



**VICERRECTORADO DE INVESTIGACIÓN,  
INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA**

**MAESTRÍA EN GERENCIA DE SISTEMAS**

**TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE  
MAGISTER EN GERENCIA DE SISTEMAS  
PROYECTO 2**

**TEMA: PROPUESTA DE UN PLAN DE CONTINGENCIAS EN  
LA EMPRESA TÉCNICOS AGROPECUARIOS DEL ECUADOR  
CIA. LTDA. TADEC POR LA IMPLANTACIÓN DE UN ERP**

**AUTOR: MOYA PACHECO, LOLIA GIOCONDA**

**DIRECTOR: ING. GERMAN, ÑACATO  
CODIRECTOR: ING. RAMIRO, DELGADO**

**SANGOLQUI**

**2015**

**UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE  
VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN  
CON LA COLECTIVIDAD**

**CERTIFICADO**

Se certifica que el trabajo titulado "PROPUESTA DE UN PLAN DE CONTINGENCIAS EN LA EMPRESA TÉCNICOS AGROPECUARIOS DEL ECUADOR CIA. LTDA. TADEC POR LA IMPLANTACIÓN DE UN ERP", fue realizado en su totalidad por la Ing. Lolía Gioconda Moya Pacheco, investigación que ha sido dirigida bajo nuestra supervisión, orientando sus conocimientos y competencias para un eficiente desarrollo del tema y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de la Fuerzas Armadas ESPE.

Sangolquí, Abril 2015



---

ING. GERMAN ÑACATO

Director



---

ING: RAMIRO DELGADO

Oponente

## AUTORÍA DE RESPONSABILIDAD

Yo Lolía Gioconda Moya Pacheco declaro que el proyecto de grado denominado "PROPUESTA DE UN PLAN DE CONTINGENCIAS EN LA EMPRESA TÉCNICOS AGROPECUARIOS DEL ECUADOR CIA. LTDA. TADEC POR LA IMPLANTACIÓN DE UN ERP", ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, cuyas citas bibliográficas que se incluyen en este documento.

Consecuentemente este trabajo es de mi autoría.

En virtud a esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolqui, Abril 2015



Lolía Gioconda Moya Pacheco

## AUTORIZACIÓN

Yo Lolía Gioconda Moya Pacheco autorizo a la Universidad de las Fuerzas Armadas ESPE, la publicación en la biblioteca virtual de la Institución, el proyecto de grado denominado "PROPUESTA DE UN PLAN DE CONTINGENCIAS EN LA EMPRESA TÉCNICOS AGROPECUARIOS DEL ECUADOR CIA. LTDA. TADEC POR LA IMPLANTACIÓN DE UN ERP", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, Abril 2015

A handwritten signature in blue ink, appearing to read 'Lolía Gioconda Moya Pacheco', is written over a large, faint circular stamp or watermark.

Lolía Gioconda Moya Pacheco

## DEDICATORIA

A Dios, por permitirme conocer el milagro de la vida Sofía.

A mi esposo, a mi madre Yolanda, a mis Hermanas Sandra, Maida y a mi Hermano Felix por el apoyo incondicional.

Lolia Gioconda Moya Pacheco

## AGRADECIMIENTO

Al finalizar un proyecto de tesis de grado viene a mi memoria todas y cada una de las personas que me apoyaron, por lo que me resulta difícil nombrarlas; sin embargo pienso que el pilar fundamental de todas mis luchas es y será la única guerrera que he conocido a lo largo de todos los tiempos, quien sin estudios de maestría o postgrados nos enseñó que los únicos límites para conseguir nuestros objetivos está en nuestras mentes, Ella y su afán de convertir a sus hijos en seres de lucha y de bien, es quién ha sido mi motor de inspiración para alcanzar los objetivos en la vida. Mi Amada Madre.

Finalmente no debo olvidar agradecer a Dios por darme la oportunidad de hacer realidad mis sueños, por darme un propósito de vida y por afianzar mi fe cuando las batallas parecían estar perdidas.

Gracias.

Lolia Gioconda Moya Pacheco

## ÍNDICE DE CONTENIDOS

AUTORÍA DE RESPONSABILIDAD .....	iii
AUTORIZACIÓN.....	iv
DEDICATORIA .....	v
AGRADECIMIENTO .....	vi
ÍNDICE DE CONTENIDOS .....	vii
ÍNDICE DE TABLAS .....	x
ÍNDICE DE CUADROS.....	xi
ÍNDICE DE FIGURAS.....	xii
LISTADO DE ANEXOS.....	xiii
RESUMEN .....	xiv
ABSTRACT.....	xv
CAPITULO I.....	1
INTRODUCCIÓN.....	1
1.1. Introducción .....	1
1.2. Justificación e Importancia.....	2
1.3. Planteamiento del Problema .....	2
1.4. Formulación del Problema .....	3
1.5. Objetivo General .....	3
1.6. Objetivos Específicos.....	3
CAPITULO II.....	5
MARCO TEÓRICO .....	5
2.1 Introducción .....	5
2.2 Antecedentes .....	6
2.3 Historia.....	9
2.4 Seguridad de la Información .....	10
2.4.1 Activos Informáticos.....	11
2.4.1.1 Información.....	12
2.4.1.2 Equipos.....	13
2.4.1.3 Personas .....	15
2.4.2 Principios Básicos de la Seguridad.....	15
2.4.3 Amenazas y Vulnerabilidades.....	17

	viii
2.4.4	Riesgos, Medidas de Seguridad y Ciclo de Seguridad ..... 20
2.4.5	Conclusiones de la Seguridad Informática..... 22
2.5	Planes de Contingencia ..... 22
2.5.1	Fases del Plan de Contingencias ..... 22
2.5.1.1	Organización ..... 22
2.5.1.2	Identificación del Riesgo..... 23
2.5.1.3	Definición de Eventos Susceptibles de Contingencia..... 24
2.5.1.4	Elaboración del Plan de Contingencia..... 25
2.5.1.5	Definición y Ejecución del Plan de Pruebas ..... 26
2.5.1.6	Implantación ..... 26
2.5.1.7	Seguimiento y Control ..... 26
2.5.2	Importancia de los Planes de Contingencias..... 27
2.5.3	Terminología relacionada con el Plan de Contingencias ..... 27
2.6	Marco Conceptual ..... 36
CAPITULO III..... 38	
METODOLOGÍA DE LA INVESTIGACIÓN..... 38	
1.1	Metodología de Investigación ..... 38
1.1.1	Ubicación Geográfica del Proyecto de Investigación..... 38
1.1.2	Método de investigación, Técnicas e Instrumentos de Recolección y Procesamiento de Datos e Información. .... 38
1.1.2.1	Método de Investigación..... 38
1.1.2.2	Técnicas e Instrumentos de Recolección ..... 38
1.1.2.3	Procesamiento de Datos e Información..... 45
1.1.3	Evaluación de Resultados y Discusión ..... 45
CAPITULO IV..... 48	
PLAN DE CONTINGENCIAS..... 48	
4.1	Objetivos ..... 48
4.1.1	General ..... 48
4.1.2	Específicos ..... 48
4.2	Alcance ..... 48
4.3	Procesos Críticos ..... 49
4.3.1	Restauración del Servidor la Base de Datos ..... 49
4.3.2	Restauración del Servidor de Aplicaciones..... 49



	ix
4.3.3 Restauración del Usuario de la Base de Datos PRD .....	49
4.3.4 Gestión de Respaldo y Recuperación del Usuario PRD .....	49
4.3.5 Restauración del Modelo Analítico de Ventas .....	49
4.3.6 Restauración del Modelo de Documentos Electrónicos.....	49
4.3.7 Restauración del Modelo Notas de Pedido para la Web .....	49
4.4 Bitácoras de Control.....	72
4.5 Responsables .....	74
4.6 Recursos.....	74
4.7 Períodos Plazos de Prueba .....	75
4.8 Cronograma de Actividades para la Ejecución del Plan.....	76
4.9 Conclusiones de la Propuesta .....	79
4.10 Recomendaciones de la Propuesta.....	79
BIBLIOGRAFÍA.....	80
SIGLAS.....	83
ANEXOS.....	88

## ÍNDICE DE TABLAS

Tabla 1. Matriz de Probabilidad de Ocurrencia, Frecuencia, Pérdida y Riesgo .....	46
Tabla 2. Matriz de Riesgos .....	47
Tabla 3. Bitácora de Registro de Control de Respaldo Diarios .....	72
Tabla 4. Bitácora de Registro de Control de Recuperación .....	72
Tabla 5. Bitácora de Registro de Control de Cambios .....	73
Tabla 6. Matriz de Responsables de Plan de Contingencias .....	74
Tabla 7. Cronograma de Ejecución del Plan de Contingencias .....	76

**ÍNDICE DE CUADROS**

Cuadro 1. Tipos de Activos: Clasificación Detallada.....	12
Cuadro 2. Proceso de la Administración del Riesgo.....	37

**ÍNDICE DE FIGURAS**

Figura 1. Jerarquía de una Política de Seguridad de la Información .....	11
Figura 2. Proceso de la comunicación de un activo .....	12
Figura 3. Causas de pérdida o daño de un activo.....	12
Figura 4. Vulnerabilidad de la información - Software.....	13
Figura 5. Seguridad de la información - Hardware.....	14
Figura 6. Seguridad de la información – Organización .....	15
Figura 7. Vulnerabilidad – Personas .....	15
Figura 8. Factor de Seguridad la Confidencialidad .....	16
Figura 9. Amenazas más frecuentes en la seguridad de la información .....	17
Figura 10. Proceso para administrar las vulnerabilidades .....	17
Figura 11. Puntos débiles o vulnerabilidades de la información .....	18
Figura 12. Tipos de Medidas de Seguridad .....	20
Figura 13. Ciclo de Seguridad de Riesgos.....	21
Figura 14. Elementos de la Vulnerabilidad .....	22
Figura 15. Procesos de Administración de un Riesgo .....	36
Figura 16. Organigrama del Comité de la Organización .....	39

