de eventos observadas y sus manifestaciones... y se fundamenta más en un proceso inductivo ya que explora y describe y luego genera perspectivas teóricas” (p. 25).

El contenido de este trabajo conllevó a realizar investigación de aspectos conceptuales, análisis del Sistema de Facturación desde el enfoque de su diseño y análisis del control interno asociado a éste, aplicando las ciencias de Ingeniería de sistemas y auditoría informática para determinar su efectividad y oportunidad de mejora para su rediseño o diseño de un nuevo Sistema integrado que cumpla las expectativas que demanda la Junta Directiva de la Distribuidora.

También se utiliza la técnica de muestreo intencional o selectivo ya que sólo se toma en cuenta a los funcionarios o empleados claves que posean un conocimiento general amplio sobre el tópico a indagar y que puedan proporcionar información valiosa que contribuyan de manera positiva y específica en la recolección de información para el Diagnóstico técnico. El universo de trabajo utilizado para este diagnóstico serán todos los involucrados en el proceso de facturación e inventario de la Distribuidora.

Para lograr este propósito se realizó como primer paso, entrevista directa con los máximos ejecutivos del negocio para conocer su visión estratégica y expectativas de este Diagnóstico.

Seguidamente, se realizó una planificación de tareas y se visitó al Responsable de Ventas para conocer el proceso de facturación, aplicando técnicas de observación directa en la atención de una solicitud hasta la entrega del producto.

Posteriormente, se analizó el Sistema de facturación y se aplicó las técnicas y herramientas adquiridas en la profesión de Ingeniería en Sistemas y Auditoría informática para conocer las fortalezas y debilidades que actualmente posee el Sistema. Para lo anterior, se preparó un formulario de preguntas. (Ver anexo No. 1)

### **3.1 Tipo de investigación**

En esta metodología se utilizó como parámetro para el análisis e interpretación de resultados obtenidos en las técnicas de encuestas y entrevistas no estructuradas a la población para sustentar los resultados. Siendo este diagnóstico de tipo evaluativo prepositivo con un enfoque cualitativo.

Los trabajos de tipo evaluativo tienden a confrontar una situación real frente a una esperada. Parten de un paradigma que sirve para comparar con una realidad, por lo que se requiere de criterios objetivos sobre la base de la construcción de escala.

Regina Jimenez-ottalengo & María Teresa Carreras, (2002) señalan que: “Los trabajos de tipo propositivo se concentran en diseñar pasos para alcanzar las metas propuestas por lo que se requiere de un diagnóstico previo. Parten de un supuesto: No lo prueba, sólo muestra los signos y los síntomas para detectar errores y corregirlos...” (p.33).

### **3.2 Enfoque de la investigación**

Empírico analítico, puesto que parte de un hecho real, en este caso análisis de la implantación de un posible sistema integrado de facturación e inventario y su incidencia en la práctica económica y a partir de esta posible realidad, se analiza sus aspectos positivos y negativos que impactarían al proceso, por lo que se efectúa una revisión documental y recopilación de información normativa del tema a fin de concluir con una evaluación analítica.

Este tipo de enfoque está presentado por la elaboración de explicaciones a los fenómenos de la realidad que se buscan sean controlados y/o transformados por

el hombre. Se pretende igualmente, que determinado el tipo de experiencia que ha resultado particularmente productivas se pueden replicar en condiciones relativamente nuevas.

### **3.3 Instrumento utilizado para la recolección de información: Entrevista no estructurada**

La entrevista no estructurada se utiliza en etapas exploratorias de la investigación. Para conocer el sistema de facturación de la Distribuidora Tropical Del Pacífico, es de gran importancia obtener la máxima información para detectar las dimensiones más relevantes y determinar las peculiaridades de la problemática, con el fin de generar un extracto de los aspectos más relevantes del sistema objeto de estudio así como aquellos procesos vinculantes. Es por eso que se utiliza este tipo de entrevista, porque permite al entrevistado que vaya narrando sus experiencias al manipular el sistema, sus puntos de vista en las debilidades y fortalezas de valorar su aplicabilidad.

### **3.4 Criterios para escoger a los entrevistados**

#### **Universo**

La población es un conjunto de unidades de estudio acerca de la cual se desea hacer alguna inferencia en ese sentido se habla de población objetivo.

El universo que se utilizó para la investigación, el cual está constituido por los sectores que representan la población objeto. Conformando un universo total: 12 personas

<b>Objeto de Estudio</b>	<b>Población</b>
<b>Directores</b>	<b>4</b>
<b>Facturadores</b>	<b>4</b>
<b>Inventario</b>	<b>4</b>

## **Método**

El método que se utilizó para los empleados de la Distribuidora fue el no probabilístico, ya que se tomaron el total de la población objetivo por tener información sensible para generar un análisis concluyente sobre bases fidedignas en aquellos aspectos de limitaciones que afectan la operatividad del negocio.

### **3.5 Otras fuentes de investigación utilizadas**

Página web, Libros sobre evaluación de seguridad y arquitectura de los sistemas, Análisis de la ISO/IEC 27002 Código de práctica de seguridad en la gestión de la información y COBIT (Control Objectives for Information Technology).

## **Capítulo IV: Informe final**

### **4.1 Aspectos organizativos**

La Distribuidora, es una empresa comercializadora de productos de consumo masivo que hace negocios en dos puntos de ventas en Managua y León, dentro de sus fortalezas se destaca su compromiso con sus clientes y proveedores, convencidos de sus valores, lidera con honestidad, creando un medio ambiente positivo que aliente la creatividad, mejora continua y motivados para afianzar su posición en el mercado por casi 18 años.

Los cimientos de la Distribuidora son la innovación del servicio y la calidad en la actividad de ventas y distribución, contribuyen al desarrollo de las marcas que venden en el país. Los objetivos siguen siendo ambiciosos y movilizan a todos los equipos para aportar al éxito de La Distribuidora y sus socios comerciales. Es una organización de consumo masivo en Nicaragua, en sus inicios se constituyó como respuesta a las necesidades de diferentes empresas regionales de distribuir sus productos.

Hoy las exigencias de los mercados y el alto índice de competencia entre las diferentes Distribuidoras de productos de consumo masivo son el impulso que obligan a brindar a sus clientes y consumidores el mejor servicio. Y es esto lo que el capital humano de La Distribuidora día a día hace para lograr la satisfacción de clientes y consumidores lo que consecuentemente lleva al logro de sus metas.

Actualmente, la Distribuidora, realiza la distribución exclusiva de marcas provenientes de importantes productores de alimentos y otras marcas tales como Riviana Pozuelo con todas sus galletas, Ducal con sus jugos, salsa de tomates, sopas instantáneas, yoplait y café tigre. Dichas marcas se hacen llegar a más de 15,000 clientes, a través de sus puntos de venta, con precios competitivos en el mercado.

## **A. Misión**

La Distribuidora Tropical comercializa productos de consumo masivo en todo el territorio nacional, a través de personal calificado y motivado, buscando siempre eficiencia en el servicio.

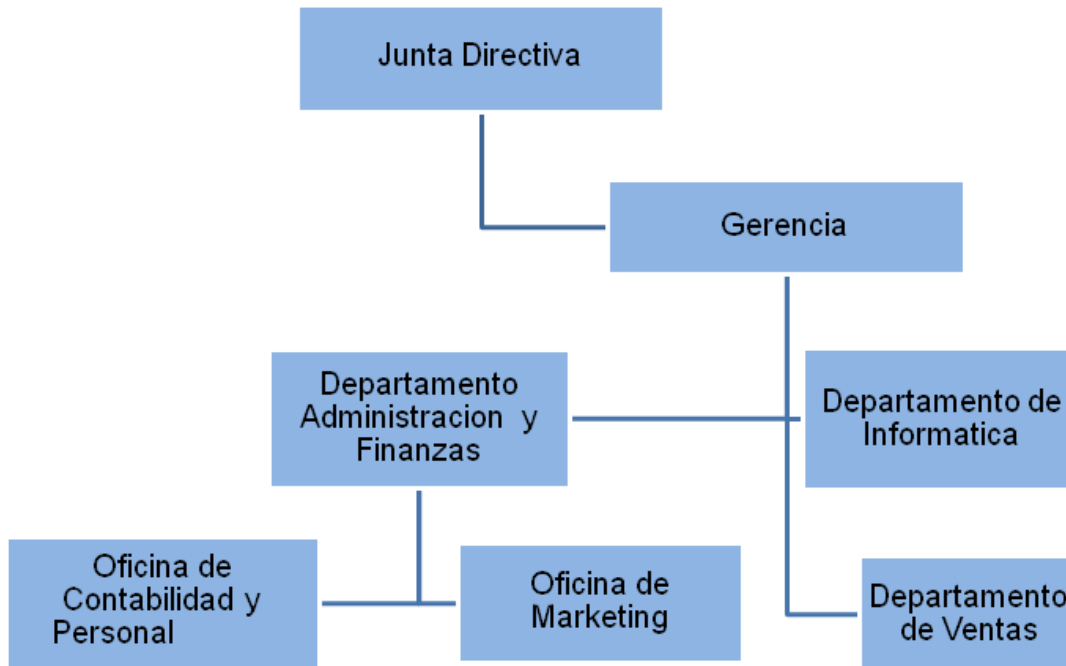
Nuestro compromiso de servicio nos permite una relación comercial estable y duradera con nuestros proveedores y clientes. Identificamos oportunidades para el desarrollo de productos y marcas que representamos, lo que contribuye a obtener los resultados financieros que garantizan el crecimiento de la empresa para el beneficio y satisfacción del consumidor final, clientes, proveedores, empleados y accionistas.

## **B. Visión**

Ser una empresa de Categoría internacional, líder en la comercialización de productos de consumo masivo, en continua búsqueda de excelencia en el servicio basado en el desarrollo del recurso humano.



## Organigrama de la Distribuidora Tropical del Pacífico S.A.



La estructura organizativa de la Distribuidora está conformada en 3 niveles de mando agrupadas por procesos y funciones, en primer lugar posee una Junta Directiva conformada por sus socios quienes dictan las tomas de decisiones estratégicas y de inversiones a ejecutar, en segundo nivel se encuentra el Gerente quien es el responsable de garantizar el funcionamiento del negocio, en tercer nivel de la estructura se encuentran los Jefes de Departamentos de Administración y Finanzas compuesto por la oficina de Contabilidad y Personal y la Oficina de Marketing, ésta última es la encargada de impulsar estrategias de mercadeo para ampliar el posicionamiento de la Distribuidora, seguidamente se encuentra el Departamento de Informática, quien es el encargado de la infraestructura tecnológica y finalmente de Departamento de Ventas, todos estos rinden cuenta al Gerente e informan de la gestión de sus procesos mensual, trimestral y si el caso lo amerita lo hacen tan pronto surge un problema o toma de decisiones que compete al Gerente. El personal ejecutivo, tienen años de trabajar en la Distribuidora y posee una amplia experiencia en sus funciones.

La Distribuidora tiene un marco normativo esencial como es: Manual de organización y funciones, Políticas de venta, normativa de ingreso y salida de productos de inventario y Procedimientos de rebajas y devoluciones de mercancía.

En el caso de las Políticas de ventas no está claramente definido en que concepto se puede regresar una mercadería, quedando sujeto a criterio del supervisor. Se observó que la documentación reglamentaria tiene 4 años de vigencia, lo que podría incurrir que en la práctica no se esté dando fiel cumplimiento a ésta, por desactualización y no responder a la dinámica del mercado y competencia lo que conllevaría en el mediano plazo a riesgos de pérdida de cliente y riesgo de imagen.

En lo que respecta a la Normativa de ingreso y salida de inventario no se cumplen fielmente debido a reportes de mercadería dada de baja por vencimiento lo que incurre en grandes riesgo financieros y de imagen. Lo anterior se constato mediante una prueba selectiva que se aplico directamente en el inventario.

Una fortaleza encontrada fue los arqueos diarios a caja según se constato en los registros auxiliares en contabilidad en un periodo de 6 meses. Sin embargo, estos no se practicaban igual en bodega, puesto que solo está establecido al menos trimestralmente, según el Procedimiento de arqueo de inventario.

De acuerdo a entrevista realizada al jefe del Departamento Administración y Finanzas se constató que no existe un Plan de Continuidad del negocio formalmente constituido, observándose existen pocos extintores contra incendios en relación al tamaño del local. De igual manera no posee, un plan de emergencia ante desastre siendo necesario debido a la existencia de productos inflamables que podrían conllevar a un incendio para el cual no están preparados ante una emergencia de estas magnitudes.

Según refirieron existe un plan de remuneración e incentivos por productividad al personal y se cumple con la disposiciones relacionadas con los derechos y obligaciones del los trabajadores.

#### **4.2 Análisis de la arquitectura del sistema de facturación**

Se ha realizado un diagnóstico del desempeño del Sistema de Facturación en la Distribuidora tomando en cuenta como referencia el manual técnico de este sistema, fue desarrollado en la herramienta de Visual Basic 6.0 y Ms Access como gestor de base de datos. Estas herramientas tienen algunas limitaciones que restringen la posibilidad de conectarse a los demás almacenes puesto que ambos no están diseñados para aplicaciones WEB esto imposibilita que puedan conectarse remotamente entre un punto de venta y otro.

Otras limitaciones que posee Ms Access es la frágil seguridad para el control de usuarios y de datos, porque también posee un almacén limitado de registros, la respuesta del servidor es lenta, sólo opera en red local y limitados usuarios, se tiene que hacer respaldos diarios del sistema de facturación para que pueda dar respuesta a nuevos registros, esto ocasiona serios atrasos para cerrar las ventas debido a que se tiene que asegurar que se realicen todos los días, de lo contrario se paralizarían las operaciones al día siguiente.

Evaluación del análisis y diseño lógico del sistema, el proceso del modelaje de entidad relación del sistema se realizó con la herramienta CASE identificándose la existencia de las entidades principales las cuales son: facturación, inventarios, clientes y créditos.

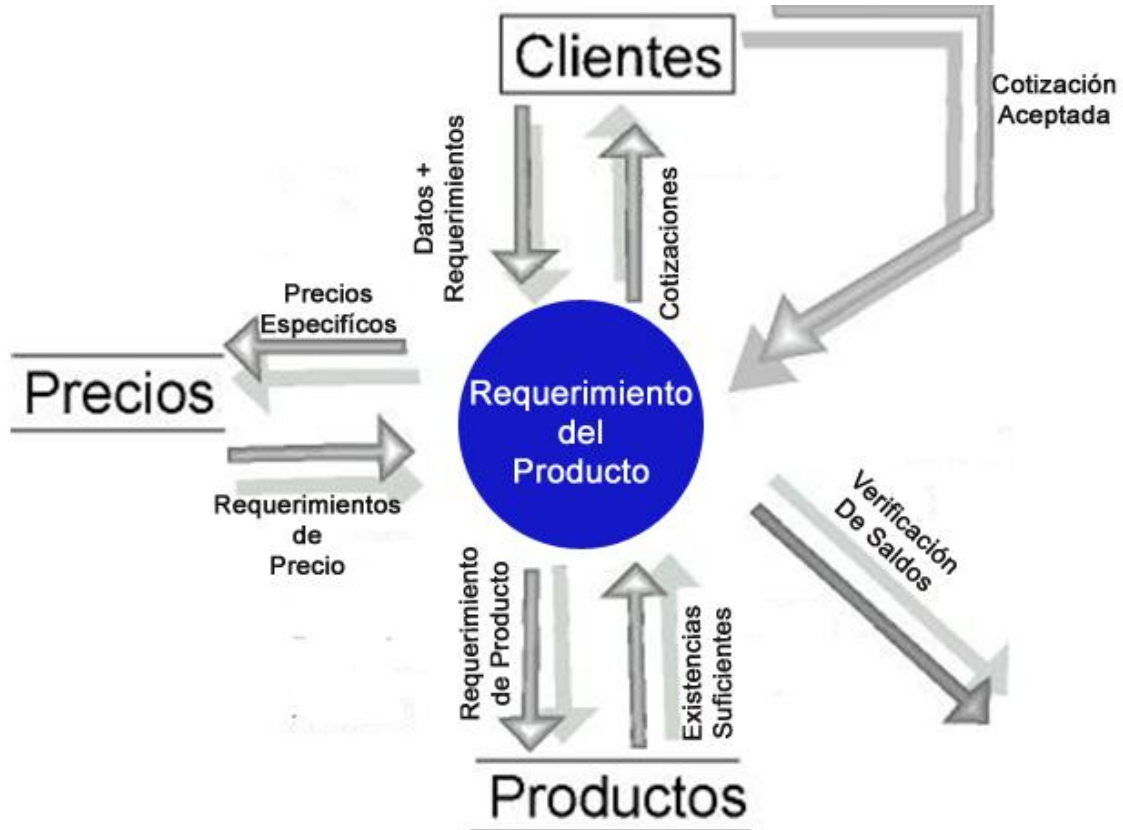
El análisis se divide en varios niveles de contexto para detallar todos los procesos involucrados a como sigue:

## Nivel de contexto (diagrama de flujo)



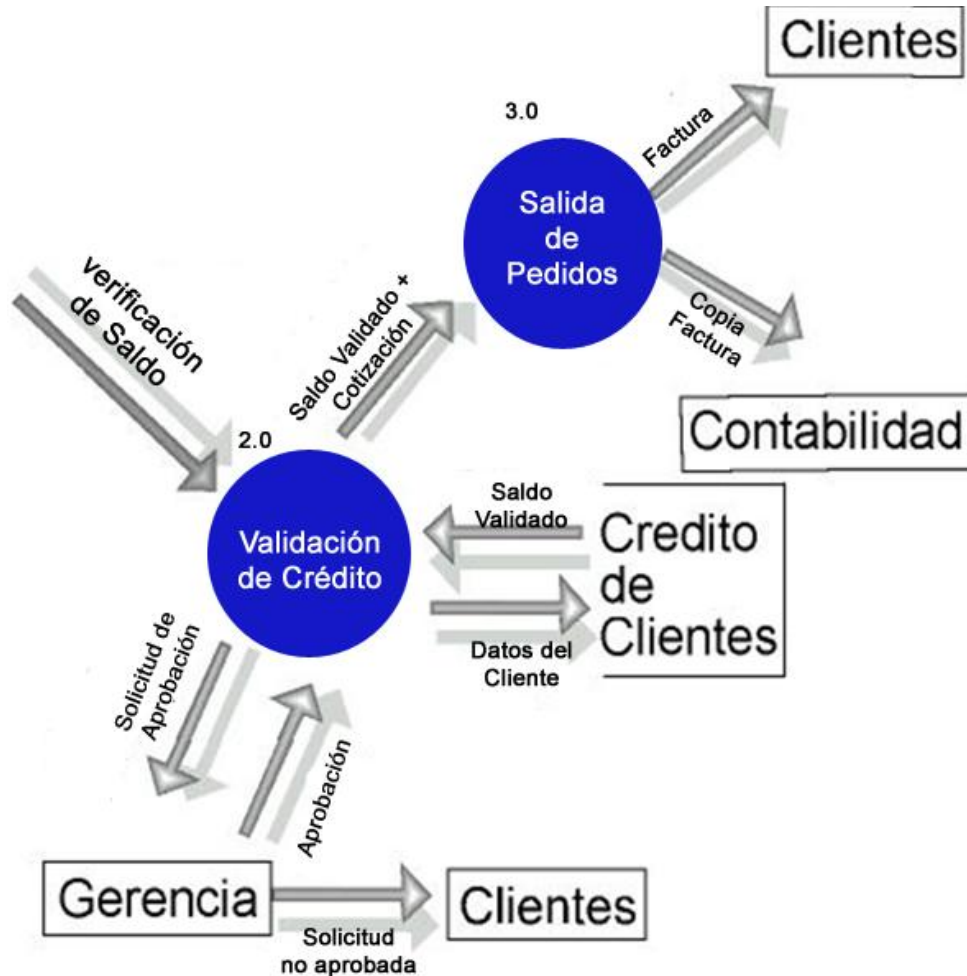
El nivel de contexto referido en el diagrama de flujo, describe los detalles de requerimientos de la estructura principal con que se relaciona el Sistema de Facturación; inicialmente el cliente proporciona los requerimientos del productos que desea (características del producto, cantidad por unidad y fecha de entrega). El vendedor le proporciona al cliente las cotizaciones, las cuales se refieren a un documento que especifica los precios actuales del producto y tipo de cambio, que el cliente requiere, la cotización se da desde el Sistema hacia la entidad cliente. Por lo tanto, el núcleo principal de Entidad Relación es facturación.

## NIVEL 1. Diagrama del proceso requerimiento del producto



El diseño del diagrama de flujo de datos del proceso, está conformado por tres entidades: cliente, precios y producto.

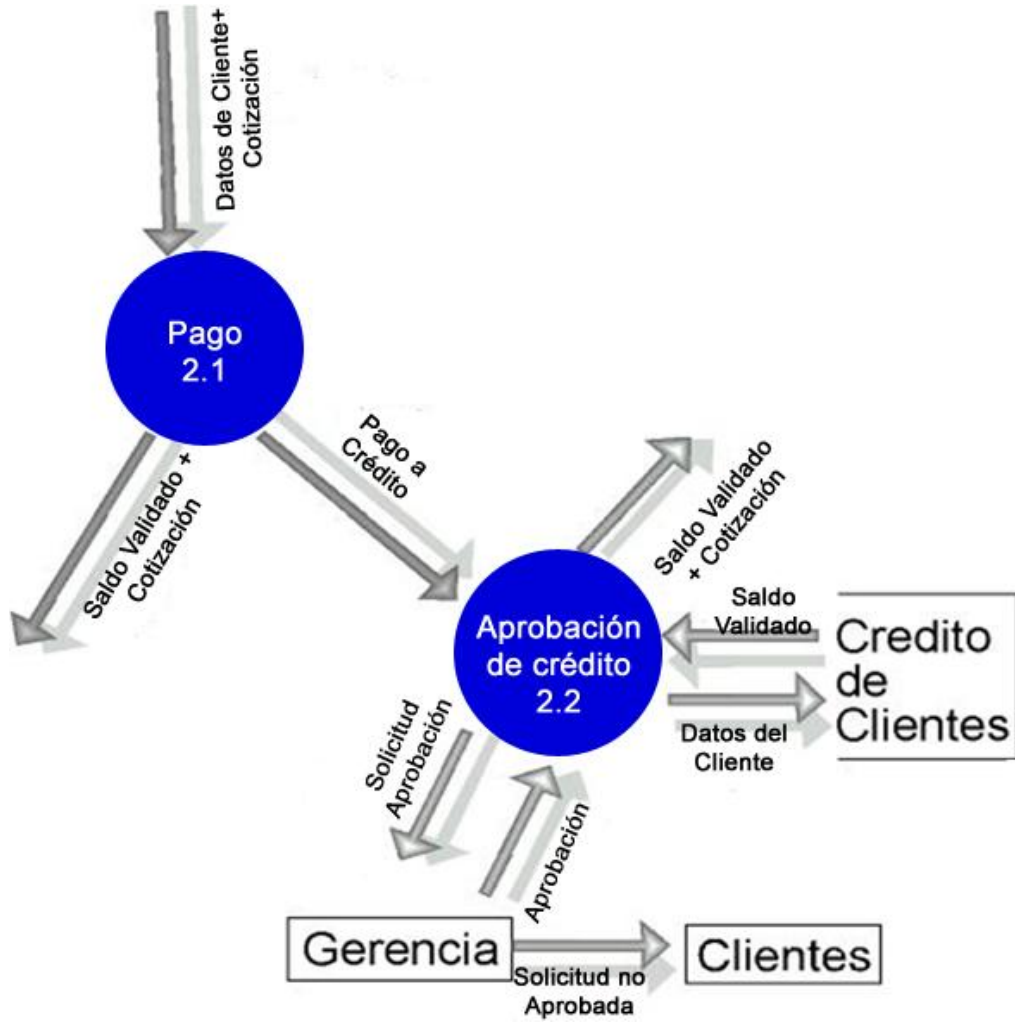
## SUBNIVEL 1. Flujo de datos del proceso salida de pedidos



El flujo de datos salida de pedidos, tiene asociado dos sub procesos internos, el primero cuando el cliente solicita un pedido y luego el sistema de facturación genera una factura, este proceso atenderá a los clientes que pagan en efectivo, por tanto la copia de la factura se tiene que enviar a la Oficina de Contabilidad y Personal para su contabilización.

El subproceso Validación de crédito, tiene asociado la tabla crédito de clientes y gerencia, la solicitud es rechazada si el cliente tiene saldos pendientes de cancelar por tanto no hay solicitud de crédito.

## SUBNIVEL 2



**Entidad Cliente:** Inicialmente el cliente proporciona los requerimientos del producto que necesita, solicita una cotización para la compra de materiales que requiere a través de una solicitud. Los datos proporcionado por el cliente en este proceso son: Características del producto, precios, cantidad por unidad, fecha de entrega y datos de cliente.

El flujo de datos en el que intervienen las cotizaciones se da desde el sistema de Facturación en el local de ventas hacia la entidad cliente. Las cotizaciones están estructurada con los siguientes datos: descripción del producto cotizado, cantidades, precios, fecha de cotización, fecha de entrega, datos del vendedor y cualquier otra información adicional necesaria.

**Cotización Aceptada:** Es la decisión que el cliente toma de acuerdo a la cotización que se le entrego, puede tener dos diferentes tipos que son: cotización aceptada, cotización rechazada. La información en este proceso está en la respuesta desde la entidad cliente al proceso de control y venta. La estructura esta de datos está definida por cotización aceptada o rechazada.

**Entidad Precios:** Esta tabla contiene cada producto en su correspondiente precio unitario y precios mayorista. Este proceso es actualizado por el Departamento de Ventas. Los atributos de esta tabla está compuesta por: Fecha, nombre de cliente, precios de producto requerido, nombre de producto.

**Requerimientos de Producto (Existencias):** Comprende la verificación del producto que el cliente requiere. El flujo de los datos se da desde la persona que factura hacia el almacenamiento producto. La estructura de este flujo comprende: Fecha, número de pedido, descripción de producto, cantidad de producto.

**Estado de Inventario:** Es la confirmación de los productos requeridos que cumplan con lo mínimo de existencia requerida de la entidad cliente. El flujo de los datos se da desde el almacenamiento de productos hacia el Cliente. Los datos



que recibe la gerencia son: número de cotización, nombre del cliente, descripción de productos, cantidad requerida, materias primas y sus costos respectivos.

**Solicitud de aprobación:** Es un documento que se le envía a la Gerencia, cuando el cliente rebasa su crédito, esta puede tomar 2 aspectos: rechazo o aprobación de crédito. El Gerente recibe esta solicitud de la persona que factura con relación al crédito del cliente. Los datos que componen este flujo son: número de cotización, fecha, datos del cliente, saldo de Cliente, cotización (Información de precios y productos).

**Solicitud Aprobada:** Es la respuesta de la solicitud de aprobación del crédito de un cliente específico, y esta puede ser negativa o positiva. En este proceso el Gerente Envía esta solicitud aprobada o rechazada a la persona que factura con relación al crédito del cliente. Los datos que componen este flujo son: número de cotización, fecha, datos del cliente, saldo de cliente, cotización (información de precios y productos), firma de aprobación o negación de crédito.

#### **4.3 Evaluación de la seguridad del sistema de facturación**

La mayoría de las empresas desconocen la magnitud del problema que enfrentan en tema de seguridad informática, muchas veces lo perciben como algo secundario y generalmente no invierten en capital humano o económico necesario para prevenir el daño y/o pérdida de la información que hoy en día con el uso de nuevas tecnologías pueden ser propensas a fugas.

Por tanto se ha estudiado los siguientes componentes: Caracterización del sistema de facturación, revisión del esquema de seguridad informática implementado y marco normativo que da sustento a los controles realizados.

Para analizar este tema, se realizó tres cuestionarios referentes a la seguridad de información que fueron aplicados al personal involucrado. Sin embargo dado que esta información es muy sensible, la Maestrante acordó con la Junta Directiva del negocio revelar aproximaciones de datos para proteger el riesgo tecnológico y

financiero a que pueda estar expuesta la Distribuidora por la invasión de un hacker.

#### **4.4 Acceso lógico del sistema de facturación**

La seguridad lógica a estudiar consiste en evaluar la aplicación de barreras y procedimientos que se implementan para el resguardo del acceso a los datos y solo se permite a personas autorizadas para hacerlo.

Dentro de las limitaciones encontradas se identificó lo siguiente: No existe un Plan de seguridad informático formalmente escrito. Sin embargo, el Departamento de Informática tiene implementado un Procedimiento administrativo para dar permisos de accesos al Sistema de facturación y sistemas automatizados por roll de permisos Operador y Autorizador, pero cuando un empleado se ausenta de manera temporal por subsidio o vacaciones de pocos días, no se deshabilita su acceso dado que no hay un reporte de permisos que la Oficina de Contabilidad y Personal envíe al Departamento de Informática para que proceda a deshabilitar los permisos de acceso a los sistemas informáticos de forma oportuna.

El sistema de facturación está protegido por un nivel sencillo de autenticación, lo que puede ser altamente vulnerable, en vista que pueden ingresar personas no autorizadas y generar autorizaciones de pedidos, razón por la cual se recomienda que la protección sea a un nivel múltiple de autenticación.

#### **4.5 Seguridad electrónica**

Los archivos primarios del sistema de facturación, están debidamente encriptados con el fin de evitar robos de información o hacer copias no autorizadas de archivos de datos con fines ilegales. No dispone de una herramienta de software de control de monitoreo, que permita supervisar en línea las actividades que desarrolla el administrador de base de datos, debido a que la Distribuidora no dispone de muchos sistemas automatizados. Como fortaleza se destaca la conexión de la red externa con protección de acceso firewalls.

El Departamento de Informática realiza las funciones de supervisión y monitoreo en el proceso de administración de base de datos, por lo cual coordina la instalación y configuración de software de bases de datos por actualización del producto o renovación del servidor.

Existe protección para que las computadoras tengan las últimas actualizaciones aplicadas a los sistemas operativos de manera de proveer un marco de seguridad y nuevas funcionalidades de los programas a fin de mejorar el desempeño del sistema de facturación y sistemas conexos. Además se actualizan los programas de protección anti virus.

#### **4.6 Seguridad en el personal**

Los sistemas de seguridad exigen que el personal que manipula los sistemas informáticos deben ser responsables de la seguridad informática y no solo el área específica que tiene a cargo esta función, además se necesita que estén capacitados en los controles de accesos lógicos y físicos, con el objetivo de minimizar errores intencionales o accidentales para prevenir la posibilidad de que tanto el administrador del sistema como los operadores o usuarios puedan cometer errores importantes o delitos. También debe considerarse la posibilidad de que personas externas a la Distribuidora (ex empleados principalmente), valiéndose de las debilidades de seguridad del sistema, ataquen al mismo con diferentes propósitos.

Por lo antes expuesto, es necesario crear controles que sean del conocimiento del personal y además darle seguimiento a su cumplimiento, por tanto, el Departamento de Informática deberá proveer un sistema de seguridad que brinde a cada usuario su ID y este a su vez defina su propio passwords (cambiado periódicamente), en vista que el Sistema de facturación, no obliga al usuario a cambiar su contraseña, también se debe orientar a los empleados que por ningún motivo debe compartir información sensible porque de ser así, cualquier error será su responsabilidad la que será identificada en la bitácora de seguridad.

Por tanto para fortalecer el acceso al Sistema de facturación y sistemas conexos, se recomienda integrar un proceso que funcionaría de la siguiente forma: El usuario se identifica en el sistema por medio de su ID y respectivo passwords, el sistema revisará si ambos componentes de identificación corresponden al mismo usuario, en caso de coincidir, el usuario podrá tener el acceso a los programas y datos; caso contrario, denegará el acceso y anotará un registro en la bitácora de seguridad.

El ID y passwords se desactivará en caso que el empleado sea despedido, sale de vacaciones u otra razón. Con la intención de asegurar el respeto de cada instrucción sobre seguridad y acceso, la administración debe definir claramente todas las Políticas y Procedimientos respectivos, establecer las sanciones que corresponden por el irrespeto de esas regulaciones y publicar los documentos respectivos.

#### **4.7 Seguridad Física**

La seguridad física son tareas y mecanismos cuyo objetivo es proteger al sistema de facturación y sistemas conexos (y por tanto, indirectamente a la información) de peligros físicos. La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

Se observó que el Departamento de Informática no tiene mecanismos de control de seguridad de entrada al local, bien pueden ingresar empleados externos y no hay ninguna barrera de protección, por ejemplo si hay algún daño o pérdida dentro del área de informática, no se puede identificar quien lo provocó, en primer lugar porque no está clasificada como un área de acceso restringido, por tanto no existe ningún registro de control de ingresos de personas externas, sobre todo porque en este lugar se encuentran los medios de almacenamiento de datos.