**LISTADO DE ANEXOS**

Anexo 1: Diagrama de Red – Enlaces .....	89
Anexo 2: Diagrama de Red PIA .....	89
Anexo 3: Hardware – Servidores .....	89
Anexo 4: Manual BI Ventas .....	89
Anexo 5: Manual Facturación Electrónica .....	89
Anexo 6: Manual Instalación Microstrategy .....	89
Anexo 7: Manual Usuario Notas Pedido .....	89

## RESUMEN

Este proyecto, consiste en la propuesta para la creación de un plan de contingencia en la empresa TADEC CIA. LTDA., con enfoque al Área de TI, asociada a Slego ERP con el fin de asegurar la disponibilidad del Software en caso de ocurrir alguno de los riesgos identificados en la Matriz de Riesgo, analizada en el proyecto No.1. El plan de contingencias se base en siete procesos críticos identificados en la matriz de riesgo: Restauración del Servidor la Base de Datos, Restauración del Servidor de Aplicaciones, Restauración del Usuario de la Base de Datos PRD, Gestión de Respaldo y Recuperación del Usuario PRD, Restauración del Modelo Analítico de Ventas, Restauración del Modelo de Documentos Electrónicos y Restauración del Modelo Notas de Pedido para la Web. Se propone el uso de estándares para administrar de mejor manera los procesos como bitácoras para el Registro de Control de Respaldo Diario, Registro de Control de Recuperación, Registro de Control de Cambios en el ERP; así como también la definición de Responsables, Recursos, Períodos y Plazos de Prueba, Cronograma de Actividades para la ejecución del plan en base a la metodología ISO 9001:2000. Al contar con un plan de contingencias asociado a Slego ERP, el área de TI se encuentra en condiciones para reaccionar a cualquier evento de riesgo identificado en la Matriz de Riesgo y disminuir notablemente el tiempo de reacción y puesta en marcha del Software para servicio tanto del usuario interno como externo, por ejemplo en el caso de las notas de pedido a través de la web que utilizan los usuarios distribuidores.

### **PALABRAS CLAVE:**

- **PLAN DE CONTINGENCIAS**
- **BITÁCORAS DE CONTROL**
- **PROCEDIMIENTOS**
- **POLÍTICAS**
- **METODOLOGÍA ISO 9001:000**
- **ENTERPRISE RESOURCE PLANNING**
- **SISTEMAS ERP**

## **ABSTRACT**

The objective of this project is to propose the creation of a contingency plan in TADEC Company with focus on IT area associated with Slego ERP, in order to ensure the availability of Software occur if any of the risks identified in the Risk Matrix , analyzed Thesis Plan No.1. The contingency plan is based on seven critical processes identified in the risk matrix: Restoring the Database Server, Restoring Application Server, Restoring User Data Base PRD, Managing Backup and Recovery User PRD, Analytical Model Restoration Sales, Restoration Model for Electronic Document and Restoration Model Order notes for the Web. The use of standards to better manage risks and logs for Backup Control Registry Journal, Control Registry Recovery Control Registry Changes proposed ERP; as well as the definition of Responsible, Resources, Periods and Deadlines Test, Schedule of Activities for Implementation of the Plan based on the methodology ISO 9001 : 2000 By having a Contingency Plan associated with Slego ERP, the TI are is able to react to any event risk identified in the Risk Matrix and considerably reduce the reaction time and implementation of ERP Software Slego both the internal users and external to the company.

### **KEYWORDS:**

- **CONTINGENCY PLAN**
- **CONTROL LOGS**
- **PROCEDURES**
- **POLICIES**
- **METHODOLOGY ISO 9001:000**
- **ENTERPRISE RESOURCE PLANNING**
- **SLEGO ERP**

# CAPITULO I

## INTRODUCCIÓN

### 1.1. Introducción

Para la empresa Técnicos Agropecuarios del Ecuador Cía. Ltda., es indispensable el uso del sistema informático Slego ERP para brindar atención permanente a los clientes internos como externos a la organización, por tal motivo proveer de información diaria y garantizar que el sistema informático esté disponible a todo nivel.

Es así que minimizar los riesgos de los recursos informáticos en torno al uso de Slego ERP es un factor fundamental para pensar en la creación de un plan de contingencias en el área de TI asociado al ERP.

El plan de contingencia es el conjunto de normas y procedimientos que, basado en el análisis de riesgos, permite a la organización encargada del área de TI, actuar durante y después de un evento de riesgo, de manera rápida y efectiva con respecto a los procesos identificados como los más sensibles de acuerdo al estudio realizado en la matriz de impacto, de probabilidad de ocurrencia y de riesgo en el proyecto No.1.

Los procesos a ser considerados dentro del plan de contingencias están asociados a las comunicaciones, servidores, software, impresoras, aplicativos web y otras aplicaciones analíticas de BI que se encuentran integradas con Slego ERP.

Por lo mencionado anteriormente en el presente proyecto se diseñará el plan de contingencias para prever cómo actuar y qué recursos son necesarios ante una situación de riesgo en la empresa Técnicos Agropecuarios del Ecuador Cia. Ltda., con el objeto de restablecer los servicios de TI asociados al ERP en el menor tiempo posible.



## **1.2. Justificación e Importancia**

La evolución de los sistemas informáticos se encuentran directamente relacionados con la evolución de las vulnerabilidades que deben ser controladas por las empresas, desde las más sencillas como cortes de energías, fallas del disco duro, pérdidas de la comunicación, pérdidas de datos, hasta los desastres más severos como destrucción de equipos por desastres naturales o llegar a los niveles más altos como son los actos de terrorismo.

Mientras que muchas de las vulnerabilidades pueden minimizarse o eliminarse a través de soluciones tecnológicas, administrativas u operacionales como parte de los esfuerzos de la administración de riesgo de la organización, es virtualmente imposible eliminar completamente todos los riesgos.

Razón por la cual se desarrollan planes de contingencia para garantizar la continuidad del negocio y se pueden aplicar a cualquier área de la empresa.

## **1.3. Planteamiento del Problema**

Con el estudio de impacto por la implantación de Slego ERP en la empresa Técnicos Agropecuarios del Ecuador Cía. Ltda. surge la necesidad de garantizar la continuidad del negocio en torno a la disponibilidad de los recursos tecnológicos como son servidores, datos, comunicaciones, archivos relacionados con la configuración del ERP, entre otros; ha surgido la necesidad de proponer un plan de contingencias para el área de TI con el enfoque específico a Slego ERP.

#### **1.4. Formulación del Problema**

Entre los problemas más relevantes se puede mencionar los siguientes:

- Caída del servidor de Base de Datos y/o de Aplicaciones principal por fallas de hardware, software, cortes de energía eléctrica, comunicaciones, desastres naturales que provoca la pérdida de información y continuidad del negocio.
- Falta de respaldos de la base de datos del usuario propietario del software que impida la recuperación de la información inmediata.
- Falta de control y registro de bitácoras de cambios solicitados directamente al Administrador de Slego ERP por errores humanos generados en la transacción.
- Ausencia de Políticas y procedimientos asociados a las actividades de respaldo y recuperación de la Base de Datos y del usuario PRD.

Por estas razones es urgente proponer un plan de contingencias para el área de TI como resultado del impacto que ha causado la implantación de Slego ERP en la empresa y principalmente en área de TI.

#### **1.5. Objetivo General**

DISEÑAR UN PLAN DE CONTINGENCIAS DEL ÁREA DE TI PARA LA EMPRESA TÉCNICOS AGROPECUARIOS DEL ECUADOR CIA. LTDA. TADEC POR LA IMPLANTACIÓN DEL ERP UTILIZANDO LA METODOLOGÍA PDCA.

#### **1.6. Objetivos Específicos**

- Realizar el diagnóstico del hardware: servidores de base de datos, de aplicaciones, de contingencias y de comunicaciones, para determinar el nivel de seguridad y proponer alternativas de respaldo de dichos equipos con el fin de garantizar la disponibilidad de los mismos.
- Establecer formatos de bitácora para el registro y control de los respaldos y recuperación diaria de la base de datos y del usuario PRD.

- Diseñar un modelo de bitácoras de los cambios solicitados del usuario al Administrador de Slego ERP que permita gestionar los cambios solicitados por el usuario.
- Elaborar un plan de contingencias para del área de TI relacionado con la implantación de Slego ERP para garantizar la continuidad del negocio.

## CAPITULO II

### MARCO TEÓRICO

#### 2.1 Introducción

El ambiente en el que hoy compiten las empresas ha cambiado dramáticamente, presentando nuevas oportunidades y retos para ejecutivos y gerentes. Debido a que el mercado continúa creciendo, también crece la exposición a riesgos informáticos y a la disponibilidad de la información.

Los enfoques e instrumentos disponibles para ayudar a las empresas a manejar las exposiciones de riesgo están desarrollándose rápidamente, tanto soluciones operacionales como transaccionales. Sin embargo, esos enfoques e instrumentos tienen sus propios retos y riesgos, como el costo de implementación de sistemas de respaldos alternativos para manejar y administrar de mejor manera los riesgos a través de sus planes de contingencias.

Las empresas líderes en el mercado internacional y nacional están preparadas para solventar dichos riesgos a través de la implementación de planes de contingencia en diferentes áreas susceptibles a la organización, de tal forma que se garantice la seguridad y la disponibilidad de la información tanto interna como externa a la organización; a través de la estandarización de procedimientos, responsables, recursos y políticas debidamente documentadas dentro de PECS como parte de la implantación de los procesos de calidad en la empresa.

Entender la exposición a los riesgos y como establecer políticas y controles apropiados para manejarlos, son los temas importantes en el mundo de los negocios. En respuesta ante lo ya mencionado es indispensable que las empresas cuenten con políticas y procedimientos para el control y prevención de riesgos, especialmente en el área de TI.

## 2.2 Antecedentes

Hacia principios de los años setenta del pasado siglo, Norman L. Harris, Edward S. Devlin y Judith Robey, tratando de encontrar un método de planificación y gestión de riesgos que evitará la continua atención de problemas en forma aleatoria, es decir, lo que en términos coloquiales llaman apagar fuegos, dieron lugar al nacimiento de una actividad que en un principio se llamó Disaster Recovery Planning, es decir, planificación ante contingencia, según el diccionario de la RAE en su segunda acepción, es cosa que puede suceder o no suceder, y su tercera acepción, riesgo. De esta forma no limitamos las causas a desastres, lo que parece indicar que otros incidentes menos espectaculares no son tenidos en cuenta.

Hasta ese momento, las actividades de planificación y prevención estaban dirigidas hacia las operaciones informáticas que, en la mayor parte de los casos se encontraban centralizadas en el Departamento de Informática, e incluso, en un lugar físico concreto. (Gaspar Martínez, 2004)

Con el paso del tiempo y la aparición de la informática distribuida, al extenderse por toda la organización las funciones soportadas en medios informáticos y telemáticos, esa actividad vario su alcance y vino a llamarse Business Continuity Planning, es decir lo que se puede traducir literalmente como la planificación de la continuidad del negocio. La palabra negocio, en castellano, tiene unos claros matices mercantiles, y dado que hoy todas las organizaciones, sean mercantiles o no, sean empresas o entidades públicas, dependen del correcto funcionamiento de las tecnologías de la información y de las comunicaciones, hablar de continuidad del negocio sería limitar mucho el alcance, por lo que sería más correcto hablar de continuidad del servicio. Sin embargo dentro del hábito de los profesionales de las Tecnologías de Información, continuidad del negocio ha venido a transformarse en un término comúnmente aceptado, tanto para organizaciones mercantiles como para organismos públicos. (Gaspar Martínez, 2004)

Hoy día el concepto de Business Continuity Planning, esta sustituido por el de Business Continuity Management, es decir, no se limita a la planificación de la continuidad, sino a la gestión integral de la misma.

Según el Business Continuity Institute British, Business Continuity Management no es simplemente recuperación ante desastres, gestión de crisis, gestión de riesgos o recuperación tecnológica. No es una disciplina realizada por especialistas profesionales, sino un enfoque global de la actividad que integra un amplio espectro de actividades de gestión encaminadas al objetivo final de la organización.

En particular crea el marco estratégico y operativo para revisar, y modificar cuando sea necesario, la forma en que la organización proporciona sus productos o servicios, al mismo tiempo que aumenta su resistencia frente a las interrupciones o pérdidas. (Gaspar Martínez, 2004)

La sociabilización de un plan de contingencias en área de TI en Ecuador inicia a partir del año 1995 para prevenir el efecto 2000 con el famoso problema del Y2K; especialmente en las entidades controladas por el gobierno estatal como es la Superintendencia de Bancos y Seguros, de Telecomunicaciones, el Servicio de Rentas Internas, y otras entidades; quienes alertaron a todo el sistema financiero y comercial del Ecuador para la implementación de un plan de contingencias que prevenga los efectos por el cambio de milenio en las computadoras de cualquier tipo.

El problema conocido como efecto 2000 se basaba en la tesis de que, una vez alcanzado el nuevo milenio, es decir, el año 2000, los equipos lo marcarían como año 00, sin tener en cuenta el cambio de siglo. Esto significa que el mundo informático viviría en año 1900. (Escuela Técnica Superior de Ingeniería Informática , 2012)

## Consecuencias

La principal consecuencia sería que todo software que incluyera el formato de fecha únicamente dos dígitos para el año (dd/mm/yy) fallaría en la fecha de la transacción del siguiente año.

Lo más temido era sin duda el efecto en cascada que hiciera que algunos sistemas primarios fallaran, tales como los suministros de energía o de transportes, produciendo a su vez fallas graves en otros sistemas.

Si fallaban las centrales de electricidad ¿De qué serviría que el ordenador de casa o el teléfono móvil funcionen perfectamente? Si los sistemas de bolsa operan correctamente pero la red telefónica ha caído, ¿cómo se podría transmitir la información?

¿Y si había problemas y se veían afectados los servicios de emergencia? Las compañías bancarias podían perder los datos reales de la situación financiera de sus clientes por el efecto de cierre de período contable, todo el mundo vería su saldo reducido a cero. Los transportes controlados mediante equipos informáticos no responderían, los teléfonos dejarían de funcionar, los servicios de emergencias colapsarían.

Por estas razones se divulgó la implantación de planes de contingencia informático a nivel mundial para prevenir el efecto del Y2K; sin embargo a pesar de las medidas que se tomaron para controlar dicho efecto surgieron catástrofes económicas en países como España con más de 420 millones de euros en pérdidas, pero las cifras mundiales fueron mayores a las esperadas. Según el IDC International Data Computer, el gasto que se hizo tanto a nivel mundial como en Estados Unidos fue superior a los daños que hubiesen supuesto las consecuencias del cambio de milenio. (Escuela Técnica Superior de Ingeniería Informática , 2012)

## 2.3 Historia

Los avances tecnológicos en el área informática, han cambiado drásticamente la vida cotidiana de las personas. En los años 60's, donde el procesamiento de datos se utilizaba casi exclusivamente para tareas contables, no se visualizaba la necesidad de un plan de contingencia, ya que los procesos críticos de las empresas no estaban autorizados, por lo que al ocurrir alguna falla en el sistema computarizado, la empresa podía continuar operando sin pérdidas perceptibles.

En los años 70's este pensamiento fue desapareciendo, debido principalmente a que la computación comenzó a liderar el manejo de la información y todas las demás operaciones se fueron automatizando, por lo que la necesidad de mantener la seguridad en los sistemas se fue haciendo cada día más importante. Con este cambio de pensamiento se fueron creando poco a poco equipos especializados en los diversos campos de la computación, expertos en hardware, software, comunicaciones y otros, los cuales fueron creando manuales de recuperación en caso de desastres, y fueron dando forma a un verdadero plan de contingencia que respondiera a las preguntas básicas que se necesitan responder en una situación de desastre, estas preguntas son: ¿Qué hacer?, ¿Dónde realizar las operaciones?, ¿Quién debería realizarlas?

Con el nacimiento de las PC's en los años 80's, la seguridad se convirtió en algo sumamente importante para las empresas, debido a que muchas más personas tenían acceso a una computadora, por lo que los problemas de seguridad se multiplicaron en gran medida. Al mismo tiempo, los planes de contingencia tendrían que ser mucho más completos y específicos.

En la actualidad, la sociedad es totalmente dependiente de la computación, por lo que cualquier falla o daño en el sistema, pueden ocasionar serios problemas, y en algunos casos hasta la pérdida de vidas humanas.



Es urgente tomar conciencia de la importancia que representa un plan de contingencia en la actualidad, especialmente para aquellas empresas que tienen un alto grado de automatización en los procesos vitales del negocio. (Massella Rivas, Maldonado Rivera, Ortíz Castro, Bardales Duarte, & Massella Rivas, 1999)

## **2.4 Seguridad de la Información**

La seguridad informática se enfoca a la protección de la información que se encuentra en una computadora o en una red y también a la protección del acceso a todos los recursos del sistema.

La información es el objeto de mayor valor en las organizaciones; debido que afecta directamente a los negocios de una empresa o una persona. Por esta razón el principal propósito de un plan de contingencias es proteger la información registrada, independientemente de los equipos donde se encuentren almacenados. (Baldeón Garzón & Coronel Guerrero.2010)

### **Evolución de la Seguridad Informática**

- 1965 - Departamento de Defensa de Estados Unidos.
- 1983 - Encriptación de información.
- 1985 - Virus.
- 1990 - Seguridad en Sistemas Operativos y Redes.
- 1995 - Firewalls.
- 2000 - Seguridad Informática General.
- 2006 – Seguridad de la Información.

### **Políticas de Seguridad de la Información**

El objeto de una política de seguridad es especificar requerimientos obligatorios mínimos para el uso correcto y la protección de la información y proveer un marco para todas las actividades relacionadas con la seguridad dentro de la organización.

Consecuentemente, el objetivo de la seguridad de la información es garantizar la confidencialidad, integridad y disponibilidad de la información.

Una política de seguridad es un conjunto de normas estructuradas jerárquicamente que definen la forma en que la organización responde a los riesgos de seguridad informática. Una política por sí sola no resuelve problemas.

Una política debe estar orientada a la información, porque este es uno de los activos más importantes de la empresa como se presenta en la figura 1.



**Figura 1. Jerarquía de una Política de Seguridad de la Información**  
Fuente: (Trelles Araujo, 2010)

### 2.4.1 Activos Informáticos

Establecer el valor de los datos es algo relativo, la información intangible versus los equipos, la documentación o las aplicaciones. Muchas veces se cree que las medidas de seguridad no influyen en la productividad del sistema por lo que las organizaciones se limitan a la asignación de recursos en esta tarea.