Para el ingreso del personal autorizado al Departamento de Informática se recomienda la incorporación de un sistema biométrico, para que cada empleado haga uso de tarjetas de identificación en este lector de seguridad, a fin de poder ingresar al local de forma electrónica.

La seguridad ambiental consiste en los procedimientos para controlar que los efectos ambientales no perjudiquen el procesamiento, los equipamientos y el personal. Las principales amenazas que se prevén en la seguridad física son:

- A. Desastres naturales, incendios accidentales, tormentas, inundaciones y terremotos.
- B. Amenazas ocasionadas por el hombre.
- C. Otros: señales de radar, instalación eléctrica, etc.

Como medidas preventivas se recomienda que la Distribuidora posea un Plan de continuidad de negocio, actualmente no tiene ningún documento formalmente escrito que oriente que acciones realizar antes de la ocurrencia de un posible desastre, o que decisiones tomar en caso de que ocurra. Siendo muy importante que este negocio posea un Centro de datos alternos para operar en casos de riesgos extremos que puedan paralizar las operaciones del negocio por tiempos mayores a 5 días, ya que de no ser así podría entrar en crisis financieras y pérdidas de clientes.

Como fortalezas identificadas se citan los siguientes aspectos:

Respaldo de datos: Copias de seguridad de la información del sistema en lugar seguro, la que puede estar disponible ante una emergencia.

Dispositivos físicos de protección, como pararrayos, detectores de humo y extintores.

#### **4.8 Seguimiento de problemas y pistas de Auditoria**

El Sistema de facturación y sistemas conexos de la Distribuidora, no tienen pistas de Auditoria, cuando sucede un problema técnico se resuelve a través del Ingeniero Informático a cargo del mantenimiento de los sistemas, pero cualquier evento que pueda suceder no se pueden identificar las situaciones que originaron el problema o error, por tanto es necesario que sean controlados a través de la revisión de logs, por lo que a continuación se presenta la importancia del establecimiento de logs y como se aplica este control.

Establecimiento de logs: Las pistas de auditoría o logs mantienen un registro de las actividades que los administradores y usuarios realizan sobre un sistema. Junto con herramientas y procedimiento adecuados, los logs pueden ayudar a detectar violaciones de seguridad, problemas de desempeño, etc. Los logs son usados como soporte para las operaciones requeridas del sistema y/o medio para asegurar políticas.

Por lo antes citado, se recomienda que el Sistema de facturación y sistemas conexos, tengan como mínimo los posibles eventos para su monitoreo:

- A. Identidad
- B. Fecha
- C. Tiempo de cada intento de entrada
- D. Fecha y tiempo de salida
- E. Dispositivos usados
- F. Las funciones ejecutadas.
- G. Intentos de login fallidos

Una auditoria podría identificar intentos de login fallidos, especialmente si no se limita el número de intentos en el sistema. Algunos sistemas no tienen la función de registrar intentos de acceso fallidos, de esta forma sólo se puede monitorear los intentos de acceso exitosos.

Se recomienda que las pistas de auditorías o logs a implantar sean establecidos para: Información confidencial por lo tanto requieren protección contra borrado o

modificación no autorizada. Fuertes controles de acceso y encriptación para preservar la confidencialidad e integridad. El acceso en línea a logs debería estar estrictamente controlado, sólo visible al personal de auditoría interna o externa para propósitos de revisión.

Es importante que los logs sean revisados ya sea ante la ocurrencia de un incidente de seguridad, automáticamente en tiempo real (monitoreo) o por una evaluación de seguridad planeada. Los auditores de sistema deberían determinar la longitud de los logs que será mantenido. Para el sistema el establecimiento de logs ayudará en los aspectos de control de acceso, reconstrucción de eventos y detección de intrusos.

Es importante que los logs se diseñen e implementen con la información apropiada que asista en la detección de intrusos, en vista que los cracker (personas que intentan romper la seguridad de un sistema, accediendo con malas intenciones a la información que se mantiene guardada en ellos) puedan detectarse en tiempo real si es posible o después de ocurrido el evento.

Se constató que por primera vez se realiza un evaluación general de la seguridad del Sistema de facturación en específico y se observó la imperante necesidad de diseñar una política de seguridad con estándares internacionales de seguridad, así mismo hacer evaluaciones periódicas de la buena conducta del personal informático y empleados claves del negocio para evitar colusiones y fraudes a través de la vía informática.

Para el análisis de este tema, se realizó entrevista no estructurada al Jefe Departamento de Informática y personal clave de esta área, así como aplicación de los siguientes instrumentos: Cuestionario sobre seguridad de la información, Cuestionario de control interno – tema: Administración del equipo informático y red institucional, Cuestionario de control interno – tema: Administración de base de datos del Sistema de facturación. Ver anexos N°: 1, 2 ,3 y 4.

## **4.9 Evaluación de Riesgos operacionales y tecnológicos**

En primer lugar, el riesgo se delimita como la probabilidad de que algo ocurra, para lo cual se debe recabar la información disponible e identificar los efectos negativos que puedan suceder, para luego analizar y medir su nivel de exposición.

Por tanto es importante conocer los riesgos que ponen en peligro la operación de la Distribuidora con el fin de obtener una visión de las acciones que se pueden llevar a cabo para medir y gestionar los distintos riesgos a los que se encuentra expuestos. Sin embargo, este análisis se ha limitado a evaluar los riesgos operacionales y tecnológicos esenciales del proceso de facturación así como aquellos que son vinculantes y que pueden paralizar la cadena de comercialización del negocio.

### **4.9.1 Metodología utilizada**

Para la definición y selección de los escenarios se consideraron 4 procesos más críticos de la Distribuidora, relacionados a la facturación de pedidos en la que incorpora riesgos tecnológicos y operacionales, a continuación se describen:

- A. Facturación
- B. Inventario
- C. Pago
- D. Contabilización

En cada proceso antes citado, se evaluaron los posibles riesgos operacionales y/o tecnológicos que podrían resultar en pérdidas económicas importantes para la Distribuidora y con probabilidad de ocurrencia. Para la clasificación de riesgos se definieron los siguientes parámetros de medición:



#### 4.9.2 Parámetros de calificación

##### 1. Estado y colorimetría

ESTADO	SIGNIFICADO	ACCIÓN
VERDE	BAJO	NIVEL TOLERABLE, NO REQUIERE ACCIÓN OBLIGATORIA. MONITOREO CONTINUO.
AMARILLO	MODERADO	REQUIERE INVESTIGACIÓN, VERIFICACIÓN Y ENTENDIMIENTO DE CAUSAS Y SE DEBEN CONSIDERAR CONTROLES Y ESTRATEGIAS (EVITAR, MITIGAR, TRANSFERIR Y ACEPTAR).
ROJO	ALTO	REQUIERE INVESTIGACIÓN, VERIFICACIÓN Y ENTENDIMIENTO DE CAUSAS Y SE DEBEN CONSIDERAR CONTROLES Y ESTRATEGIAS URGENTES, PARA SU MITIGACIÓN. REQUIERE UNA ACCIÓN URGENTE

##### 2. Escalas de probabilidad

Valor	Probabilidad	Descripción
1	Remoto	Nunca ha sucedido y es casi imposible que suceda.
2	Improbable	Es difícil que suceda
3	Posible	Ha sucedido esporádicamente
4	Probable	Ha sucedido y podría volver a suceder.
5	Cierto	Existe la posibilidad que suceda

##### 3. Escalas de impacto

Valor	Impacto	Descripción
1	Insignificante	No afecta el cumplimiento de los objetivos
2	Menor	Podría afectar el cumplimiento de los objetivos
3	Moderado	Afecta el cumplimiento de los objetivos
4	Mayor	Afecta de manera importante al cumplimiento de los objetivos
5	Catastrófico	No permite el cumplimiento de los objetivos

#### 4. Nivel de riesgo

5	6	7	8	9	10
4	5	6	7	8	9
3	4	5	6	7	8
2	3	4	5	6	7
1	2	3	4	5	6
	1	2	3	4	5

NIVEL DE RIESGO
Acceptable $\leq 4.9$
Medio $5 \leq \text{Nivel} < 6$
Serio $\Rightarrow 6$

#### 4.10 Riesgos potenciales identificados

Los riesgos más significativos identificados fueron obtenidos mediante el análisis de los procesos y con ellos se pretende obtener una visión general del nivel de riesgos al proceso de facturación y vinculantes de la Distribuidora. A continuación se describen los escenarios con sus respectivas medidas correctivas:

## Escenarios de riesgos

Área	No. Riesgo	Descripción del escenario	Proceso	Medidas correctivas	Clasificación del Riesgo		
					Probabilidad	Impacto	Nivel de riesgo
Departamento de Informática	1	Riesgo de que el sistema de facturación no se ajuste a los principios de contabilidad generalmente aceptados y efectúe mala aplicación de retención de impuesto sobre ventas.	Facturación	Valorar si el sistema de facturación no se le puede ajustar conforme las nuevas retenciones de impuesto, caso contrario extraer del Sistema de facturación datos esenciales y realizar tabla dinámica para calcular nuevo impuesto, esto se deberá realizar por cada factura emitida, esta función deberá ser realizada por el Depto. de Ventas.	1	2	3
Departamento de Ventas	2	Registro incompleto y/o incorrecto de la mercadería y/o precios en el sistema de facturación	Inventario	Segregar las funciones de Operador, Supervisor y Autorizador para verificar el correcto registro de mercancías.	1	3	4

Área	No. Riesgo	Descripción del escenario	Proceso	Medidas correctivas	Clasificación del Riesgo		
					Probabilidad	Impacto	Nivel de riesgo
Departamento de Informática Departamento Contabilidad Departamento de Ventas	3	Falta de correspondencia entre el registro de existencias de mercadería y el registro contable.	Inventario/contabilización	Desarrollar una interfaz entre el sistema de facturación y sistema de contabilidad para evitar errores de conciliación de saldos.	3	3.6	6.6
Departamento de Informática	4	La complejidad del sistema de facturación permite encubrir operaciones ilegales. Deterioro de auditabilidad	Inventario/contabilización	Adoptar un sistema de alertas que permita identificar operaciones sospechosas.	1	3	4
Departamento de Informática	5	La ausencia de una pista de auditoría adecuada dificulta la realización de un control de pago eficaz y efectivo basado en la auditoría.	Facturación/ Inventario/ Pago/ Contabilización	Creación de pista de auditoría en sistemas de facturación y contabilidad.	2	4	6

Área	No. Riesgo	Descripción del escenario	Proceso	Medidas correctivas	Clasificación del Riesgo		
					Probabilidad	Impacto	Nivel de riesgo
Departamento de Informática Departamento de Ventas	6	Falta de control sobre la seguridad y el acceso al sistema de facturación.	Facturación	Crear normas de acceso al sistema de facturación y evaluar permanentemente su cumplimiento.	2	3	5



Área	No. Riesgo	Descripción del escenario	Proceso	Medidas correctivas	Clasificación del Riesgo		
					Probabilidad	Impacto	Nivel de riesgo
Departamento de Ventas Departamento de Contabilidad /Inventario	8	Uso indebido del sistema de facturación del operador para poner en riesgo la cadena de suministro	Facturación, Pago, Inventario, Contabilización	Clasificar documentos: Públicos, Reservados y Restringidos y Elaborar e implementar Norma para el acceso autorizado a los documentos según su clasificación.	3	2.4	5.4
Protección Física, Departamento Administrativo y Finanzas	9	Conocimiento inadecuado de los aspectos relacionados con la seguridad y la protección en todos los departamentos relevantes de la Distribuidora.	Facturación/Inventario	Evaluar los riesgos relacionados con la seguridad y la protección (% de probabilidad o nivel de riesgo: bajo/medio/alto); Asegurarse de que todos los riesgos pertinentes se abordan con medidas preventivas y correctiva	1	2	3

Área	No. Riesgo	Descripción del escenario	Proceso	Medidas correctivas	Clasificación del Riesgo		
					Probabilidad	Impacto	Nivel de riesgo
Departamento de Informática, Departamento de Contabilidad Almacén/ Dirección de Ventas/ Protección Física	10	La inexistencia de controles internos o su ineficacia posibilita el fraude y el desarrollo de actividades no autorizadas o ilegales.	Facturación/Inventario/Pago/Contabilización	<p>Instalación de cámaras de vigilancia de circuito cerrado y grabación de videos para su monitoreo permanente. Manual de Organización y Funciones elaborado y divulgado</p> <p>Libro de registro de incidencias que contenga, por ejemplo, la fecha, la anomalía observada, el nombre de la persona que la detectó, las medidas de respuesta, la firma de la persona competente, etc.;</p>	2.3	3.5	5.8



Área	No. Riesgo	Descripción del escenario	Proceso	Medidas correctivas	Clasificación del Riesgo		
					Probabilidad	Impacto	Nivel de riesgo
Inventario	11	La ausencia de control de los movimientos de existencias de mercadería aumenta el riesgo de las fechas de vencimientos de productos o escasez del producto en inventario	Facturación/Inventario	Realizar políticas de inventario para asegurar que los productos sean rotados y evitar su vencimiento. Realizar inventarios trimestrales de productos. Separar por anaqueles los productos según su vida útil	1	4.6	5.6
Departamento de Contabilidad y Personal, Almacén, Departamento de Ventas	12	Falta de coincidencia entre las mercancías pedidas, las mercancías recibidas y los asientos contables.	Facturación, Inventario, Pago, Contabilización	Realizar conciliaciones de saldos de sistema de facturación, sistema contable y sistema de inventario.	2	3.8	5.8

Área	No. Riesgo	Descripción del escenario	Proceso	Medidas correctivas	Clasificación del Riesgo		
					Probabilidad	Impacto	Nivel de riesgo
Departamento de Contabilidad, Almacén, Departamento de Ventas	13	Ausencia de procedimientos para la segregación de tareas entre el registro y los controles internos	Facturación / Inventario/ Pago / Contabilización	Elaborar procedimientos administrativos de los procesos de contabilidad, almacén y ventas	2	2	4
Departamento de Informática y Contabilidad, Almacén, Departamento de Ventas	14	Incapacidad de emprender oportunamente una auditoría debido a la pérdida de información o las deficiencias en los archivos.	Facturación/Inventario/ Pago/ Contabilización	Facturación / Inventario/ Pago/ Contabilización	2	2	4
Departamento Informática Departamento de Ventas	15	Falta de procedimientos relativos a la copia de seguridad de datos.	Facturación, Inventario, Pago, Contabilización	Procedimiento administrativo para el respaldo de bases de datos del sistema de facturación, contabilidad e inventario y resguardo de copia de seguridad en cintas magnéticas	2	5.9	7.9

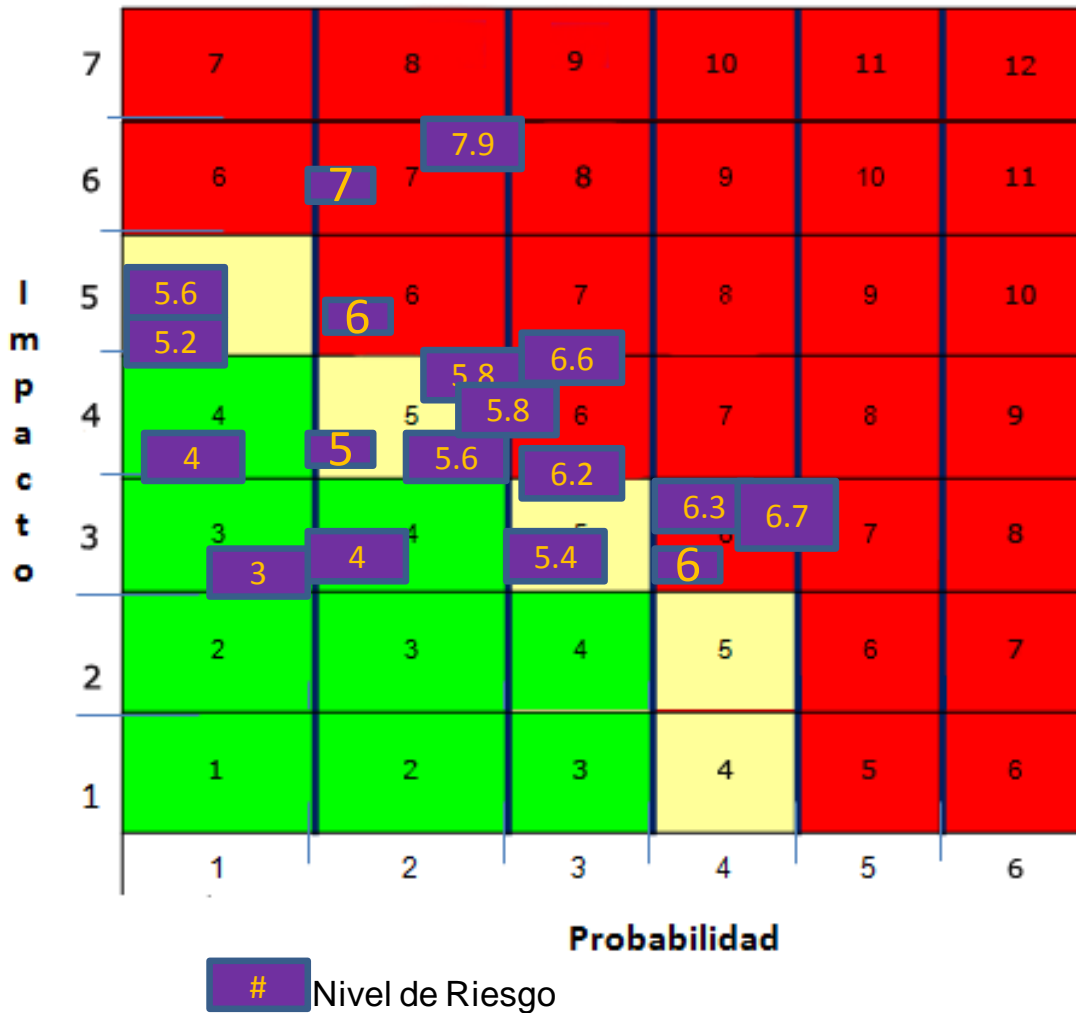
Área	No. Riesgo	Descripción del escenario	Proceso	Medidas correctivas	Clasificación del Riesgo		
					Probabilidad	Impacto	Nivel de riesgo
Dirección Informática Departamento de Informática , Oficina de Contabilidad y Personal Departamento de Ventas	16	Dstrucción deliberada o pérdida de información importante que ponga en riesgo las finanzas de la Distribuidora	Facturación / Inventario / Pago / Contabilización	Archivo y almacenamiento seguro de documentos; Procedimientos para abordar los incidentes y emprender acciones correctivas; Registro y copia de respaldo de documentos, incluido el escaneado; Plan de contingencia para gestionar las pérdidas; Posibilidad de utilizar programas de cifrado en caso necesario; Los agentes comerciales deben conocer las medidas de seguridad en sus desplazamientos (no consultar nunca documentos "sensibles" en medios de transporte); Establecer niveles de acceso a la información estratégica con arreglo a las diferentes categorías del personal; Gestión segura de las computadoras desechadas; Acuerdos con socios comerciales respecto a la protección y el uso de documentación.	3	3.2	6.2

Área	No. Riesgo	Descripción del escenario	Proceso	Medidas correctivas	Clasificación del Riesgo		
					Probabilidad	Impacto	Nivel de riesgo
Protección física/ Departamento Administración y Finanzas	17	Acceso inadecuado al centro de cómputos, pocas medidas de seguridad	Facturación/Inventario	Medidas de seguridad física interna establecidas, usando carnet biométricos para personal de zonas restringidas	4	2.3	6.3
Protección física/ Departamento Administración y Finanzas	18	Alteración de las unidades de carga	Facturación/Inventario	Elaborar e implementar procedimientos para el registro, la investigación y la adopción de acciones correctivas en casos de detección de accesos no autorizados o de alteración de las mercancías; - en su caso, supervisión adecuada mediante CCTV.	1	4.2	5.2

Área	No. Riesgo	Descripción del escenario	Proceso	Medidas correctivas	Clasificación del Riesgo		
					Probabilidad	Impacto	Nivel de riesgo
Departamento Administración y Finanzas, Departamento de Ventas	19	Ausencia de mecanismos para formar a los empleados sobre el manejo de los sistemas informáticos y en consecuencia provoque errores en la selección o digitación de datos.	Facturación / Inventario	Plan de capacitación para formar a empleados sobre el manejo de los sistemas informáticos asociados al puesto.	2	2	4
Departamento de Informática	20	Fallas severas en los sistemas que paralicen operaciones por problemas en: Hardware, Software básico, Software aplicativo, suministros	Facturación / Inventario/ Pago Contabilización	Elaborar e implementar plan de continuidad del negocio.	4	2.7	6.7

#### 4.11 Mapeo de escenarios de riesgos

De la información recopilada de los escenarios, los resultados de la valoración de los posibles grados de probabilidad de ocurrencia se presentan por medio de mapa de riesgo, a fin de establecer prioridades en el fortalecimiento de los controles para su mitigación.



De acuerdo al mapa de riesgos, se obtuvo que de los 20 escenarios de riesgos se identificaron 11 eventos con nivel de riesgo mayor del 5.6 alcanzando el máximo riesgo una puntuación de 7.9, los que mayor se destacan corresponden a posibles incidentes en: Falta de correspondencia entre el registro de existencias de mercadería y el registro contable, La ausencia de una pista de auditoría adecuada dificulta la realización de un control de pago eficaz y efectivo basado en la auditoría, Acceso no autorizado y/o intrusión en los sistemas o programas

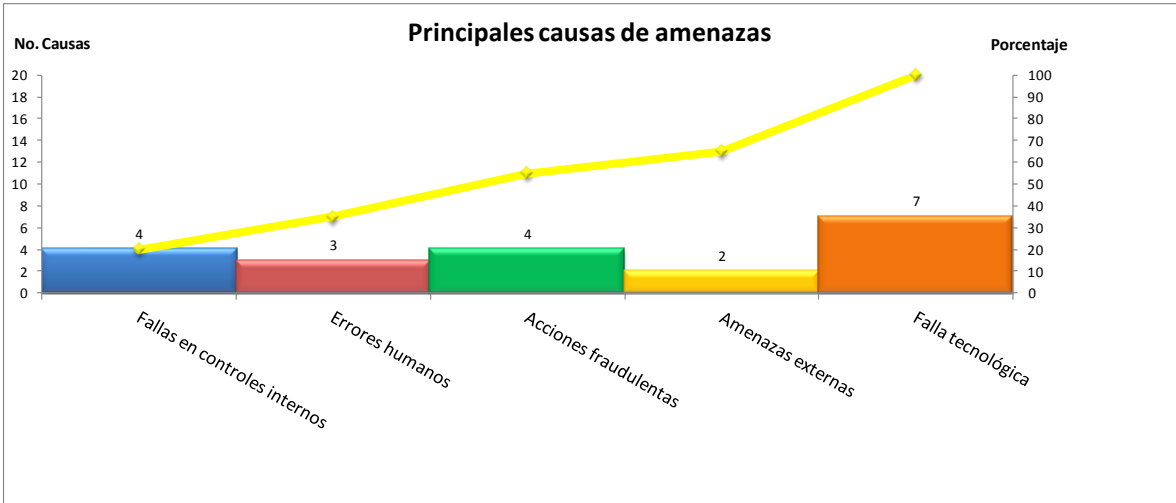
informáticos, Falta de procedimientos relativos a la copia de seguridad de datos, Acceso no autorizado y/o intrusión en los sistemas o programas informáticos, Destrucción deliberada o pérdida de información importante que ponga en riesgo las finanzas de la Distribuidora y Fallas severas en los sistemas que paraliquen operaciones por problemas en: Hardware, Software básico, Software aplicativo, suministros. Los 9 eventos restantes que calificaron en riesgo están asociados a registros incorrectos, pocos controles o procedimientos inexistentes y necesidad de fortalecer la vigilancia en áreas que deben ser de carácter restrictivo.

#### **4.12 Identificación de causas**

Como resultado de este análisis, se identificaron las cinco causas más relevantes y recurrentes en los escenarios de riesgo en estudio, las cuales son:

1. Fallas en controles internos (controles ineficientes o que no existen)
2. Errores humanos (mala digitación, omisión o falta de capacitación)
3. Acciones fraudulentas
4. Amenazas externas a la Distribuidora (colusión para robos)
5. Mal funcionamiento de plataforma tecnológica

En el siguiente diagrama de Pareto se asocian los escenarios con sus causas de ocurrencia respectivas, lo cual revela los principales aspectos a priorizar de cara a un mejoramiento de la infraestructura tecnológica y administración de ventas de la Distribuidora.



Conforme a los resultados anteriores, se observa que el 35 por ciento de posible materialización de los escenarios de riesgo analizados recaen en debilidades de los controles establecidos y fallas tecnológicas.

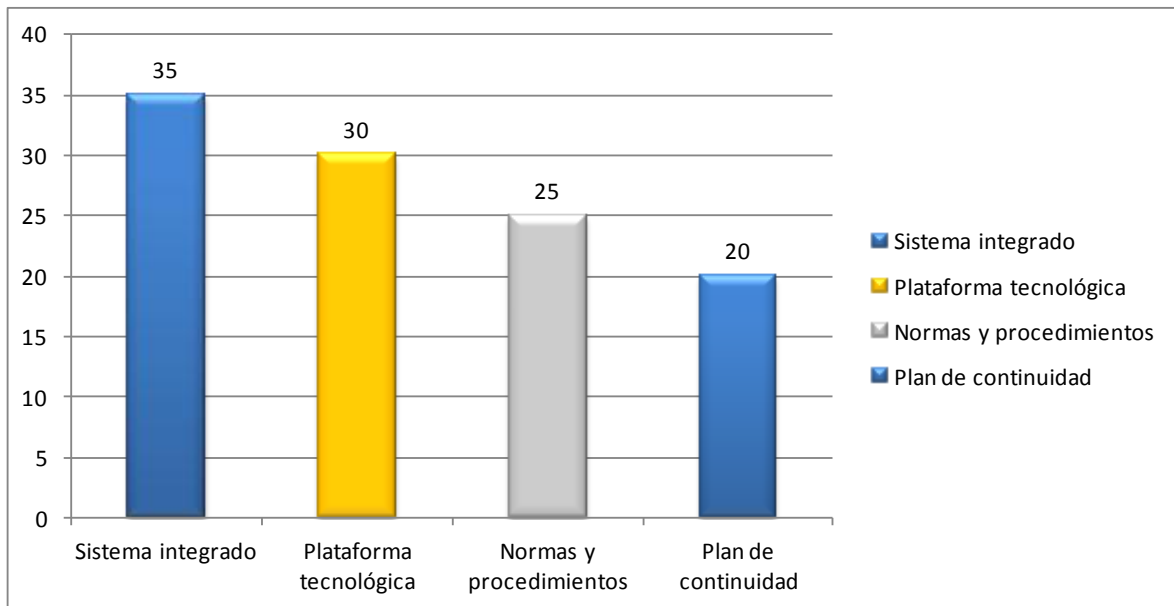


### 4.13 Tratamientos de Riesgos Identificados

El análisis de la documentación de los escenarios, permitió identificar las causas de su ocurrencia e hizo posible que las áreas vinculadas al proceso de facturación lograran visualizar los puntos débiles de la cadena de registro, control y comercialización, lo que conllevó a orientar con mayor precisión la formulación de tratamientos hacia su fortalecimiento y mejora.

Los tratamientos propuestos y analizados por las áreas organizativas se alinearon en torno a cuatro tipos de requerimientos particulares para el fortalecimiento de la Distribuidora, distribuidos conforme lo expresa el siguiente gráfico:

### 4.14 Requerimientos para el fortalecimiento de la Distribuidora



En este gráfico se puede observar la necesidad de desarrollar e implementar un Sistema Integrado de facturación, inventario y contabilidad, en vista que el Sistema de contabilidad está desvinculado, lo que origina limitaciones en el registro y control de mercaderías, debido a que los saldos de existencias de productos en inventario se realizan un día desfasado, posterior al cierre de ventas en los registros contables.

En un segundo lugar, se necesita robustecer la plataforma tecnológica a fin de diseñar políticas de seguridad acorde a normas internacionales, procedimientos y normas en materia de tecnología de información adoptados y a disposición del personal informático; Procedimientos para la concesión o la denegación de derechos de acceso a personas autorizadas; Utilización de programas de codificación, cuando convenga; Cortafuegos; Licencias antivirus robustas; Protección mediante contraseñas; Pruebas contra accesos no autorizados; restricciones a salas de servidores y realización de pruebas periódicas de intrusión y Ejecución de procedimientos para el tratamiento de los incidentes. Adoptar un sistema de alertas que permita identificar operaciones sospechosas.

Como tercer aspecto a mejorar sería el control interno, mediante la elaboración de Normas y procedimientos administrativos, siendo indispensable clasificar documentos en: Públicos, Reservados y Restringidos con su correspondiente Norma de acceso a la información según su rol y perfil del puesto de trabajo, esta acción permitirá establecer reglas y minimizar la fuga de información que la competencia pueda obtener a fin de evitar competencias desleales.

Además de lo anterior, será necesario actualizar las Políticas de inventario para asegurar que los productos sean rotados y evitar su vencimiento. Así mismo, se requiere elaborar Procedimientos administrativos de los procesos de facturación, inventario y contabilidad de manera que el flujo de los procesos no sea interrumpido y se mantengan los saldos de inventario y contabilidad conciliados.

Finalmente, se requiere elaborar un Plan de Continuidad del Negocio en vista que no existe y las acciones correctivas se hacen cuando suceden los problemas. Por tal razón, se ha diseñado un Plan de continuidad, con el fin de identificar las acciones necesarias de una forma organizada para dar una capacidad de respuesta ante situaciones de emergencia, incluso en las extremas, mediante la práctica de operaciones preventivas de mitigación de riesgos que se presenten, para evitar la discontinuidad de las actividades para no afectar el cierre de operaciones de ventas. En Anexo N°5 se adjunta Plan de continuidad del negocio.

Los tratamientos planteados anteriormente son claves para el logro de los objetivos de la Distribuidora, en conjunto forman un flujo para poder administrar de manera adecuada los riesgos con probabilidad de ocurrencia. Se pretende que con la ejecución de los mismos, se logre disminuir la probabilidad de ocurrencia o prevenir desastres que puedan afectar la operatividad del negocio.

Es importante tomar en cuenta que las áreas, involucradas en la ejecución de dichos tratamientos, deberán asegurar el cumplimiento de las estrategias establecidas, así como también valorar las medidas correctivas identificadas en los diferentes escenarios de riesgos identificados en este capítulo.

#### **4.15 Nivel de seguridad del sistema de facturación**

La base de datos del sistema no es segura porque no tiene la capacidad de almacenamiento de datos históricos, lo que limita a generar reportes estadísticos del comportamiento de las ventas.

Al estar segregado el Sistema de Facturación en cada almacén, la información puede ser distorsionada porque en cada uno de éstos, el personal que interactúa con el Sistema puede modificar los datos lo que podría elevar el riesgo de una pérdida financiera considerable, si no existe un control permanente y un supervisor leal que valide las transacciones.

Esta situación se intensifica porque no existe una relación automática para que el encargado de contabilidad tenga acceso a los reportes de ventas a fin de contabilizar las operaciones en el mismo día y a su vez monitorear los ingresos y salidas de inventario, éste lo hace a través de las copias de facturas que pueden ser objeto de alternación.

A nivel de estación de trabajo exige contraseñas, pero éstas no son fuertes (alta seguridad) y tampoco son programadas lo que incide a no obligar a los usuarios a cambiarlas y pueden ser compartidas.

El sistema de facturación posee software de firewall (cinturón de fuego) destacándose como una fortaleza.

Las computadoras donde reside el sistema en estudio, están protegidas por Norton antivirus lo que mitiga el riesgo tecnológico de ser contaminadas.

#### **4.16 Estrategia para fortalecer el sistema de facturación**

La Informática, es la plataforma en la gestión integral de las empresas, y por eso las normas y estándares propiamente informáticos deben estar sometidos a controles. Cabe aclarar que la Informática no gestiona propiamente la empresa, pero si ayuda a la toma de decisiones, debido a que no decide por sí misma.

De acuerdo al Diagnóstico del desempeño del Sistema de Facturación en la Distribuidora Tropical del Pacífico S.A, en el primer trimestre del año 2013, se identificó una serie de limitaciones entre las que se destacan, la falta de vinculación con el sistema contable lo que conlleva a no tener conciliaciones de saldos en tiempo real tales como ingresos por ventas y saldos en inventarios, las medidas de seguridad del sistema objeto de estudio tenía pocas fortalezas porque no podía migrar a una plataforma con entorno de red robusta, una razón fundamental que merece destacarse es que al haber sido desarrollado en la herramienta de Ms Access y Visual Basic 6.0 no permiten que este sistema sea integrado en otros almacenes en línea, dado que fue diseñado solo para una red local interna.