Un activo es un elemento que es parte de todo un proceso de comunicación, partiendo de la información, emisor, medio de transmisor y receptor como se muestra en la figura 2. (Trelles Araujo , 2010)



**Figura 2. Proceso de la comunicación de un activo**  
**Fuente: (Trelles Araujo , 2010)**

En la figura 3 se muestran las causas de pérdida o daño de un activo.



**Figura 3. Causas de pérdida o daño de un activo**  
**Fuente: (Trelles Araujo , 2010)**

En el cuadro 1 se muestra la clasificación detallada de los tipos de activos de la tecnología.

**Cuadro 1.**

***Tipos de Activos: Clasificación Detallada***

A. Información	
B. Equipos	B.1. Software B.2. Hardware B.3. Organización
C. Personas	

Fuente: (Massella, 1999)

### **2.4.1.1 Información**

Se define como el elemento que contiene datos registrados en medios magnéticos o físicos; la información puede estar almacenada en documentos, informes, libros, manuales, correspondencias, patentes, estudios de mercadeo, programas, códigos fuentes, reportes, archivos, planillas de pagos, planes de negocio, etc. (Trelles Araujo , 2010)

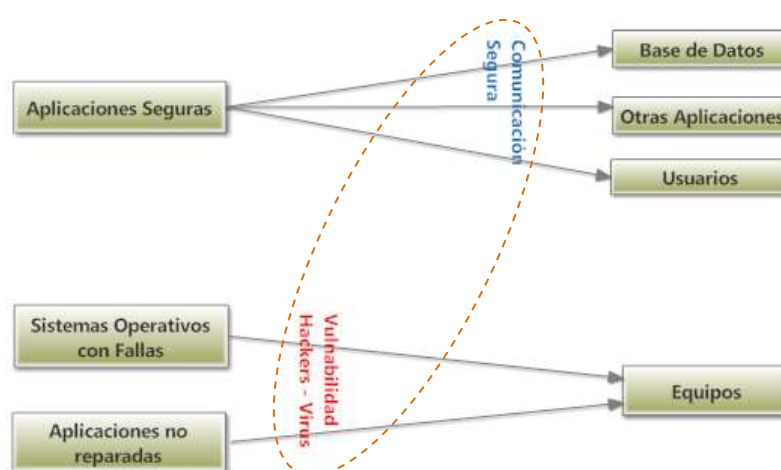
## 2.4.1.2 Equipos

### Software

Son programas de computadoras que ayudan a la automatización de los procesos de una empresa, por ejemplo: los ERP, modelos analíticos de negocios, dataware house, sistemas operativos, base de datos, antivirus, aplicaciones varias, entre otros.

La seguridad de la información evalúa la creación, disposición y utilización de los sistemas; por lo tanto, como parte de las políticas de seguridad esta detectar y corregir errores o problemas de comunicación entre los sistemas. (Trelles Araujo , 2010)

Como se muestra en la figura 4, las aplicaciones seguras ofrecen un entorno de comunicación segura entre el software de la organización. Así también las aplicaciones inseguras evidencian vulnerabilidades en la información.



**Figura 4. Vulnerabilidad de la información - Software**  
Fuente: (Trelles Araujo, 2010)

### Hardware

Comprende toda la infraestructura tecnológica que brinda soporte a la información durante su uso, tránsito y almacenamiento. Por lo tanto un activo

de hardware es cualquier equipo en el cual se almacena, procesa o transmite información de la empresa. (Trelles Araujo , 2010)

Como se muestra en la figura 5 toda la infraestructura de la organización está sujeta a diferentes tipos de fallas, tales como: eléctricas, errores de configuración, desastres de cualquier tipo, robos o atentados, lo que provoca la no disponibilidad de la información, pérdida de la misma o se ve reflejado en los tiempos de respuesta de los equipos para el procesamiento de datos.

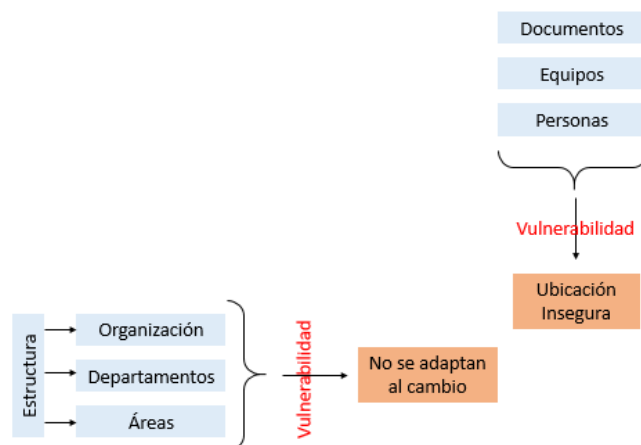


**Figura 5. Seguridad de la información - Hardware**  
Fuente: (Trelles Araujo , 2010)

## Organización

Son los aspectos que conforman la estructura física y lógica de la empresa. La estructura organizativa comprende las diferentes áreas departamentales, funciones y procedimientos, flujo de información y de trabajo, organigrama estructural de la empresa, entre otros. Básicamente se refiere al listado de activos fijos que utiliza la empresa para su funcionamiento. (Trelles Araujo , 2010)

Como se muestra en la figura 6 la estructura organizativa de la empresa está directamente relacionada con la vulnerabilidad de la información, por falta de políticas y control de accesos, llaves de dispositivo, RAC's mal ubicados o mal asignados los cuales corren el riesgo de provocar mal funcionamiento de los equipos y por ende ocasionar problemas con la disponibilidad de la información.

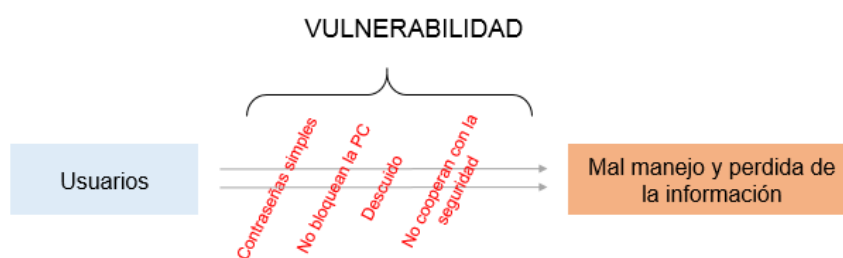


**Figura 6. Seguridad de la información – Organización**  
Fuente: (Trelles Araujo , 2010)

### 2.4.1.3 Personas

Usuarios son individuos que utilizan la infraestructura tecnológica y de comunicación de la empresa, que manejan y administran los sistemas de información. (Trelles Araujo , 2010)

Como se muestra en la figura 7 los usuarios están asociados directamente con las vulnerabilidades por el mal manejo de las claves de acceso, bloqueos de PC's, acceso al internet que ocasionan problemas con la disponibilidad de la información.



**Figura 7. Vulnerabilidad – Personas**  
Fuente: (Trelles Araujo , 2010)

## 2.4.2 Principios Básicos de la Seguridad

### Integridad

Permite garantizar que la información no sea alterada, es decir, que sea íntegra. Estar íntegra significa que esté en su estado original sin haber sido alterada por agentes no autorizados. (Trelles Araujo, 2010)

El quiebre de la Integridad ocurre cuando la información es corrompida, falsificada y burlada. Como en alteraciones del contenido del documento: inserción, sustitución o remoción, o en alteraciones en los elementos que soportan la información: alteración física y lógica en los medios de almacenaje. (Trelles Araujo, 2010)

### **Confidencialidad**

Se encarga y se asegura de proporcionar la información correcta a los usuarios correctos. La pérdida de confidencialidad es igual a la pérdida de secreto, la información confidencial se debe guardar con seguridad sin divulgar a personas no autorizadas, es decir, toda la información no debe ser vista por todos los usuarios. Como se muestra en la figura 8, garantizar la confidencialidad es uno de los factores determinantes para la seguridad.



**Figura 8. Factor de Seguridad la Confidencialidad**  
Fuente: (Trelles Araujo , 2010)

### **Disponibilidad**

La información debe llegar a su destino en el momento oportuno y preciso. La disponibilidad permite que la información se use cuando sea necesario, que esté al alcance de los usuarios y que pueda ser recuperada cuando se necesite.

Las garantías de la disponibilidad de la información son la configuración segura en el ambiente para una disponibilidad adecuada, la planeación de copias de seguridad, los backups, el definir estrategias para situaciones de contingencia y el fijar rutas alternativas para el tránsito de la información. (Trelles Araujo, 2010)

### 2.4.3 Amenazas y Vulnerabilidades

#### Amenazas

Son agentes capaces de hacer explotar los fallos de seguridad o los puntos débiles causando pérdidas y daños a los activos y afectando al negocio. Las causas más comunes son del tipo: naturales, no naturales, internas y externas. Las principales amenazas más frecuentes son: ocurrencia de virus; divulgación de contraseñas; acción de hackers. (Trelles Araujo, 2010) como se muestra en la figura 9.