Por lo antes citado y como aporte al fortalecimiento de la gestión comercial de la Distribuidora, la Maestrante ha propuesto un Perfil del Sistema de facturación e inventario vinculado al sistema contable, tomando como base la Norma Internacional ISO/IEC 27001, la que es un estándar para la seguridad de la información. A continuación se describe:

#### **4.17 Parámetros de requerimientos técnicos del perfil del Sistema**

Los productos esperados que debe contener el Sistema integrado facturación e inventario se describen a continuación:

1. El desarrollo de solución de software integral, debe ser diseñado con tres interfaces específicas: una interfaz de escritorio (PC), una interfaz móvil (PDA) y una interfaz Web (Internet), que permitan la comercialización efectiva de la venta de productos, como valor agregado se incorpora que desde que un cliente visita la distribuidora puede ser atendido inmediatamente por algún ejecutivo de ventas y puede facturar desde un dispositivo móvil (PDA), este automáticamente genera en el punto de red la factura comercial, también se propone una opción de compras en línea a través de la página Web del negocio.

El aplicativo deberá contemplar la estructura de la base de datos del sistema de facturación e inventario, sistema de contabilidad y relaciones lógicas de los puntos de ventas, que es donde se aplican las transacciones de ventas.

2. Estas tres interfaces interactuarán con el Sistema integrado de facturación e inventario (SIFE) y servirán como auxiliar para automatizar los siguientes procesos:
  - A. Ingreso de nuevos productos en inventario por cada almacén
  - B. Movimiento de inventarios por procesos: Altas, bajas y cambios
  - C. Conciliación de saldos del Sistema SIFE vs. Sistema de Contabilidad
  - D. Automatizar página Web para el servicio de pedidos en línea
3. La plataforma de desarrollo será Microsoft SQL Server, Microsoft SQL Mobile Edition y Microsoft visual studio.net para las interfaces.
4. La interfaz de escritorio tendrá relación directa con la interfaz móvil PDA y tendrá un módulo de administración de usuarios (seguridad), configuración de parámetros, manejo de los procesos de importación y exportación de la

data de productos, clientes, contabilidad y precios a la interfaz móvil PDA. Esta interfaz permitirá la generación de reportes relacionados con los catálogos del sistema, inconsistencias, movimientos y modificación de productos para la toma de decisiones.

5. Este sistema tendrá dos opciones: inventarios de productos e inventario de activo fijo (este último es para controlar todo el activo fijo de cada almacén), en la que contará con una opción de generación de tablas con datos temporales del activo fijo actualizado en espera de validación por la Oficina de Contabilidad y Personal. Esta interfaz se encargara de la administración de movimientos de activos altas, bajas y (cambios y traslados entre dependencias). Actualmente este proceso es manual se realiza de forma independiente.
6. Por otro lado tendrá que disponer de un Módulo de reportes, encargado de presentar la siguiente información:
  - A. Reportes de Ítems etiquetados por código de almacén, fecha y grupo de activos
  - B. Reportes de catálogos del sistema: usuarios, parámetros generales
  - C. Reportes de ventas por almacén
  - D. Mensajes de alerta por almacén de productos a vencer con al menos dos meses de su fecha de vencimiento
  - E. Reportes de inconsistencias por inventario
  - F. Reporte de datos de activos modificados
  - G. Reporte de movimientos de inventario por almacén
  - H. Reporte de conciliación de saldos de ventas y contabilidad
7. La interfaz móvil tendrá también un módulo de administración de accesos por usuarios (seguridad). Además contará con una opción para la carga de datos desde archivo importación en formato XML a base de datos SQL móvil. Esta interfaz permitirá principalmente la recopilación de los datos de

factura del cliente y tendrá una relación directa con la interfaz de escritorio (PC), para generar la factura de compra.

8. En lo que respecta al inventario de activo fijo se realizará a través de esta interfaz donde se ejecutará el levantamiento de inventario de activo fijo por centro de costo asignado y funcionario o empleado, que permitirá establecer una comparación de inventario de activos asignados por empleado (computadoras personales, mobiliario) versus el inventario de activo fijo de cada punto de venta.
9. La interfaz móvil deberá disponer de una opción de cierre de inventario y exportación de datos en formatos XML, protocolo de comunicación, utilizada entre las interfaces de Escritorio y Móvil que permitirá la carga, descarga, procesamiento y gestión de movimientos de ventas e inventarios.
10. Finalmente se encuentra la interfaz Web (Internet), la cual deberá incluir un módulo de administración de acceso por usuarios (seguridad) y se dividirá en:
  - A. Una aplicación como servicio Web que permitirá mantener el control de pedidos (validación) integrada al Sistema Integrado de facturación e inventario para la compra en línea de productos. Este nuevo servicio se propone diseñar rutas de transporte para la entrega de pedidos a domicilio.
  - B. Una aplicación que brindará las opciones para validación y consulta del inventario de activo fijo asignado por empleado. Esta nueva alternativa de control permitirá responsabilizar a Jefes y empleados de cuidar de los bienes y equipos asignados los que deberán entregar una vez se hayan retirado del negocio.

- C. El alcance de la solución del software involucra impulsar la sistematización de las tres interfaces para cortar a cero el volumen de papelería de las áreas internas e imprimir únicamente aquellas que son de respaldo de comprobantes contables.
- D. Debe incluir y no limitarse a: Lenguaje de programación, componentes de terceros, manejadores de reportes, manejador de base de datos entre otros, además usar en el desarrollo del programa.
- E. Los requerimientos de hardware para desarrollar este sistema, necesita las siguientes características:
- Una Impresora para impresión de códigos de barra para los productos y activos fijos, administrados por el responsable de inventarios que ofrecerá las siguientes características de forma general:
    - 2 MB DRAM, Memoria flash de 2 MB
    - Dual motor impulsada por el diseño de artes
    - Capacidad para 300 metros de cinta de suministro de 1 básico (revestido de lado)
    - 4.3 OD suministro de los medios de comunicación internos, opcional 8.4 externa OD titular de los medios de comunicación.
    - 4 pulgadas por segundo la velocidad de impresión
    - Interfaces serial &USB
    - Software etiquetado incluido
    - 16,000 unidades de etiquetas 2 x 1 metalizadas para activo fijo
    - 2 rodillos para etiquetas (Cantidad aproximada de etiquetas impresas por rodillo: 10 millares de acuerdo a consulta técnica con este tipo de proveedores de servicios).
    - 4 recolectores digitales PDA para el levantamiento de inventario, 2 para el control de movimientos de inventario por el área de inventario y 2 para el control de salidas de productos a otros



almacenes o puntos de ventas, que cumplan con los siguientes atributos y características de forma general:

- Diseño: Ultra compacto (pequeño), fino, ligero menor a 300 g. con excelente ergonomía para ser utilizado con una sola mano.
- Arquitectura madura y estable: Al tener presente un sistema operativo industrial con microprocesador Intel PXA pensado para desarrollo de aplicaciones y alta portabilidad.
- Memoria: Conlleva ranura 5D accesible para Backups y gestionar grandes bases de datos.
- Comunicación: Red inalámbrica WLAN (IEEE 802.15), conexión por Bluetooth®, IEEE 802.11 b/g o WPAN integrado para acceder a cualquier infraestructura de forma inmediata.
- Robustez: Le permitirá soportar caídas desde 1.2 m. y estar expuesto al agua y polvo de acuerdo a protección industrial IP54.
- Versátil: Con una pantalla TFT QVGA a color, táctil, resistente y brillante con teclado numérico tipo teléfono para satisfacer la movilidad.
- Listo para usar: Con soporte de tecnología “Plus & Play”. Este paquete debe incluir una fuente de alimentación y cable mini USB. Por lo general, integra un CD de instalación de software de productividad como terminal emulation (TCL™ y Locked Web Browser™).
- 1 escáner laser de sobremesa utilizado para probar códigos de barra y recepción de activos en inventario, que ofrecerá las siguientes características de forma general:
  - Liviano menor a 150 g
  - Ergonomía de forma de pistola que sea fácil de manipular y usar
  - Soporte de interfaces múltiples: Decodificador de teclado, RS-232-USB
  - Ventana del lector fácil de sustituir

- Tecnología listo para usar “Plus & Play “disponible. El paquete debe incluir un lector (blanco o negro), un cable de interfaz y un soporte “manos libres”
- Compatibilidad con códigos de barras lineales y con las simbologías GS1 DataBar™, el cual es el estándar para aplicaciones generales de lectura de códigos de barras.
- Como soporte flexible disponible para brindar al usuario la opción de utilizar el lector en modo manos libres.
- 1 servidor SQL Server para administración de la base de datos de la interfaz de escritorio PC.

#### 11. Calidad de la interfaz gráfica

La interfaz gráfica debe ser amigable, fácil de usar, consistente y con características de buena visualización con colores adecuados y presentación profesional. Este debe aplicarse también para la documentación de usuario y la ayuda en línea.

#### 12. Seguridad y auditoria

El sistema debe garantizar:

1. Un esquema de seguridad que protejan los datos almacenados en la base de datos de las tres interfaces PC, Móvil PDA y Web, de acceso a la información a través de usuarios, claves y permisos sobre las opciones asignadas a cada usuario.
2. Pistas de auditoría que registren quien realizó cada operación y cuando, que usuario realizó modificaciones y eliminación de datos indicando la fecha y hora.

### 13. Desempeño

La aplicación debe mantener un desempeño adecuado para las operaciones y transmisión de datos, previendo que cuando la base de datos crezca no se degrade su desempeño.

### 14. Entrenamiento

El Ingeniero Informático o la firma desarrolladora del software, deberá brindar entrenamiento con énfasis práctico para los usuarios finales en la utilización del sistema integrado, con una duración mínimo de 8 horas previa realización de pruebas.

También deberá brindar capacitación técnica para manejo de código fuente, diseño de la base de datos, procedimientos de transmisión de datos, configuración e instalación del sistema, entre otros, al Departamento de Informática de la Distribuidora con duración mínima de 25 horas.

### 15. Adaptabilidad al cambio – flexibilidad – parametrización

El sistema deberá ser diseñado de forma tal que los requerimientos de cambios de los usuarios puedan ser integrados de la forma más rápida y segura. El sistema resultante debe facilitar la adaptación a cambios requeridos a corto o mediano plazo, es decir, que sea de fácil mantenimiento. Por ejemplo, no debe ser necesario hacer modificaciones en el código fuente del programa para cambiar alguna dependencia de los puntos de ventas y reportes asociados.

16. Plataforma (lenguaje de programación, gestor de base de datos, sistema operativo)

El software debe ser desarrollado en un lenguaje de última generación de preferencia “código abierto”, robusto, que permita una fácil y rápida programación, que sea conocido en el ámbito nacional.

Se debe usar un manejador de base de datos relacionales robustas y de buena capacidad de procesamiento.

17. Transmisión de datos

A. Presentar el esquema de seguridad a nivel de la transferencia de la data en los procesos de Exportación e Importación entre las interfaces PC, Móvil y PDA a utilizarse para garantizar la confidencialidad, integridad y disponibilidad oportuna para los datos registrados.

B. Definir y documentar la configuración requerida para la seguridad debida a la base de datos local de carácter temporal.

C. Debe considerarse para la trasmisión de datos el uso de Web Services.

Asegurar pruebas de transmisión y sincronización de datos con volúmenes de datos similares a los que serán transmitidos regularmente debe ser realizado a satisfacción del personal del Departamento de Informática.

#### **4.18 Plan de continuidad del negocio**

Las Normas Jurídicas de Nicaragua establecen requisitos para uso de sistemas de facturación computarizadas – Disposición técnica n° 09-2007, en la que establece que cada negocio debe contener un Plan de Continuidad del Negocio, en vista que la Distribuidora no posee este vital instrumento, la Maestrante ha propuesto un Plan de Continuidad cuyo propósito principal es salvaguardar la integridad del Sistema de Facturación así como aquellos procesos asociados, para dar una capacidad de respuesta ante situaciones de emergencia, incluso en las extremas, mediante la práctica de acciones preventivas de mitigación de riesgos que se presenten, para evitar la discontinuidad de las actividades y no afectar el cierre de operaciones de ventas. Ver anexos N° 5 y 6 (Norma Jurídica de Nicaragua y Plan de continuidad del negocio).

## **Capítulo V: CONCLUSIONES Y RECOMENDACIONES**

### **5.1 Conclusiones**

Debido a la gran competencia que existe en el mercado, los socios de la Distribuidora Tropical del Pacífico, S.A, desean ampliar su mercado con altos estándares de calidad para ser competitivos y alcanzar mayores márgenes de ganancias. De esta manera se beneficia la propia compañía, como también sus clientes antiguos y futuros, porque una empresa bien organizada trabaja con más rapidez y con mejor calidad; por tal motivo, la Junta Directiva de este negocio, desea ampliar su mercado en otras zonas de Nicaragua, ante este reto, solicitó un Diagnóstico del desempeño del Sistema de facturación actual, para tomar decisiones sobre su viabilidad de integrarse en los futuros puntos de ventas a impulsar o invertir en un nuevo Sistema integrado de Facturación.

Tomando como base los lineamientos antes citados por la Junta Directiva de la Distribuidora, se analizó la arquitectura lógica, física y de seguridad del sistema de facturación, en la que se concluye que no existe posibilidad de escalamiento del sistema en estudio para su interconexión en una red corporativa, debido a las limitaciones que tiene el lenguaje de programación que fue utilizado en su desarrollo e implementación así como el gestor de base de datos.

Otro aspecto fundamental que se evaluó, es la identificación de las amenazas y estimación de los riesgos del proceso de facturación y aquellos procesos vinculantes, obteniendo como resultado que el nivel de riesgo inherente para la seguridad informática es alto y medio y los controles internos son bastante frágiles en relación a la Norma internacional para la seguridad de la información ISO/IEC 27002. Sin embargo, en los eventos de riesgos identificados se propuso tratamientos de riesgos.

Con el propósito de contribuir al fortalecimiento de la Distribuidora, se elaboró las siguientes estrategias: Perfil del proyecto del Sistema integrado de facturación e inventario, con interfaz al Sistema de contabilidad, cuyos alcances y requerimientos sería un gran desafío para la Distribuidora en caso de desarrollarse

e implementarse esta propuesta de Sistema, ya que ofrece como beneficios esperados, que todos los productos sean con códigos de barras, pueda ser integrado en todos los puntos de ventas del país y obtener incluso indicadores de medición de ventas, por almacén y global, además que se integraría el inventario de mercadería y activos fijos, la facturación podría hacerse mediante un dispositivo móvil (PDA) que tendrían asignado los ejecutivos de ventas, evitando largas filas para facturar el producto, otro nuevo servicio que ofrecería serían las ventas por Internet, a través de la conexión del sistema a una página Web de la Distribuidora, así como atributos de seguridad física y electrónica con estándares internacionales de la ISO/IEC 27002.

Además del perfil del proyecto del sistema integrado, se propuso un Plan de continuidad del negocio, con el propósito de tomar las medidas antes de la materialización de un riesgo o bien una vez ocurrido el evento y evitar la discontinuidad operacional.

Es importante destacar, que los riesgos siempre cohabitan continuamente con el diario quehacer, siempre están latentes, aun cuando no se les pueda o no se los quiera identificar. Sin embargo, el éxito de la Distribuidora, será que sus altos ejecutivos estén conscientes de que la administración del riesgo informático debe ser una actividad priorizada y llevada a la par de implementaciones de nuevas tecnologías o de nuevos sistemas de información.

## 5.2 Recomendaciones

La tecnología es un punto clave en este nuevo milenio. Básicamente los negocios que no han optado por esta opción se están quedando atrás. Los mismos clientes están exigiendo esta nueva herramienta ya que la palabra tecnología es sinónimo de rapidez y esto conlleva a agilizar la distribución y despacho de los productos y/o servicios que se ofrecen en un mercado altamente competitivo.

Por lo antes expuesto, se recomienda a los altos ejecutivos de la Distribuidora, invertir en la compra del Sistema Integrado de facturación e inventario de acuerdo a la propuesta del Perfil del proyecto presentado, además de lo anterior, se requiere que realicen una significativa inversión en herramientas de seguridad informática para robustecer la actual plataforma tecnológica, debido al incremento del crimen cibernético que pueda paralizar las operaciones del negocio e incluso llevarlo a la quiebra.

Ante el crecimiento de la empresa, es conveniente la contratación de una firma de auditores para que puedan realizar auditorías informáticas, a fin de monitorear que tan efectivos y eficientes se están manejando estos recursos tecnológicos y cómo proteger a los socios ante una colusión interna para el fraude por la vía informática.

Debido a que los riesgos cohabitan continuamente, es necesario crear un Comité de Riesgo y capacitar al personal en este tema, para tomar las acciones oportunas antes de que ocurra un siniestro, siendo necesaria la creación de un Centro de Datos Alternos, ante una materialización de riesgos que pueda paralizar las operaciones por un tiempo mayor a cinco días, para lo cual se recomienda la implementación del Plan de Continuidad Operacional.

Es necesario la capacitación permanente del personal y políticas de incentivos de producción con el ánimo de disponer de un capital humano leal, comprometido y con excelencia.



# **ANEXOS**

## CUESTIONARIO SOBRE SEGURIDAD DE LA INFORMACIÓN

El objetivo del control de seguridad de información a través de este cuestionario, es identificar cualquier debilidad potencial a fin de minimizar el impacto de pérdidas y desastres.

### PRACTICAS DE INFORMACIÓN

Responda a la derecha de cada pregunta, hay cuatro posibles respuestas: Si, No, NA (no aplica), D (Desconozco).

#### Conocimiento de la seguridad de información

1. ¿Tiene la Distribuidora un grupo formal de políticas de seguridad de la información?  
SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_
2. ¿Hay curso de adiestramiento a los nuevos empleados sobre políticas de Seguridad de la Información?  
SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_
3. ¿Se capacita a los empleados para el eficiente manejo de los sistemas que interactúan?  
SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_
4. Al salir de vacaciones los empleados con acceso a sistemas o cuando renuncian, ¿Se les deshabilita de forma automática los acceso?  
SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

#### Control de acceso

5. ¿La Distribuidora tiene prácticas que aseguren el uso de contraseñas fuertes ("Strong passwords")?  
SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

6. ¿Están protegidos los sistemas de información por un nivel sencillo de autenticación?

SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

7. ¿Están protegidos los sistemas de información por un nivel múltiple de autenticación?

SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

### Análisis de riesgos

8. ¿Se realiza un análisis de riesgos de la seguridad electrónica regularmente?

SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

9. ¿Se realiza mitigación del riesgo de la vulnerabilidad electrónica regularmente?

SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

10. ¿Se realiza mitigación de riesgo de la vulnerabilidad física regularmente?

SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

### Seguridad electrónica

11. ¿Están los archivos primarios de información encriptados?

SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

12. ¿Se realizan rutinariamente copias de resguardo (“backup”) de los archivos de información?

SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

13. ¿Están encriptados las copias de resguardo (“backup”) de información?

SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

14. ¿La conexión de red externa tiene una protección de acceso (“firewalls”)?

SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

15. ¿Tienen conexión de red que cruce la protección de acceso (“firewalls”) organizacionales?

SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

Protección continúa

16. ¿Hay un proceso continuo para asegurarse que todas las computadoras tienen las últimas actualizaciones aplicadas a sus sistemas operativos?

SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

17. ¿Hay un proceso continuo para asegurarse que todas las computadoras tienen las últimas actualizaciones de seguridad aplicadas a sus programas de aplicación?

SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

18. ¿Hay un proceso continuo para asegurarse que todas las computadoras tienen las últimas actualizaciones de sus programas de protección de virus?

SI\_\_\_ NO\_\_\_ NA\_\_\_ D\_\_\_

## Anexo 2

### DISTRIBUIDORA TROPICAL DEL PACÍFICO, S.A.

#### CUESTIONARIO DE CONTROL INTERNO A JEFE DE DIRECCIÓN DE INFORMÁTICA

#### TEMA: ADMINISTRACIÓN DEL EQUIPO INFORMÁTICO Y RED INSTITUCIONAL

N°	PREGUNTAS	SI	NO	NA	D	RESPUESTA
1	¿Tiene usted conocimientos de las políticas, normativas y procedimientos relacionados a la administración del equipo de cómputo y red informática?				X	Desconozco
2	¿Existe sistema informático para el control del equipo informático, componente de red que es retirado para efectuar reparaciones por empresas de servicios fuera de las instalaciones de la Distribuidora?	X				Existe pero los niveles de seguridad son bajos debido a los avances de la tecnología información, siendo necesario realizar inversiones para las adquisiciones de estos equipos.
3	¿Cómo se procede para la salida de algún equipo informático o componente de red que es retirado para efectuar reparaciones por empresas de servicios fuera de las instalaciones de la Distribuidora?	X				Generalmente se realizan las reparaciones a lo interno de la empresa, otras veces se hace una hoja de salida en donde firma el técnico de la empresa externa que hará la reparación y jefe de informática.
4	¿Existe un listado del equipamiento informático, componentes de red o dispositivos para la seguridad física que se encuentra fuera de las instalaciones por motivos de reparaciones o préstamos?		X			

N°	PREGUNTAS	SI	NO	NA	D	RESPUESTA
5	¿Cómo procede para la verificación, especificaciones técnicas y estado del equipo informático que ingresa como adquisición (compra o licitación)?	X				Se realizan pruebas técnicas y se revisan sus especificaciones, caso contrario se realizan los reclamos con la empresa.
6	¿Codifican los equipos informático, componentes de red y dispositivos de comunicación electrónica propiedad de la Distribuidora?	X				Se asignan códigos y se lleva un inventario con su asignación del personal que tiene bajo su responsabilidad caso específico las computadoras.
7	¿Efectúa el Departamento de Administración, arqueos aleatorios frecuentes para el control del equipamiento informático, componentes de red y dispositivos de comunicación electrónica?		X			No se realiza
8	¿Existe un listado de equipos informáticos, componentes de red y de seguridad que cumplieron su vida útil o en mal estado técnico que impide su reactivación y su costo de recuperación sea muy alto, que han sido retirados de las Áreas para ser dados de Baja?	X				Se lleva un inventario actualizado por parte de la Dirección, según las órdenes de entrada y retiro.
9	¿Tiene usted algún comentario adicional relacionado a la Administración del equipo informático y red de la Distribuidora?		X			

**DISTRIBUIDORA TROPICAL DEL PACÍFICO, S.A.**

**CUESTIONARIO DE CONTROL INTERNO A JEFE DE DIRECCIÓN DE INFORMÁTICA**

TEMA: Administración de Base Datos del Sistema de Facturación

N°	PREGUNTAS	SI	NO	NA	D	RESPUESTA
1	¿Quién es el responsable de Administrar las Bases de Datos y los respaldos de estas?					Ing. Emiliano Chacón López
2	¿La Distribuidora cuenta con herramientas de Software especializada en comparar programas fuentes y código ejecutable de los Sistemas en Producción?		X			Actualmente no posee porque solo tres sistemas posee: Sistema de contabilidad, Sistema de facturación y Sistema de Inventario
3	¿Han existido eventos imprevistos que hayan puesto en riesgo la seguridad de la información contenida y procesada en el sistema de facturación? Comentar.	X				En algún momento se aplicaron cortes de energía en la zona por desperfectos de un trasmisor, esto implicó que duró la reparación más de dos días y la planta energética de emergencia era de muy poca capacidad para mantener los refrigerantes y conexión de sistemas, lo que provocó daños en algunos productos y las baterías de las computadoras se desactivaron por el prolongado fallo de la energía. No obstante, a raíz de esta problemática se adquirió e instaló una planta de emergencia con mayor capacidad.
5	¿Qué funciones de supervisión/monitoreo ejecuta informática en el proceso de administración de Base de Datos?	X				Coordinar la instalación y configuración de software de base de datos por actualización del producto o renovación de servidores. Planificar los respaldos en coordinación con el Analista de sistemas y verificar su correcta ejecución, así como la realización de pruebas de verificación de su funcionalidad. Analizar la plataforma tecnológica y gestionar renovación y compra de software asociado.

N°	PREGUNTAS	SI	NO	NA	D	RESPUESTA
1	¿Quién es el responsable de Administrar las Bases de Datos y los respaldos de estas?					Ing. Emiliano Chacón López
2	¿La Distribuidora cuenta con herramientas de Software especializada en comparar programas fuentes y código ejecutable de los Sistemas en Producción?		X			Actualmente no posee porque solo tres sistemas posee: Sistema de contabilidad, Sistema de facturación y Sistema de Inventario
6	¿El área de informática cuenta con personal capacitado en Administración y Seguridad de Base de Datos?	X				Existe un ingeniero que tiene más de años de experiencia en el campo.
7	¿Se cuenta con una herramienta de software de control/monitoreo, que permita supervisar en líneas las actividades que desarrolla el administrador de Base de Datos?		X			No se tiene dado que la Distribuidora no dispone de muchos sistemas automatizados.
8	¿Existe un plan de continuidad informática?			X		Solo se tiene las funciones de los puestos de trabajo.
9	¿Actualiza periódicamente los Diagramas de Entidad Relación Versus las relaciones de tablas y campos establecidas a nivel de Base de Datos en línea?		X			Nunca se ha hecho.
10	El área cuenta con un Manual de Procedimientos Administrativos para Administrar la Base de Datos.	X				Esta desactualizado con respecto a las nuevas disposiciones que se aplican.
11	¿Qué mecanismos utilizan para la recuperación de respaldos?	X				Procedimientos de respaldo de rutina.



## **Seguridad de la Información ISO 27001**

Protección de la información, el activo más valioso

¿Por qué la norma ISO 27001 es útil para la gestión de la seguridad de la información?

La ISO 27001 es norma adecuada para mejorar la posición de mercado de las organizaciones, también ayuda a organizar todas las actividades de seguridad de la información dentro de un marco claramente definido, y por consiguiente, disminuirá los niveles de riesgos.

Esta norma permite disminuir el tiempo necesario para determinar cómo establecer un sistema para planificar la implementación, evaluar y tratar los riesgos, involucrará a la dirección en momentos cruciales y permitirá el cumplimiento de objetivos

La norma ISO 27001 muestra todo su potencial si se aplica a lo largo de todo el proceso del proyecto de seguridad de la información: desde la planificación e implementación de todas las actividades hasta su medición para evaluar si alcanzaron los objetivos deseados.

La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la

seguridad de la información se ha implementado en esa organización de la mejor forma posible.

A raíz de la importancia de la norma ISO 27001, muchas legislaturas han tomado de la protección de datos personales, protección de información confidencial, protección de sistemas de información, gestión de riesgos operativos en instituciones financieras, etc.

Cuatro fases del sistema de gestión de seguridad de la información:

La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información. Un sistema de gestión de este tipo, igual que las normas ISO 9001 o ISO 14001, está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

Las fases son las siguientes:

- La fase de planificación: esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles).
- La fase de implementación: esta fase implica la realización de todo lo planificado en la fase anterior.
- La fase de revisión: el objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos “canales” y verificar si los resultados cumplen los objetivos establecidos.
- La fase de mantenimiento y mejora: el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

### **Documentos de ISO 27001**

La norma ISO 27001 requiere los siguientes documentos:

- El alcance del SGSI.
- La política del SGSI.
- Procedimientos para control de documentación, auditorías internas y procedimientos para medidas correctivas y preventivas.
- Todos los demás documentos, según controles aplicables.
- Metodología de evaluación de riesgos.
- Declaración de aplicabilidad.
- Plan de tratamiento del riesgo.

Otras normas relacionadas con la seguridad de la información

Además de la ISO 27001, la norma ISO 27002 es una norma auxiliar que proporciona más información sobre como implementar los controles de seguridad especificados en la ISO 27002.

**Normas Jurídicas de Nicaragua**

**Materia:** Tributario

**Rango:** Normas Técnicas

**REQUISITOS PARA USO DE SISTEMAS DE FACTURACIÓN COMPUTARIZADAS**

**DISPOSICIÓN TÉCNICA No. 09-2007.** Aprobada el 23 de Mayo del 2007  
Publicada en La Gaceta No. 134 del 16 de Julio del 2007

El suscrito Director General de Ingresos en uso de las facultades que le confieren el Arto 223 numeral 3 de la Ley 562 Código Tributario de la República de Nicaragua (CTr.) y sus reformas publicado en la Gaceta Diario Oficial No. 177 del 23 de Noviembre del 2005.

**CONSIDERANDO**

**I**

Que es necesario regular y definir el procedimiento para autorización y uso del sistema de facturación computarizado de los contribuyentes y responsables, dedicados a cualquier actividad económica que deseen utilizar este sistema a fin de soportar sus transacciones por ventas de bienes, prestación de servicios e importaciones.

**II**

Que los contribuyentes o responsables conforme lo establecido en el Arto 81 y 126 numeral 4 del CTr. podrán solicitar autorización para utilizar sistemas en medios electrónicos para emitir sus facturas de las actividades y operaciones que se vinculen con los tributos.

**DISPONE:**

**PRIMERO:** De conformidad al Arto.81 CTr. todo contribuyente o responsable podrá hacer uso de medios electrónicos de información, para facturar sus enajenaciones, servicios en general e internaciones previa autorización avalada

por auditores del Departamento de Fiscalización de la Dirección de Grandes Contribuyentes o Administración de Rentas según corresponda.

**SEGUNDO:** La solicitud de autorización del uso de Sistemas de Facturación Computarizado deberá cumplir con los requisitos siguientes:

Indicar el primer día del mes en que dará inicio con la aplicación del sistema (señalando día, mes y año)

1.2 Detallar datos generales del sistema:

- a. Nombre del sistema.
- b. Lenguaje en que fue desarrollado.
- c. Informar si poseen programas fuentes.
- d. Informar si el sistema está integrado a otros módulos, indicando cada uno de ellos.
- e. Nombre del autor y/o proveedor del sistema, número RUC, número de cédula de identidad si es persona natural, dirección, país, teléfono, correo electrónico. El número RUC y cédula de identidad no serán necesarios si el proveedor es extranjero.
- f. Fecha en que fue adquirido el sistema. Adjuntar fotocopia de la factura de compra o contrato de asistencia técnica.

**1.3 Seguridad de Acceso:** El acceso al sistema debe estar controlado mediante nombre y clave de usuarios.

**1.4 Respaldo de Soportes:** Garantizar el respaldo de la información en medios magnéticos. Este deberá efectuarse para resguardar la información de las operaciones diarias.

**1.5 Manuales:** Debe disponer de un manual técnico y un manual de usuario en español.

**1.6 Notificación de Imprevistos:** Cualquier variante, modificación o cancelación del sistema deberá ser previamente notificado a la Dirección de Grandes Contribuyentes o Administración de Rentas según corresponda, adjuntando la documentación soportes correspondientes, para su debido control y posterior verificación.

**1.7 Numeración de Facturas:** Garantizar la continuidad numérica de las facturas, la numeración debe ser inalterable, en caso de usar formato pre impreso se debe garantizar que la numeración sea igual a la emitida por el sistema, diferenciando la factura de contado o crédito.

**1.8 Formalidades de Facturas:** Toda factura deberá cumplir con lo establecido en el Decreto 1357 "Ley para el control de las facturaciones- o "Ley de pie de imprenta fiscal," (número RUC, orden de trabajo de la imprenta, fecha de emisión, cantidad de libretas y numeración correlativa). Además debe reflejarse en el encabezado de la factura nombre completo de la persona natural o jurídica, ubicación del negocio, número telefónico, nombre comercial si lo tiene, así mismo indicar si es factura de contado o crédito, o si el formulario reimpresso es para los dos tipos de facturas. Estas facturas deberán ser elaboradas en las imprentas autorizadas indicadas en la página Web de la DGI.

**1.9 Desglose de Impuestos:** Conforme Arto. 61 numeral 5) de la Ley de Equidad Fiscal, se emitirá la factura con el valor de las operaciones gravadas, señalando en ella, expresamente y por separado, el IVA que se traslada, en la forma y con los requisitos establecidos en las leyes fiscales vigentes.

**1.10 Anulación de Facturas:** Toda factura que se anule por cualquier razón, deberá conservarse la factura original con todas las copias pre impresas sin excepción alguna, estampando en cada una de ellas el sello de anulado.

**1.11 Cantidad de Copias:** Cuando una Distribuidora adopte el sistema de facturación pro forma, esta deberá imprimirse en original y copia, así como tener

pre impreso "Factura Pro forma", la que no tendrá ningún valor para efectos de aplicación del impuesto, ni de trámites ante instituciones de la policía, ni de ninguna índole. Su único propósito es informar al cliente sobre el precio de los productos, servicio u otros que estimen conveniente.