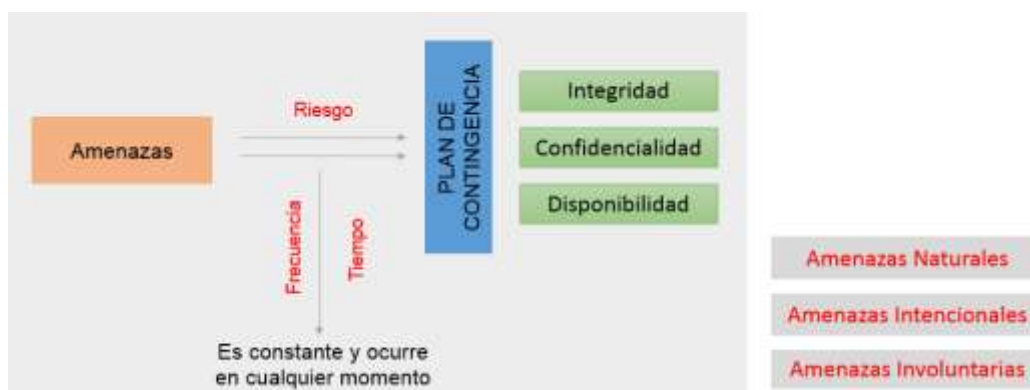


Figura 9. Amenazas más frecuentes en la seguridad de la información  
Fuente: (Trelles Araujo, 2010)

#### Vulnerabilidades

Son elementos que al ser explotados por amenazas afectan la integridad, confidencialidad y disponibilidad de la información. Como se muestra en la figura 10 y 11 los puntos débiles dependen de la forma en que se organice el ambiente en que se maneja la información. (Trelles Araujo, 2010)

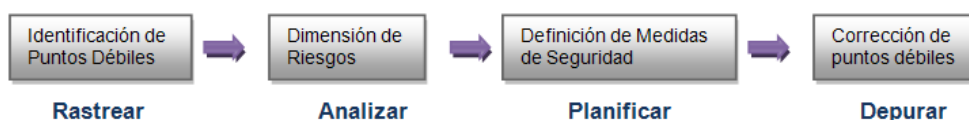


Figura 10. Proceso para administrar las vulnerabilidades  
Fuente: (Trelles Araujo, 2010)





**Figura 11. Puntos débiles o vulnerabilidades de la información**  
 Fuente: (Trelles Araujo, 2010)

### **Tipos de Vulnerabilidades**

Vulnerabilidades físicas.- están presentes en los ambientes en los cuales la información se está almacenando o manejando, tales como: instalaciones inadecuadas, ausencia de equipos de seguridad, cableados desordenados y expuestos, falta de identificación de personas, equipos y áreas. Las vulnerabilidades físicas ponen en riesgo principalmente al principio de disponibilidad.

Vulnerabilidades naturales.- están relacionadas con las condiciones de la naturaleza, tales como: humedad, polvo, temperaturas indebidas, agentes contaminantes naturales, desastres naturales, sismos, entre otros.

Vulnerabilidades de hardware.- los defectos o fallas de fabricación o configuración de los equipos atacan y/o alteran los mismos, entre estos se menciona: la ausencia de actualizaciones y conservación inadecuada, la configuración y dimensión para su correcto funcionamiento, el almacenamiento suficiente y el procesamiento y velocidad adecuada.

Vulnerabilidades de software.- permite la ocurrencia de accesos indebidos a los sistemas y por ende a la información. Entre ellos constan: configuración e instalación indebida de los programas, sistemas operativos mal configurados y mal organizados, correos maliciosos, ejecución de macro virus y navegadores de Internet.

Vulnerabilidades de medios de almacenaje- la utilización inadecuada de los medios de almacenaje afectan la integridad, la confidencialidad y la disponibilidad de la información, entre los que constan: plazo de validez y de caducidad; defectos de fabricación, uso incorrecto, mala calidad, áreas o lugares de depósito inadecuados (humedad, calor, moho, magnetismo, etc.)

Vulnerabilidades de comunicación: abarca todo el tránsito de la información, ya sea cableado, satelital, fibra óptica u ondas de radio inalámbricas. El éxito en el tránsito de los datos es crucial en la seguridad de la información porque la seguridad de la información está asociada al desempeño de los equipos involucrados en la comunicación.

Las consecuencias son: información no disponible para los usuarios; información disponible a usuarios incorrectos afectando el principio de confidencialidad; altera el estado original de la información afectando el principio de Integridad.

Las principales causas son: ausencia de sistemas de encriptación; mala elección en los sistemas de comunicación.

Vulnerabilidades humanas: son daños que las personas pueden causar a la información, a los equipos y a los ambientes tecnológicos. Los puntos débiles humanos pueden ser intencionados o no. La mayor vulnerabilidad es el desconocimiento de las medidas de seguridad adecuadas o simplemente el no acatarlas. Los puntos débiles más frecuentes de origen interno son: falta de capacitación específica y adecuada, falta de conciencia de seguridad en los usuarios. Y los puntos débiles más frecuentes de origen externo son: vandalismo, estafas, invasiones, hurto / robo.

Las causas: contraseñas débiles; falta de criptografía en la comunicación; Identificadores: nombres de usuarios, credenciales, etc. (Trelles Araujo , 2010)

## 2.4.4 Riesgos, Medidas de Seguridad y Ciclo de Seguridad

### Riesgos

Son las probabilidades que las amenazas exploten los puntos débiles o vulnerabilidades causando daños y pérdidas, y afectando completamente la integridad, confidencialidad y disponibilidad. La seguridad es una práctica orientada hacia la eliminación de las vulnerabilidades para evitar o reducir las posibilidades que las potenciales amenazas se concreten.

Su objetivo es garantizar el éxito de la comunicación segura con información íntegra, disponible y confidencial, a través de medidas de seguridad. (Trelles Araujo, 2010)

### Medidas de Seguridad

Son acciones orientadas hacia la eliminación de vulnerabilidades. Deben existir medidas de seguridad específicas para el tratamiento de cada caso. Es decir, diferentes medidas para casos distintos. (Trelles Araujo, 2010)

Las medidas de seguridad son un conjunto de prácticas que se integran para buscar un mismo fin y un mismo objetivo global de seguridad. En la figura 12 se muestran los diferentes tipos de medidas de seguridad para eliminar las vulnerabilidades.



**Figura 12. Tipos de Medidas de Seguridad**  
Fuente: (Trelles Araujo, 2010)

## Principales Medidas de Seguridad

**Análisis de Riesgos.-** Busca rastrear vulnerabilidades en los activos que puedan ser explotados por amenazas. Del análisis de riesgos se obtiene como resultado un grupo de recomendaciones para la corrección y protección de activos.

**Políticas de Seguridad.-** Busca establecer los estándares de seguridad a seguir, esto apunta a todos los involucrados con el uso y mantenimiento de los activos. Las Políticas de Seguridad es un conjunto de normas, y es el primer paso para aumentar la conciencia de la seguridad en las personas.

**Especificaciones de Seguridad.-** Son medidas para instruir la correcta implementación de nuevos ambientes tecnológicos por medio del detalle de sus elementos constituyentes.

**Administración de la Seguridad.-** Son medidas integradas e integrales que buscan gestionar los riesgos de un ambiente. Involucra a todas las medidas anteriores en forma preventiva, perceptiva y correctiva. (Trelles Araujo, 2010)

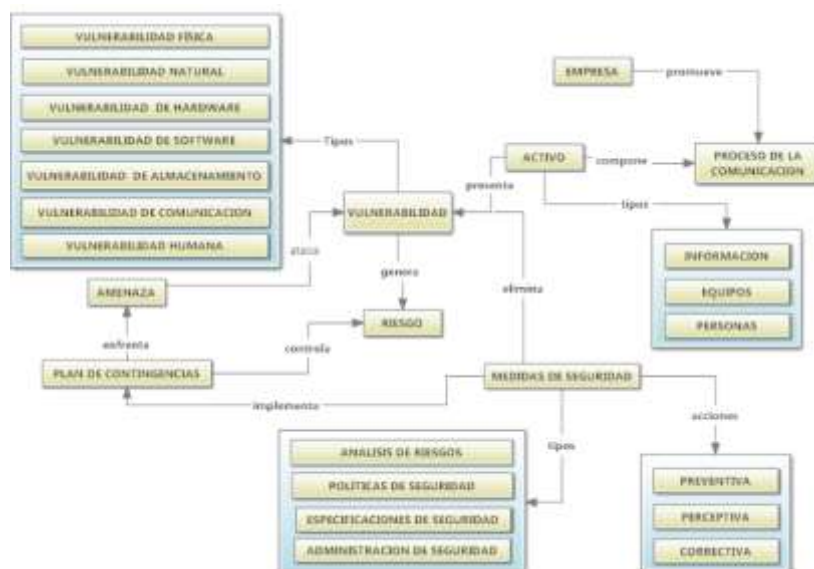
## Ciclo de Seguridad

En la figura 13 se muestra el ciclo de seguridad en relación a los riesgos de pérdida de información.



**Figura 13. Ciclo de Seguridad de Riesgos**  
Fuente: (Trelles Araujo, 2010)

En la figura 14 se indica el esquema de los elementos que afectan en la aparición de los diferentes tipos de vulnerabilidades.



**Figura 14. Elementos de la Vulnerabilidad**  
Fuente: (Trelles Araujo, 2010)

## 2.4.5 Conclusiones de la Seguridad Informática

La seguridad busca proteger la confidencialidad de la información contra accesos no autorizados, evitar alteraciones indebidas que pongan en peligro la integridad de la información y garantizar la disponibilidad de la información.

La seguridad es instrumentada por políticas y procedimientos de seguridad que permiten la identificación, el control de amenazas y puntos débiles, con el fin de preservar la integridad, confidencialidad y disponibilidad de la información.

## 2.5 Planes de Contingencia

### 2.5.1 Fases del Plan de Contingencias

#### 2.5.1.1 Organización

Uno de los aspectos que evidencia un carácter formal y serio en toda la organización es que ésta se encuentre siempre preparada para afrontar cualquier evento de contingencia o dificultades en general y que le permitan

poder superarlos por lo menos de manera transitoria mientras dure dicho evento.

Es necesario entonces que la definición de un Plan de Contingencia Informático deba hacerse de manera formal y responsable de tal forma que involucre en mayor o menor medida a toda la organización en el Plan de Prevención, Ejecución y Recuperación, por lo que se sugiere formar un equipo de trabajo que coordine, controle y ejecute el plan.

### **2.5.1.2 Identificación del Riesgo**

Denominamos incidencia al hecho que se pueda presentar en cualquier momento, bajo una probabilidad de ocurrencia.

#### **Análisis del Riesgo**

El análisis del riesgo se basa en la información generada en la fase de identificación, que se convierte ahora en información para la toma de decisiones. En la fase del análisis, se consideran tres elementos que permiten aproximar un valor objetivo de riesgo de la lista de riesgos principales: la probabilidad de ocurrencia, la matriz de impacto y finalmente determinar la matriz de riesgo. Con éstas matrices se procede a categorizar los riesgos y a identificar los procesos más vulnerables a ser considerados en el plan.

#### **Probabilidad del Riesgo**

Es la probabilidad de que un suceso se produzca realmente. La probabilidad del riesgo debe ser superior a cero, de no ser así el riesgo no plantea una amenaza al servicio. Así mismo, la probabilidad debe ser inferior al 100% o el riesgo será una certeza; dicho de otro modo, es un problema conocido.

La probabilidad se puede entender también como la posibilidad de la consecuencia, porque si el suceso se produce se supone que la probabilidad de la consecuencia será del 100%.

## **Impacto del Riesgo**

El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida, causados por la consecuencia. Es una calificación aplicada al riesgo, para describir su impacto en relación al grado de afectación del nivel de servicio normal. Cuanto mayor sea el número, mayor es el impacto.

## **Definición de la Matriz de Riesgo**

La ocurrencia de un evento tiene una implicancia sobre las actividades operativas del servicio, en tal sentido, resulta vital conocer el impacto del evento cuando este se presenta, por lo que resulta necesario cuantificar la misma, a efectos de ser objetivos en su análisis.

### **2.5.1.3 Definición de Eventos Susceptibles de Contingencia**

El plan de contingencia abarca todos los aspectos que forman parte del servicio informático, en tal sentido, resulta de vital importancia considerar todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia. Los principales elementos que serán considerados para su evaluación:

#### **Hardware**

- Servidor de base de datos
- Servidor de aplicaciones
- Servidor de notas de pedido
- Servidor de inteligencia de negocios
- Impresoras y colas de impresión

#### **Comunicaciones**

- Equipos de comunicaciones switch y conectores RJ-45
- Equipo de comunicaciones Router y LAN
- Enlaces de cobre y fibra óptica

- Cableado de red de datos.

### **Software**

- Base de datos Oracle 10GR5 / transaccional
- Base de datos Oracle 10GR5 / Datawarehouse
- Servidor de aplicaciones OAS
- Servidor de aplicaciones IIS
- Slego ERP
- Software de notas de pedido por la WEB
- Aplicaciones de BI
- Sistemas operativos
- Antivirus para protección de servidores y estaciones de trabajo.

### **Infraestructura Física**

- Oficina (Matriz – PIA Parque Industrial Ambato)
- Oficina (Planta de producción – Pachanlica)
- Recursos humanos
- Disponibilidad de personal del área de sistemas
- Disponibilidad de personal administrativo
- Disponibilidad de personal de seguridad

#### **2.5.1.4 Elaboración del Plan de Contingencia**

Una de las fases importantes del plan de contingencia es la documentación y revisión de la información que formará parte del plan. En esta fase se detallan los procedimientos, políticas y funciones de los procesos identificados como vulnerables de acuerdo a la matriz de impacto del proyecto 1, en formatos definidos por la Norma ISO 20000:2005 que la empresa está calificada.



### **2.5.1.5 Definición y Ejecución del Plan de Pruebas**

En esta fase se realiza un plan de pruebas para simular que la contingencia puede ocurrir de tal forma que se garantice la reacción inmediata, por intermedio de anexos y formularios de pruebas diseñados por el área de TI de acuerdo a las Normas ISO 20000:2005.

Para el plan de contingencia es importante y conveniente que una autoridad independiente aplique las pruebas de verificación. Para sistemas de menor importancia, la verificación puede realizarse internamente. Las pruebas de verificación, también conocidas como pruebas de calidad, pueden incluir:

- Probar los equipos bajo condiciones que simulen las de operación real.
- Probar los programas para asegurar que se siguen los estándares apropiados y que desempeñan las funciones esperadas.
- Asegurar que la documentación sea la adecuada y esté completa.
- Asegurar que los sistemas de comunicación se ciñan a los estándares establecidos y funcionen de manera efectiva.
- Verificar que los sistemas sean capaces de operar bajo condiciones normales, pero también bajo potenciales condiciones inesperadas.
- Asegurar que se cuente con las debidas medidas de seguridad y que estas se ciñan a las normas establecidas.

### **2.5.1.6 Implantación**

La implantación del plan se lo realizará inmediatamente luego de la aprobación de la Gerencia General Administrativa de la empresa.

### **2.5.1.7 Seguimiento y Control**

En la mayoría de las organizaciones se realizan planes de contingencia y no se utilizan o se encuentran desactualizados, sin embargo es importante que los planes sean mantenidos, puesto que de existir cambios en cualquier parte que conforma el plan, ya sean equipos, responsables, contactos,

procedimientos, políticas y funciones desactualizados, el plan pierde valor y el fin para el cual fue creado.

Cuando se realizan cambios al plan de contingencia, se deben probar completamente y hacer las correcciones requeridas. Esto implica el uso de procedimientos formales de control de cambios bajo el manejo del líder del equipo del plan de contingencia.

### **2.5.2 Importancia de los Planes de Contingencias**

Todas las instituciones deberían contar con un plan de contingencia actualizado, debido a que es una valiosa herramienta para disminuir los riesgos que se identificaron en la fase de análisis.

Un plan nos permite ejecutar un conjunto de normas, procedimientos y acciones básicas de respuesta que se debería tomar para afrontar de manera oportuna, adecuada y efectiva la eventualidad de incidentes, accidentes y/o estados de emergencias que pudieran ocurrir en cualquier área de la empresa.

### **2.5.3 Terminología relacionada con el Plan de Contingencias**

#### **Análisis de Riesgo**

Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo. (Gordillo)

#### **Bitácora**

Es un registro escrito de las acciones que se llevaron a cabo en cierto trabajo o tarea. Esta bitácora incluye todos los sucesos que tuvieron lugar durante la realización de dicha tarea, las fallas que se produjeron, los

cambios que se introdujeron y los costos que se ocasionaron. (Biblioteca Juridica Virtual)

### **Business Continuity Planning**

El plan de continuidad de negocio (o sus siglas en inglés BCP, por Business Continuity Plan) es un “paraguas” bajo el que se engloban planes proactivos de negocio, gestión de crisis y planes de recuperación de desastres. El plan pretende establecer las acciones previas que deberán realizarse de manera proactiva en previsión de posibles desastres y las acciones a llevar a cabo con posterioridad a un desastre para la recuperación de servicios con el fin de poder volver a la normalidad. (N, 2012)

El plan pretende establecer las acciones previas que deberán realizarse de manera proactiva en previsión de posibles desastres y las acciones a llevar a cabo con posterioridad a un desastre para la recuperación de servicios con el fin de poder volver a la normalidad.

### **Business Continuity Management**

El British Continuity Institute BCI y el British Standar Institute BSI define Business Continuity Management (BCM) como un proceso de gestion integral que identifica potenciales impactos de una amenaza a la organización y provee una estructura flexible y una capacidad de efectiva respuesta que resguarde los intereses de sus inversionistas, clientes, empleados, reputación, marca y creación de valor. (Posada, 2010)

### **Comité de Contingencia**

El comité de contingencias es el órgano donde se coordinan y aprueban todas las actividades previamente planificadas para ejecutarse en el caso de contingencias del servicio. Este comité se reunirá por lo menos con una periodicidad trimestral y en él se definirán los lineamientos a través de los

cuales se sustentará el plan de contingencia. (Instituto del Mar del Perú IMARPE, 2012)

### **Copias de Respaldo o Seguridad**

La palabra Backup significa respaldo, siendo común el uso de este término dentro del ámbito informático. El respaldo de información es la copia de los datos importantes de un dispositivo primario en uno o varios dispositivos secundarios, esto para que en caso de que el primer dispositivo sufra una avería electromecánica o un error en su estructura lógica, sea posible contar con la mayor parte de la información necesaria para continuar con las actividades rutinarias y evitar pérdida generalizada de datos. (Informatica Moderna)

### **Costos Estimados**

Los costos estimados representan únicamente una tentativa en la anticipación de los costos reales y están sujetos a rectificaciones a medida que se comparan con los mismos. Constituyen un sistema de costos predeterminados tomando en consideración la experiencia de ejercicios anteriores. (González Seco)

### **Desastre**

Son fallas de un sistema crítico, red o fuente de poder en un ambiente de cómputo; las pérdidas irreparables de la información o la interrupción de la funcionalidad del negocio sin un plan para recuperar las actividades lo más pronto posible. (Massella Rivas, Maldonado Rivera, Ortíz Castro, Bardales Duarte, & Massella Rivas, 1999)

### **Diagnóstico**

El diagnóstico es un estudio previo a toda planificación o proyecto y que consiste en la recopilación de información, su ordenamiento, su interpretación y la obtención de conclusiones e hipótesis. Consiste en analizar un sistema y comprender su funcionamiento, de tal manera de

poder proponer cambios en el mismo y cuyos resultados sean previsibles.  
(Cauqueva)

## **ERP**

ERP es una herramienta que permite una mejor administración y gestión de todos los recursos de la organización a través de módulos totalmente integrados unos con otros sobre una plataforma tecnológica centralizada y robusta. (elegirERP)

## **Estrategias de back-up**

Método alternativo de operación para facilitar la operación del sistema en el momento de un desastre. (Massella Rivas, Maldonado Rivera, Ortíz Castro, Bardales Duarte, & Massella Rivas, 1999)

## **Eventos**

Un evento es una variante de las propiedades para los campos cuyos tipos sean delegados. Es decir, permiten controlar la forma en que se accede a los campos delegados y dan la posibilidad de asociar código a ejecutar cada vez que se añada o elimine un método de un campo delegado. (González Seco)

## **Fases**

Son una serie de pasos lógicos secuenciales parte de un proyecto.