**1.12** Adjuntar en la solicitud de autorización una copia del formato (muestra) de la factura computarizada a utilizar.

**TERCERO:** Otras consideraciones a tomar en cuenta.

### **3.1 Sucursales o agencias:**

Los **contribuyentes** y responsables que establezcan sucursales o agencias en cualquier parte del territorio nacional, deberán tener formularios con numeración consecutiva en concordancia con su casa matriz a partir del número uno, diferenciándose ésta a través de una serie.

### **3.2 Recibos de caja:**

En los casos que el contribuyente para el cobro de sus servicios no adopten el sistema de facturación, y emitan recibos de caja, estos deberán cumplir con todos los requisitos establecidos para la facturación, con la salvedad de que siempre equivaldrán a factura de contado. En estos recibos de caja deberá desglosarse el valor de la venta y/o servicio, así como el impuesto al valor agregado (IVA).

Los contribuyentes y responsables que tienen sistema de facturación por venta al crédito, el recibo de caja servirá para justificar la recepción del abono o cancelación de las mismas o de otros conceptos.

### **3.3 Plan de contingencia:**

En casos de posibles fallas del equipo computarizado o falta de energía eléctrica y el contribuyente tenga la necesidad de facturar procederá de la siguiente manera:

a. Mantener un stop de facturas reimpresas que reúnan los requisitos señalados en el ordinal segundo numeral 1.8 de esta Disposición Técnica, la numeración correlativa del stop de facturas en existencia deberá ser diferente a la utilizada en el sistema de facturación computarizado. Debe reportar a la Dirección de Grandes Contribuyentes o Administración de Rentas, la numeración correlativa de estas facturas.

b. Proceder a utilizar las facturas pre impresas ya sea a máquina de escribir o manualmente entregándole la factura original al cliente, una vez superado el problema de facturación deberá proceder a ingresar al sistema de facturación computarizado las facturas elaboradas manualmente e indicar con una nota el número de la factura manual que corresponde a esa factura elaborada, así como deberá imprimir la factura computarizada en original y copia, adjuntando como soporte la copia de la facturación manual.

### **3.4 Devoluciones y/o anulaciones:**

Cuando se efectúen devoluciones y/o anulaciones de facturas en días posteriores al de la fecha de facturación original, es decir que no son anulaciones en el mismo día, se procederá de la siguiente manera:

a. Elaboración de nota de crédito; correspondiente para efectuar anulación de factura Arto. 46 Ley de Equidad Fiscal y Arto. 102 de su Reglamento. Si el sistema de facturación está integrado al sistema de Inventario, el proceso de la nota de crédito deberá revertir el descargo-del inventario y/o almacén, mediante comprobante que detalle el concepto de dicha operación con numeración consecutiva y fecha en que se efectuó.

b. No hacer anulaciones en formularios de facturas computarizadas por las devoluciones que le efectuaron en días posteriores al de la fecha de facturación original.



**CUARTO:** La Dirección de Grandes Contribuyentes o Administración de Rentas que corresponda, emitirá carta de autorización para uso del sistema de facturación computarizado, previa verificación de los datos suministrados por el contribuyente, indicados en el ordinal segundo de la presente Disposición Técnica.

**QUINTO:** Los contribuyentes autorizados para utilizar sistema de facturación computarizado deberán registrar el número de autorización otorgado por la DGI en la parte inferior derecha de cada factura.

**SEXTO:** Autoridades fiscales debidamente identificadas de la Dirección General de Ingresos, verificarán el cumplimiento de las obligaciones descritas en los ordinales anteriores, de conformidad a las facultades que le otorga el Arto. 148 numeral 5) del Código Tributario.

**SÉPTIMO:** Los contribuyentes que no cumplan con lo descrito en la presente Disposición Técnica o con lo establecido en el Arto. 126 numeral 4) del Código Tributario serán sancionados conforme lo indicado en el Arto. 127 numeral 2) del Código Tributario.

**OCTAVO:** La presente Disposición Técnica sustituye el Comunicado No. 012-2000 del 13 de febrero del 2000 y entra en vigencia a partir de su publicación en dos medios de comunicación escrito de circulación nacional sin detrimento de su posterior publicación en la Gaceta Diario Oficial.

Dado en la ciudad de Managua, a los veintitrés días del mes de Mayo del año dos mil siete. WALTER PORRAS, DIRECTOR GENERAL DE INGRESOS.

-

---

**Asamblea Nacional de la República de Nicaragua  
Complejo Legislativo Carlos Núñez Téllez. Avenida Bolívar.**

Enviar sus comentarios a: [División de Información Legislativa](#)

**Nota:** Cualquier Diferencia existente entre el Texto de la Ley impreso y el publicado aquí, solicitamos sea comunicado a la División de Información Legislativa de la Asamblea Nacional de Nicaragua.

## **Plan de Continuidad del Negocio**

### **INTRODUCCIÓN**

La información es considerada el principal activo de las empresas por esta razón, contar con un respaldo de información o back-up —como también se le conoce— es una inversión segura si se considera que la pérdida de datos claves puede repercutir en la estabilidad y continuidad de la empresa.

Hoy en día, las organizaciones deben estar preparadas para afrontar las múltiples amenazas que ponen en riesgo su operatividad y, en consecuencia, la continuidad del negocio, elementos adversos como un incendio, terremoto, huracán o asaltos con fuerza pueden ocurrir. Sin embargo, no es necesario un desastre de dimensiones parecidas a las mencionados anteriormente para poner en peligro no sólo la buena marcha del negocio sino su misma supervivencia; eventos como la invasión de un virus o la caída de un sistema pueden conducir a la paralización temporal de los sistemas automatizados, la pérdida de información crítica o, en última instancia, la inutilización de las infraestructuras informáticas.

Para asegurar la continuidad del negocio, se requiere realizar una evaluación de la situación actual, a fin de identificar los servicios y recursos tecnológicos, entender los riesgos, sus causas e impactos y definir planes de continuidad. Por tanto, considerando el interés y suma importancia para la Empresa, se realizó Diagnóstico informático del Sistema de Facturación en la Distribuidora Tropical Del Pacifico S.A, enfatizando en la evaluación de algunos componentes, a partir de los cuales, se identificó la necesidad de disponer de un Plan de Continuidad del Negocio, para responder ante riesgos operativos y tecnológicos.

El Plan de Continuidad del Negocio, tiene como propósito principal salvaguardar la integridad del Sistema de Facturación, para dar una capacidad de respuesta ante situaciones de emergencia, incluso en las extremas, mediante la práctica de

acciones preventivas de mitigación de riesgos que se presenten, para evitar la discontinuidad de las actividades y no afectar el cierre de operaciones de ventas, así como, estrategias para la operatividad de la Distribuidora en la que involucra a toda la organización.

El presente Plan de Continuidad del Negocio, establece los lineamientos institucionales, o estrategias que deberá seguir la Distribuidora, en los próximos años, con el fin de mantener su vigencia. Para lo cual, deberá ser revisado y actualizado por posibles cambios internos y externos asociados a la organización que puedan demandar esfuerzos ante nuevos riesgos o amenazas.

## OBJETIVO

Asegurar razonablemente la continuidad de los procesos de facturación y venta y, por ende, los servicios críticos de la Distribuidora ante un evento que cause una interrupción no planeada a sus operaciones normales, así como definir los mecanismos que permitan prevenir o mitigar el riesgo de fallas o desastres que puedan afectarle.

### 1. DEFINICIONES TÉCNICAS

Término	Definición
Centro de Datos Alternos	Es un local alterno ( <i>fuera de la empresa</i> ) donde se almacena un servidor con réplica de datos en tiempo real de todos los movimientos de un sistema, de manera que si ocurriera una interrupción por ataque de un hacker o un virus troyano, o robos que causaron daños a los equipos de cómputo, se pueda usar este servidor y demás componentes informáticos ubicados en el Centro de Datos Alternos. Gabriel Díaz Orueta, Francisco Mur

Término	Definición
	Pérez, Elio Sancristóbal Ruiz, Manuel Alonso Castro Gil & Juan Peire Arroba (2012)
Plan de Continuidad del Negocio	Un plan claramente definido y documentado a ser utilizado en una situación de emergencia, evento, incidente o crisis. Usualmente un plan considera la recuperación de recursos, servicios y acciones necesarias a realizar con personal clave, que son requeridas para manejar el proceso. Juan Gaspar Martínez (2010).
Análisis de Impacto al Negocio	Es un análisis a nivel ejecutivo por medio de la cual una organización determina de manera cuantitativa y cualitativa impactos, efectos, y pérdidas que podrían resultar si la organización sufre un evento serio. Establece las funciones y procesos críticos, sus prioridades de recuperación e interdependencias a fin de determinar tiempos de recuperación objetivo y puntos objetivos de recuperación. Los resultados son utilizados para la toma de decisiones respecto a las estrategias de recuperación. J. Gaspar (2004).
Crisis	Una ocurrencia o percepción de un evento o situación que amenaza las operaciones, personal, valor accionario, accionistas, marca, reputación, confianza, y/o cualquier riesgo estratégico que afecte los objetivos del negocio. J. Gaspar (2004).
Desastre	Un evento catastrófico repentino no planeado que causa daños o pérdidas irreparables que compromete la disponibilidad de funciones críticas, procesos o servicios por un período de tiempo de manera no aceptable. J. Gaspar (2004).
Posible Desastre	Ha ocurrido una falla en el área que ha paralizado el

<b>Término</b>	<b>Definición</b>
	proceso, pero todavía está en evolución. Es una alerta, solo se pide que se informe de la situación actual, para tomar las acciones correspondientes pero no implica movilización de personal. J. Gaspar (2004).

## 2. Integración de comité

A fin de contar con una instancia organizada para la toma de decisiones en materia de riesgo y gestión de continuidad, existirá un Comité de Administración Riesgos y Continuidad, estará conformado por el siguiente personal:

<b>Nombres y apellidos</b>	<b>Cargo</b>	<b>Teléfono de Oficina</b>	<b>Teléfono de casa</b>
Leonardo Jerez	Gerente	22435469	26435469
Juan Pérez	Jefe de Protección Física	22485419	22435469
Eliseo Picado	Jefe Departamento Administración y Finanzas	24447631	23546893
Juan Maradiaga	Jefe Departamento de Informática	23457631	2556893
Carlos Aráuz	Jefe Departamento de Ventas	28347631	23546893
Martín Urrutia	Miembro de la brigada contingente	24847631	23546893
Danilo Rodríguez	Miembro de la brigada contingente	22435469	26435469
Bismarck Martínez	Miembro de la brigada contingente	24447031	24546893

### **3. Funciones del comité de administración del riesgo y continuidad**

- a) Fomentar una apropiada cultura de gestión de riesgos en la Distribuidora, para minimizar inseguridades ante eventos fortuitos.
- b) Evaluar y definir los procesos críticos de la Distribuidora en conjunto con las áreas involucradas.
- c) Elaborar metodología de gestión de riesgos y someter a aprobación por las autoridades superiores de la Distribuidora.
- d) Aprobar los niveles de tolerancia al riesgo por categorías de impacto y la metodología para la aplicación de la gestión de riesgos.
- e) Velar porque la Metodología de Gestión de Riesgo sean implementadas y mantenidas en todos los niveles de la Distribuidora.
- f) Revisar y recomendar los límites generales y específicos de exposición al riesgo.
- g) Sugerir a la Gerencia los mecanismos necesarios de control interno que faciliten el cumplimiento del Plan de continuidad del negocio.
- h) Monitorear los riesgos que impacten los objetivos de la Distribuidora como consecuencia de sus operaciones, a fin de recomendar las medidas adecuadas para mitigar los mismos.
- i) Tomar las medidas correctivas que se consideren con las dependencias que no muestren el nivel de avance esperado o ante la ocurrencia de un evento que impacte de manera considerable los intereses de la Distribuidora.
- j) Rendir informes y reportes periódicos a la Gerencia sobre el nivel de ejecución del Plan de continuidad del negocio, así como informar de manera oportuna la ocurrencia de eventos, incidentes, excepciones o pérdidas que afecten a la Distribuidora.

- k) Mantener una estrecha comunicación y coordinación con el equipo ejecutivo de las áreas organizativas de la Distribuidora, para establecer controles adecuados que mitiguen el riesgo dentro de los procesos.

#### **4. Roles y responsabilidades de las áreas**

##### **A. Gerencia**

La Gerencia General será la responsable de la implementación y seguimiento razonable de la Continuidad de las operaciones en la Distribuidora, considerando de manera específica las siguientes responsabilidades:

1. Tomar las provisiones necesarias ante la posible ocurrencia de eventos no previstos, que pudieran afectar la operatividad del negocio.
2. Tomar las decisiones pertinentes ante la ocurrencia de eventos que requieran de acción inmediata.
3. Establecer mecanismos que aseguren una adecuada comunicación para coadyuvar a la continuidad de las operaciones ante situaciones de emergencia.
4. Asegurar que el personal directivo esté oportunamente informado de los cambios que ocurran en el Plan de Continuidad del Negocio.
5. Apoyar al Comité de Administración de Riesgo y Continuidad en los aspectos referentes a la continuidad de las operaciones del negocio.

##### **A. Unidades organizativas**

Cada dependencia de la Distribuidora participará activamente en la implementación del Plan de Continuidad del negocio y designará un interlocutor o enlace con el Comité de Riesgo y Continuidad, para estos fines. Considerarán de manera específica los siguientes roles:



1. Conocer la ubicación y recursos disponibles del sitio alternativo de trabajo.
2. Conocer adecuadamente el Plan de Continuidad del Negocio, a fin de estar preparadas adecuadamente ante la ocurrencia de un posible desastre.
3. Tomar las medidas de aseguramiento correspondientes a su dependencia para ejecutar acciones en beneficio del personal y de la Distribuidora ante la ocurrencia de un evento de desastre.
4. Conocer adecuadamente el esquema de escalamiento, notificación y activación del Plan.
5. Identificar claramente los miembros primarios de los procesos, así como los miembros suplentes para cada proceso y mantener actualizada la lista de contactos.
6. Colaborar en la elaboración del Análisis de impacto al Negocio.
7. Participar activamente en las pruebas y ejercicios de continuidad.
8. Participar activamente en las campañas de capacitación y concientización.
9. Identificar cambios significativos en sus dependencias y determinar en conjunto con el Comité, la necesidad de actualización del Plan de Continuidad.

## 5. Estrategias de respuesta antes de la materialización de riesgos

A continuación se presentan los diferentes escenarios considerados dentro del alcance del presente Plan de Continuidad del Negocio que contempla las estrategias o acciones a implementar así como los responsables de asegurar su ejecución.

### 5.1 Estrategias preventivas para minimizar Crisis generales antes de que ocurran.

- i) **Responsabilidad del Jefe de Protección Física: Asegurar el** mantenimiento y operatividad de los siguientes elementos:

Acciones	Fechas de cumplimiento
1. Mantener en constante entrenamiento al personal de vigilancia.	Enero - Diciembre
2. Armas de Fuego en excelente estado.	Enero - Diciembre
3. Actualizar el Sistemas de señalización y alarmas de evacuación.	Enero y Diciembre
4. Instalar sistema automático contra incendios (extintores, detectores de humo, hidrantes).	Enero - Diciembre
5. Sistemas de comunicación de alertas (por ejemplo, para casos de huelgas en las zonas aledañas).	Enero - Diciembre
6. Sistemas de circuito cerrado de TV ubicarlo en lugares críticos.	Enero - Diciembre
7. Sistemas de control de acceso estableciendo controles en las entradas y salidas implementados y monitoreados permanentemente.	Enero - Diciembre

<b>Acciones</b>	<b>Fechas de cumplimiento</b>
8. Asegurar el mantenimiento del esquema de comunicación con las entidades o agencias externas de apoyo (Bomberos, Policía Nacional, Cruz Roja, etc.).	Enero - Diciembre
9. Asegurar el aprovisionamiento de mascarillas, chalecos, cascos, linternas, radios de comunicación, y otros.	Enero - Diciembre
10. Gestionar el fortalecimiento de la seguridad física en el acceso a las instalaciones y zonas críticas del área informática.	Enero - Diciembre
11. Mantenerse informado sobre la ubicación de controles de electricidad, agua, aires acondicionados y cómo desconectarlos.	Enero - Diciembre
12. Establecer y poner en práctica procedimientos que permitan identificar y manejar los eventos o fallas que pudieran presentarse y originar una situación de riesgo, la cual en la medida de lo posible debe anticiparse y prevenirse tales como conatos de incendios.	Enero - Diciembre
13. Implementar la evaluación anual de riesgos y controles e implementar las mejoras identificadas producto de la misma.	Enero - Diciembre
14. Gestionar la compra de chalecos, máscaras y demás instrumentos necesarios para realizar pruebas con los miembros de la brigada.	Enero - Diciembre

**ii) Responsabilidad del Jefe Departamento Administrativo:**

Asegurar el mantenimiento preventivo de los siguientes elementos:

<b>Acciones</b>	<b>Fechas de cumplimiento</b>
1. Valorar la cobertura de seguros a fin de presentar a la Gerencia para su aprobación la ampliación de cobertura de seguros para proteger a la empresa ante pérdidas financieras.	Enero
2. Mantener en perfecto estado el funcionamiento del sistema eléctrico principal que supe a la Distribuidora y sus dependencias al igual que los sistemas eléctricos suplementarios, así como bombas inyectoras pluviales, de aguas negras y bombas de desagüe.	Enero - Diciembre
3. Climatización y enfriamiento en áreas que lo requieran: Centro de cómputos, bodegas de enlatados, etc.	Enero – Diciembre
4. Mantener en perfecto estado el funcionamiento de la iluminación general y de emergencia de la Distribuidora y sus dependencias.	Enero - Diciembre
5. Corregir con impermeabilizantes o con los materiales adecuados cualquier posible filtración detectada en techos y paredes del área informática.	Enero – Abril
6. Verificar que la disposición de líquidos inflamables, gases y elementos similares esté fuera de contactos eléctricos.	Enero - Diciembre
7. Verificar que los tanques de almacenamiento de agua y cisternas se mantengan en niveles adecuados.	Enero - Diciembre

Acciones	Fechas de cumplimiento
8. Verificar que la instalación de cualquier anaquel, estante o mueble estén debidamente fijados a las paredes.	Enero - Diciembre
9. Efectuar una evaluación anual de la infraestructura física de las instalaciones.	Enero – Diciembre
10. Efectuar una evaluación anual de riesgos y controles e implementar las mejoras identificadas.	Diciembre
11. Implementar alarmas de emergencia y conatos de incendios para ser activados ante una materialización de riesgos.	Enero – Diciembre
12. Formar y entrenar permanentemente una brigada de primeros auxilios.	Enero – Diciembre
13. Mantener lista de contactos, teléfonos y direcciones de todo el personal de la Distribuidora.	Enero – Diciembre

**iii) Responsabilidad del Jefe Departamento de Informática:**

Asegurar el mantenimiento preventivo de los siguientes elementos:

Acciones	Fechas de cumplimiento
1. Crear y mantener Centro de Procesamiento Alterno de Datos actualizado y protegido que se habilite en tiempo real ante contingencias como: ataques informáticos, robo, incendios, inundaciones u otro desastre.	Febrero
2. Seguridad física: cada vértice de red debe estar instalado en un Rack o gabinete enllavado y rotulado que evite su manipulación por personal no autorizado. La conexión de	Enero

Acciones	Fechas de cumplimiento
fibra óptica que une la red del negocio esté debidamente protegida así como la subterránea para evitar su manipulación por personal no autorizado.	
3. Disponer de un software de monitoreo de los principales equipos que se encuentran conectados a los puntos de ventas a través de What's Up. Las impresoras pueden ser monitoreadas vía Browser, lo que permitirá controlar la configuración remotamente, a fin de responder en tiempo real ante fallas en el funcionamiento del sistema de facturación.	Enero-Diciembre
4. Mantener capacitado al equipo técnico informático para el mantenimiento de los sistemas de información	Enero - Diciembre
5. Disponer de baterías contingentes que permitan reemplazar la batera principal en caso de fallas para garantizar el correcto funcionamiento del Centro de datos.	Enero
6. Mantener todos los respaldos informáticos actualizados.	Enero - Diciembre
7. Asegurar el inventario actualizado de todo el equipo computacional y asegurar su funcionamiento.	Enero - Diciembre
8. Efectuar una evaluación anual de riesgos y controles e implementar las mejoras identificadas producto de la misma.	Enero - Diciembre
9. Establecer y poner en práctica procedimientos que permitan identificar y manejar los eventos o fallas que pudieran presentarse y originar una situación de riesgo, la cual en la medida de lo	Enero - Diciembre

Acciones	Fechas de cumplimiento
posible debe anticiparse y prevenirse.	
10. Asegurar la contratación y renovación de licencias de antivirus robustas.	Conforme a contrato
11. Renovación de enlaces de fibra óptica de la red de la distribuidora para fortalecer la continuidad de los servicios informáticos.	En dependencia de la evaluación de daños en el cableado exterior o por obsolescencia
12. Adquisición de unidades de distribución de energía (PDU) monitoreable para reemplazar regletas ordinarias por PDUS que permitan llevar control de la carga eléctrica por rack y evitar sobrecargas.	Anual
13. Adquisición y mantenimiento de unidades recolectora de datos (PDA) para la facturación de pedidos en tiempo real	Anual
14. Realizar simulacros del Plan de Continuidad relacionada a tecnología de información con toda la logística y posibles eventos para que sea corregido en aquellos aspectos que deben mejorarse para su actualización, capacitar a todos los involucrados directa e indirectamente y darlo a conocer al personal clave.	Trimestral
15. Crear e implementar disposiciones administrativas de restricción de acceso al área del centro de datos.	Enero
16. Virtualizar 2 estaciones de trabajo para el mantenimiento del sistema de facturación u otro sistema crítico en caso de requerimientos técnicos fuera de la jornada laboral.	Enero - Diciembre
17. Disponer de un servidor dedicado al servicio de Firewall para que corra el programa Firewall de	Enero- Diciembre

Acciones	Fechas de cumplimiento
<p>la empresa checkpoint que guarde el perímetro de la Red corporativa del Internet y otras redes externas. La licencia debe ser renovada año con año y disponer de un firewall contingente para que entre a funcionar cuando el otro falla. Así mismo disponer de una contingencia de Sistema Integral Antivirus (SIA).</p>	
<p>18. Asegurar la actualización de documentación del sistema de facturación de forma continua de modo que se cuente con información técnica que facilite la solución de los problemas reportados: (Manual Técnico, Manual de Operación, Manual de Usuarios)</p>	<p>Enero</p>

## 5.2 Estrategias para la etapa durante la materialización de riesgos

Con el propósito de generar una capacidad de respuesta, ante un riesgo materializado, que pueda paralizar la continuidad de las operaciones de la Distribuidora Tropical el Pacífico, S.A, se definieron las siguientes acciones:

Acciones	Responsable
<p>1. Activar el presente Plan de Continuidad</p>	<p>Jefe Departamento Administrativo</p>
<p>2. Activar alarmas de emergencias en el momento que sea declarada una alerta frente a un fenómeno previsible o en el caso de presentarse un evento de aparición súbita y contactar a miembros de la brigada.</p>	<p>Jefe de Protección Física</p>
<p>3. Mantener equipamiento de seguridad y comunicación constante con Jefe de</p>	<p>Miembros de la brigada</p>



Acciones	Responsable
Protección Física.	
4. Integración de brigadas de protección y primeros auxilios con equipamientos según el caso.	Miembros de la brigada y coordinados por Jefe de Protección física
5. En caso de incendio, el alejamiento inmediato de las zonas de alto riesgo y la movilización del personal y clientes hacia las zonas próximas marcadas como Seguras.	Miembros de la brigada y coordinados por Jefe de Protección física
6. En caso de disturbio social, la recomendación al personal para que se mantenga dentro de la instalación y comunicación a los que se encuentren trabajando fuera de las instalaciones.	Miembros de la brigada y coordinados por Jefe de Protección física Jefe de Protección física
7. En caso de apagón de energía eléctrica, activar la planta eléctrica de emergencia.	Jefe de mantenimiento
8. En caso de problemas energéticos con horarios extendidos mayor a un día. Utilizar baterías de respaldo que le permitan enfrentar problemas de suministro eléctrico, además de esto la Distribuidora debe disponer de un generador eléctrico que suministre energía al servidor central.	Jefe Departamento de Informática
9. Fallas en el servidor (HW) Servidores de aplicación (ubicación de los programas) Servidores de bases de datos se deberá habilitar servidores de contingencia (réplicas).	Jefe Departamento de Informática
10. Fallas en las Bases de Datos (Software manejador de BD) se deberá habilitar	Jefe Departamento de Informática

Acciones	Responsable
servidores de contingencia (réplicas)	
11. Fallas de conexión a la red del negocio, solicitar a lo inmediato al proveedor la reparación técnica de la red.	Jefe Departamento de Informática
12. Errores del sistema de facturación, habilitar copia de software requerido para mantenimiento de los sistemas, a fin de poder reinstalarlos en caso de fallas en las PCS.	Jefe Departamento de Informática
13. En casos de daños a los medios informáticos de gran impacto que impidan su continuidad, proceder a habilitar el centro de datos alterno.	Jefe Departamento de Informática
14. En caso que el evento ocurra en horario no laborable se deberá avisar a los empleados que ejecutan los procesos de menor urgencia para que no asistan a trabajar y contactar a aquellos que realizan los procesos de mayor urgencia cuya asistencia será muy necesaria, según listado predefinido para que se dirijan a su trabajo o al centro de datos alterno, según el caso.	Asistente del Jefe Departamento Administrativo

## 6. Lista actualizada de proveedores críticos

Al disponer de los contactos de comunicación de proveedores críticos, conllevará a establecer una comunicación efectiva sobre un evento u ocurrencia que pudiera interrumpir la operatividad normal de la Distribuidora, a fin de contactar a lo inmediato al proveedor que se requiera para brindar el servicio y continuar la cadena de producción.

<b>Servicio</b>	<b>Licencias Oracle</b>		
Proveedor:	Microsoft		
Representante/ Mario Fuentes	Teléfono oficina 22535444	Teléfono celular 8886764	Correo electrónico mfuentes@microsoft.net
<b>Servicio:</b>	<b>Mantenimiento de red corporativa</b>		
Proveedor:	Claro		
Representante/ Eliseo Gurdián	Teléfono oficina 26535444	Teléfono celular 8486764	Correo electrónico <a href="mailto:egurdian@claro.ni">egurdian@claro.ni</a>
<b>Servicio:</b>	<b>Frigoríferos tropicales S.A.</b>		
Proveedor:	Distribuidora Tropical de Costa Rica		
Representante Carlos Gómez	Teléfono oficina 506-5354469	Teléfono celular	Correo electrónico cgdt@tropicos.cr

## 7. Lista actualizada de clientes

Para la continuidad del negocio debe tener en cuenta todos los clientes importantes, a fin de contactarlos e informarles que la atención del servicio de la Distribuidora, se ofrecerá en el sitio alternativo o las decisiones que se tengan a bien informar para continuar brindando el servicio.

Cliente	Representante	Teléfono de Oficina	Teléfono celular	Correo electrónico
Supermercado la Colonia	Ing. Oscar Pereira	22535444	8886764	opereira@colonia.ni
Supermercado la Unión	Lic. José Treminio	26535444	8885564	Treminio@launion.ni
Distribuidora El Mayoreo	Sr. Denis Montes	28535444	8832564	

## 8. Matriz servicios informáticos críticos

La Distribuidora, dispone de servicios informáticos para el desarrollo de sus operaciones comerciales, a través del Sistema de facturación se registran todas las transacciones de ventas, por medio del Sistema Contable, obtiene los Estados financieros de la empresa. Al disponer de este tipo de sistemas se genera ahorros, aumenta la efectividad, la rapidez e incluso se reducen los errores, por tal motivo, en la planificación de la continuidad operacional del negocio se presentan los servicios informáticos necesarios:

No.	Servicio informático	Función	Área Responsable	Áreas involucradas
1.	Red	Conectividad a red del negocio	Departamento de Informática	Todos
2.	Firewall	Sistema principal de seguridad de acceso	Departamento de Informática	Todos – Red Distribuidora
3.	Aplicación Server	Servidor que contiene los ejecutables de los principales sistemas	Departamento de Informática	Todos
5.	Sitio Web Distribuidora	Portal Web	Políticas promocionales de ventas y mercadeo	Mercadeo
6.	Antivirus	Sistema de protección de virus Spam	Departamento de Informática	Todas

## 9. Capacitación, entrenamiento y pruebas

Para la gestión de la continuidad se deberá desarrollar e implementar un Plan de concientización y capacitación para todos los involucrados en el presente Plan de Continuidad del Negocio, con el propósito de garantizar el entendimiento

adecuado de los temas propios de continuidad, así como también de la operación de los procesos y servicios críticos de la Distribuidora ante la posible materialización de riesgos.

El Plan de pruebas y ejercicios debe contener el alcance, objetivos y criterios de evaluación de cada prueba a ser coordinados por el Comité de Administración de Riesgos y Continuidad. Las pruebas deben realizarse por lo menos dos (2) veces al año.

#### **10. Mantenimiento y vigencia del plan de continuidad**

Cada cambio efectuado al Plan de Continuidad de la Distribuidora, generará la prueba correspondiente. La responsabilidad de la efectividad y vigencia del presente Plan, será del Comité de Administración del Riesgo y continuidad y Equipo de trabajo que ha sido asignado con tareas específicas. Sin embargo, el contenido presentado en este documento, no agota la gama de alternativas en el transcurso del tiempo o cuando surjan situaciones críticas que podrían adicionar u originar otras posibles opciones viables de implementar no contempladas en el mismo.

De esta manera, el equipo de Directores involucrados en determinado momento ante la presentación de un incidente podrán tomar medidas o decisiones que consideren conveniente y que no necesariamente están contenidas en este Plan.

El presente documento será aprobado por el Gerente y será responsabilidad del Jefe del Departamento Administración y Finanzas comunicarlo a todo el personal involucrado, así como promover su capacitación y actualización.

## Referencias Bibliográficas

- Aguilera López Purificación (2010), *Seguridad informática*, Editex, (p.44).
- Antoni Olive Ramón & Ernest Teniente López (2004) *Diseño de sistemas software en UML*, Ediciones UPC (p.11)
- Areitio Bertolín Javier, (2008), *Seguridad de la Información Redes, Informática y Sistemas de Información*, Paraninfo, (p. 321).
- C. J. Date &, Sergio Luis & María Ruiz Faudón (2001) *Introducción a los sistemas de bases de datos*, Pearson Educación, séptima edición, (p. 327).
- Control Objectives for Information and Related Technology (COBIT)
- Coopers & Lybrand (1997), *Los Nuevos Conceptos del Control Interno: Informe COSO*, Diaz de Santos (p.15).
- Cortes Morales Roberto (2010), *Introducción al análisis de sistema e ingeniería de software*, (p. 54).
- Ernest Teniente, López Antoni Olivé Ramon, Enric Mayol Sarroca, Cristina Gómez Seone, *Diseño de sistemas software en UML*, Ediciones UPC, (p.11)
- Galán Quiroz Leonor (1996), *Informática y auditoría para las ciencias empresariales*, Primera Edición, UNA, (p.52, 53, 114, 116).
- Gaspar Martínez Juan (2004), *Planes de Contingencia la Continuidad Del Negocio en Las Organizaciones*, Ediciones Díaz de Santos, (p.12)
- Ian Sommerville (2006), *Ingeniería del software*, Séptima Edición, Pearson Educación, (p.6)
- ISO/IEC 27002 (anteriormente denominada ISO 17799).

- Jimenez-ottalengo Regina & Carreras María Teresa (2002), *Metodología Para la Investigación en Ciencias de Lo Humano*, Publicaciones Cruz O., S.A. (p.33).
- Kenneth E. Kendall & Julie E. Kendall (2005), *Análisis y Diseño de Sistemas*, Pearson Educación, (p.32).
- M. Gómez Marcelo (2006), *Introducción a la metodología de la investigación científica*, Editorial Brujas, (p.25).
- Martínez González Raquel Amaya (1993), *Diagnostico Pedagógico: fundamentos teóricos*, Servicio de publicaciones Universidad de Oviedo, (p.20).
- Mejía Quijano Rubí Consuelo, (2006), *Administración de riesgos: Un enfoque empresarial*, Universidad Eafit, fondo Editorial, (p.39-40).
- Normas Jurídicas de Nicaragua, requisitos para uso de sistemas de facturación computarizadas.