## **Frecuencia de ocurrencia**

La cantidad de veces que ocurre un evento durante un periodo de tiempo.

## **Implantación**

Es la última fase del desarrollo de sistemas, es el proceso de instalar equipos o software nuevos, resultado de un análisis y diseño previo como

resultado de la sustitución o mejoramiento de la forma de llevar a cabo un proceso automatizado. (tareas)

### **Implementación**

La implementación es la etapa donde efectivamente la arquitectura y el sistema informático se unen como un todo. La implementación de tecnología informática requiere de ciertas habilidades que normalmente no están disponibles en todas las empresas, por eso se debe tener en cuenta los factores propios de los proyectos informáticos. (conceptUP technology)

### **Impacto**

Son daños ocasionados a la empresa como resultado del ataque de una amenaza a la vulnerabilidad del sistema. Por lo general es cuantificada en unidades monetarias o por pérdidas ocasionadas. (Massella Rivas, Maldonado Rivera, Ortíz Castro, Bardales Duarte, & Massella Rivas, 1999)

### **Impacto del Riesgo**

El impacto del riesgo mide la gravedad de los efectos adversos, o la magnitud de una pérdida, causados por la consecuencia. Es una calificación aplicada al riesgo, para describir su impacto en relación al grado de afectación del nivel de servicio normal. Cuanto mayor sea el número, mayor es el impacto. (Instituto del Mar del Perú IMARPE, 2012)

### **Mantenimiento del Plan**

Una de las etapas que usualmente se desarrollan en la elaboración de un plan de contingencias en donde se definen los responsables de mantenimiento del plan, se definen para cada área, responsables para la actualización de la información y se definen procedimientos de revisión y actualización del plan. (EPM Microdata Ltda )

## **Matriz de Riesgo**

Una matriz de riesgo constituye una herramienta de control y de gestión normalmente utilizada para identificar las actividades, procesos y productos, de una empresa, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos relacionados con estos riesgos o factores de riesgo. Igualmente, una matriz de riesgo permite evaluar la efectividad de una adecuada gestión y administración de los riesgos que pudieran impactar los resultados y por ende al logro de los objetivos de una organización.

## **Metodología PDCA**

El ciclo PDCA de mejora continua, también conocido como ciclo de Deming, es una metodología para la mejora. Nace de un análisis de riesgo donde, entre otras amenazas, se identifican aquellas que afectan a la continuidad del negocio. (Aiteco Consultores)

## **Plan de Contingencias**

El plan de contingencia informático es un documento que reúne conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones – TICs, cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización. (Instituto del Mar del Perú IMARPE, 2012)

## **Plan de Ejecución**

Es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente de contingencia y que activa un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentre disponible. (Instituto del Mar del Perú IMARPE, 2012)

### **Plan de Prevención o de Respaldo**

Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en los factores identificados en el presente plan. (conceptUP technology)

### **Plan de Pruebas**

Un plan de pruebas permite especificar lo que desea probar y cómo ejecutar dichas pruebas. Un plan de pruebas se puede aplicar a una iteración concreta de un proyecto. Se puede tener solo un conjunto de pruebas predeterminado para los casos de prueba o puede crear una jerarquía de conjuntos de pruebas. (Microsoft , 2013)

### **Plan de Recuperación**

Es el conjunto de acciones que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia. (SolucionesenTI)

### **Prevención**

La prevención contra los riesgos diversos tiene como finalidad la protección de las personas, equipos y trabajos vinculados con la actividad informática. (Biblioteca Juridica Virtual)

### **Probabilidad de Ocurrencia**

Es la probabilidad de que una condición se produzca realmente. La probabilidad del riesgo debe ser superior a cero, pues si no el riesgo no plantea una amenaza al servicio.



## **Procesos Críticos**

Son aplicaciones que han sido definidas como importantes para la operación de la empresa que no es permitida ni la más mínima pérdida de su disponibilidad. (Massella Rivas, Maldonado Rivera, Ortíz Castro, Bardales Duarte, & Massella Rivas, 1999)

## **Recuperación de la Información**

Es proporcionar información relevante al usuario para satisfacer una necesidad de información. Este proceso comienza cuando una persona necesita información sobre un tema especial, ya sea que desee buscarla por si misma o necesite la ayuda de un especialista en recuperación de información, a esto es lo se llama solicitud de búsqueda de información. Para este proceso se requiere de un sistema de recuperación de información. (Pinto Molina, 2009)

## **Recursos**

Un recurso es una fuente o suministro del cual se produce un beneficio. Normalmente, los recursos son material u otros activos que son transformados para producir beneficio y en el proceso pueden ser consumidos o no estar más disponibles. (Mimi Economía)

## **Riesgos**

Un riesgo es un problema potencial que puede ocurrir en un procesador segmentado. Típicamente los riesgos se clasifican en tres tipos: riesgos de datos, riesgos de salto o de control y riesgos estructurales. (Osorio Osorio, 2013)

## **Simulación**

La simulación es una técnica para analizar y estudiar sistemas complejos. Permite reunir información pertinente sobre comportamiento del sistema o proceso.

## **Sistemas de Información**

Un sistema de información es un conjunto de elementos interrelacionados con el propósito de prestar atención a las demandas de información de una organización, para elevar el nivel de conocimientos que permitan un mejor apoyo a la toma de decisiones y desarrollo de acciones. (Dangel)

## **Tecnología de Información**

Se conoce como tecnología de información TI a la utilización de tecnología, específicamente computadoras y ordenadores electrónicos, para el manejo y procesamiento de información, específicamente la captura, transformación, almacenamiento, protección, y recuperación de datos e información.

## **Validación**

La validación de datos es una de las áreas más importantes a tener en cuenta, especialmente en el desarrollo de sistemas conectados a redes como Internet. Validar datos hace referencia a verificar, controlar o filtrar cada una de las entradas de datos que provienen desde el exterior del sistema. (ALEGSA)

## **Vulnerabilidad**

Cualquier debilidad existente en un sistema. Más específicamente, la susceptibilidad de un sistema para hacer atacada por alguna amenaza. La vulnerabilidad de un sistema puede existir independientemente de cualquier amenaza existente. (Massella Rivas, Maldonado Rivera, Ortíz Castro, Bardales Duarte, & Massella Rivas, 1999)

## PECS

Son los procesos estratégicos, procesos claves y procesos de soporte. Se refiere al establecimiento y aplicación de los procesos que permita alcanzar los objetivos.

## Y2K

Es una sigla que en el lenguaje de Internet indica el año 2000. La letra Y significa año (year) y K, kilo (1.000). El famoso Y2K (también conocido como efecto 2000, error del milenio, problema informático del año 2000) es un bug o error de software causado por la costumbre que habían adoptado los programadores de omitir la centuria en el año para el almacenamiento de fechas, generalmente para economizar memoria, asumiendo que el software sólo funcionaría durante los años cuyos nombres comenzaran con 19. Lo anterior tendría como consecuencia que después del 31 de diciembre de 1999, sería el 1 de enero de 1900 en vez de 1 de enero de 2000. (Libertad Digital INTERNET)

## 2.6 Marco Conceptual

En la figura 15 se mencionan los temas relacionados al proceso de administración de un riesgo aplicando las fases de la implantación de un plan de contingencias.

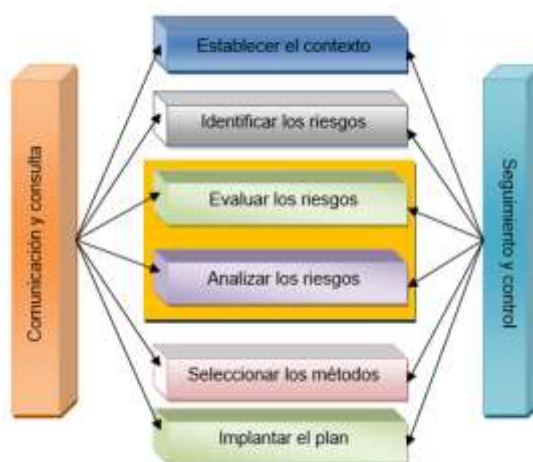


Figura 15. Procesos de Administración de un Riesgo

En el cuadro 2 se describe el proceso de administración de un riesgo aplicando las fases de la implantación de un plan de contingencias.

**Cuadro 2.**  
**Proceso de la Administración del Riesgo**

Paso	Definición
IDENTIFICACIÓN DEL RIESGO	Determinar cuáles son las exposiciones más importantes al riesgo en la unidad de análisis (familia, empresa o entidad).
EVALUACIÓN DEL RIESGO	Es la cuantificación de los costos asociados a riesgos que ya han sido identificados.
SELECCIÓN DE MÉTODOS DE LA ADMINISTRACIÓN DEL RIESGO	Depende de la postura que se quiera tomar: evitar del riesgo (no exponerse a un riesgo determinado); prevención y control de pérdidas (medidas tendientes a disminuir la probabilidad o gravedad de pérdida); retención del riesgo (absorber el riesgo y cubrir las pérdidas con los propios recursos) y finalmente, la transferencia del riesgo (que consiste en trasladar el riesgo a otros, ya sea vendiendo el activo riesgoso o comprando una póliza de seguros).
IMPLEMENTACIÓN	Poner en práctica la decisión tomada.
REPASO Y SEGUIMIENTO	Las decisiones se deben de evaluar y revisar periódicamente.

## **CAPITULO III**

### **METODOLOGÍA DE LA INVESTIGACIÓN**

#### **1.1 Metodología de Investigación**

##### **1.1.1 Ubicación Geográfica del Proyecto de Investigación.**

Una vez implementado el ERP en la empresa Técnicos Agropecuarios del Ecuador TADEC CIA. LTDA. se ha procedido a realizar el levantamiento de la información en el área de TI de la empresa.

##### **1.1.2 Método de investigación, Técnicas e Instrumentos de Recolección y Procesamiento de Datos e Información.**

###### **1.1.2.1 Método de Investigación**

###### **Bibliográfica documental**

La investigación tuvo esta modalidad porque se acudió a fuentes de información secundaria en libros, revistas especializadas, publicaciones módulos y artículos de Internet. Por necesidad se acudió a fuentes primarias obtenidas a través de documentos válidos y confiables.

###### **De campo**

Se trabajó con la modalidad de investigación de campo porque el investigador acudió al lugar en donde se producen los hechos donde interactuó y recabó información de una realidad o contexto determinado.

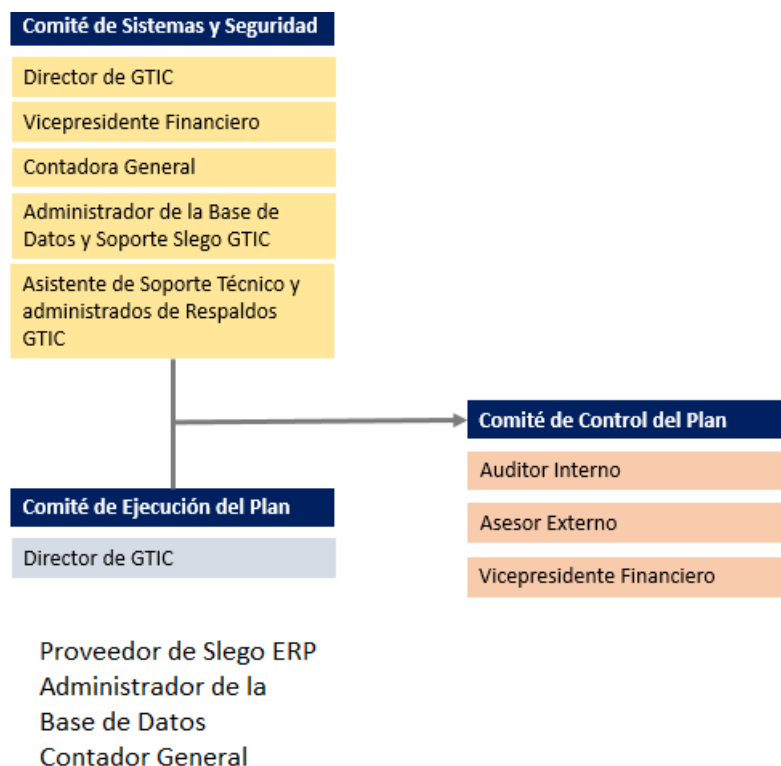
###### **1.1.2.2 Técnicas e Instrumentos de Recolección**

###### **Levantamiento de Información**

Se ha procedido al levantamiento de información de los siguientes recursos:


## Comité de la Organización

En la figura 16 se muestra el organigrama la distribución del comité de la organización.



**Figura 16. Organigrama del Comité de la Organización**

A continuación se describe el manual de funciones del área de TI

	<b>PROCEDIMIENTO GTIC</b>	Código: 001
	MANUAL DE DESCRIPCION DE FUNCIONES	
<b>OBJETIVO</b>	<b>ALCANCE</b>	
Contar con un documento que norme la estructura organizacional actual del departamento de GTIC permitiendo de esta manera mejorar los servicios que proporcionamos. Además, de definir para cada puesto los deberes y responsabilidades, estableciendo los requisitos mínimos para ocupar cada uno de éstos.	Desde las funciones Hasta Los requisitos del cargo.	
<b>I. IDENTIFICACIÓN</b>		
<b>Nombre del Puesto</b>	<b>DIRECTOR GTIC</b>	
<b>N° Personas a</b>	2	

<b>cargo</b>	
<b>Ubicación</b>	Parque Industrial
<b>Ámbito de Operación</b>	Operativo
<b>II. RELACIONES DE AUTORIDAD</b>	
<b>Jefe Inmediato</b>	Vicepresidente Administrativo
<b>Subordinados directos</b>	Asistente Hardware y Software, Administrador de Base de Datos
<b>Dependencia Funcional</b>	Gerencia General
<b>III. PROPÓSITO DEL PUESTO</b>	
<ol style="list-style-type: none"> <li>1. Dirigir en forma administrativa y técnica del área de procesamiento de datos en la empresa, seleccionar Software y Hardware, programación y operaciones.</li> <li>2. Interactuar con los Jefes Departamentales de otras áreas que tengan relación con el departamento de sistemas, para lograr satisfacer las necesidades de las áreas usuaria.</li> <li>3. Proporcionar la visión y liderazgo para el desarrollo e implementación de iniciativas de tecnología de la información.</li> </ol>	
<b>IV. FUNCIONES Y RESPONSABILIDADES</b>	
<ol style="list-style-type: none"> <li>1. Coordinar el mantenimiento preventivo y correctivo a las computadoras.</li> <li>2. Cotizar equipos de cómputo.</li> <li>3. Obtener respaldos de información.</li> <li>4. Creación de cuentas de usuario para comunicación interna y externa vía mail.</li> <li>5. Realizar informes del estado de las máquinas y de las redes.</li> <li>6. Cumplir con las órdenes de trabajo.</li> <li>7. Planear, organizar, dirigir y controlar, el funcionamiento del Área de Sistemas.</li> <li>8. Determina normas y procedimientos del uso de HW y SW.</li> <li>9. Proponer, elaborar e implantar nuevos sistemas necesarios en la Institución.</li> <li>10. Supervisar y revisar la elaboración de proyectos de organización, métodos y procedimientos, organigramas estructurales, funcionales y de niveles jerárquicos.</li> <li>11. Realiza flujogramas de procesos, normas y procedimientos de Sistemas.</li> <li>12. Coordinar y supervisar la elaboración de manuales, instructivos y formularios para HW y SW.</li> <li>13. Mantener al día las copias de Seguridad y la Seguridad de la Información en la Institución.</li> <li>14. Elaborar informes mensuales de las actividades realizadas.</li> <li>15. Supervisar el trabajo del personal a su cargo.</li> </ol>	
<b>V. REQUISITOS PARA EL PUESTO</b>	
<b>Formación</b>	Título Universitario en el campo de la Informática, Sistemas, Maestría en Ingeniería de Sistemas, Informática, Tecnología de la Información o Administración de Empresas.
<b>Conocimientos</b>	Sólidos conocimientos sobre el desarrollo, implementación y mantenimiento de. Conocimiento de Informática, plataformas de hardware, aplicaciones de software empresarial y sistemas externos. Buena comprensión de las características de los sistemas

	informáticos y las capacidades de integración.
<b>Experiencia</b>	2 años en cargos similares.
<b>Competencias</b>	Emprendimiento, Pensamiento Estratégico, Liderazgo, Orientación a resultados Habilidad numérica
<b>Personalidad</b>	Capacidad para motivar, poseer un alto espíritu de colaboración y de servicio, adaptarse a los cambios con facilidad ser líder, paciente

<b>I. IDENTIFICACIÓN</b>	
<b>Nombre del Puesto</b>	<b>ADMINISTRADOR DE LA BASE DE DATOS Y SOPORTE SLEGO</b>
<b>N° Personas a cargo</b>	1
<b>Ubicación</b>	Parque Industrial
<b>Ámbito de Operación</b>	Operativo
<b>II. RELACIONES DE AUTORIDAD</b>	
<b>Jefe Inmediato</b>	Director GTIC
<b>Subordinados directos</b>	No Aplica
<b>Dependencia Funcional</b>	Gerencia General
<b>III. PROPÓSITO DEL PUESTO</b>	
<ol style="list-style-type: none"> <li>1. Administrar la estructura de la Base de Datos.</li> <li>2. Administrar la actividad de los datos.</li> <li>3. Administrar el Sistema Manejador de Base de Datos.</li> <li>4. Establecer el Diccionario de Datos.</li> <li>5. Asegurar la confiabilidad de la Base de Datos.</li> <li>6. Confirmar la seguridad de la Base de Datos.</li> </ol>	
<b>IV. FUNCIONES Y RESPONSABILIDADES</b>	
<ol style="list-style-type: none"> <li>1. Diseñar, implantar y mantener las bases de datos de la institución.</li> <li>2. Desarrollar y administrar las políticas de acceso, estadísticas, encriptación, monitoreo, etc.</li> <li>3. Mantener un alto nivel de seguridad, rendimiento y utilización de las bases de datos y aplicaciones de la Institución.</li> <li>4. Implantar medidas de control que garanticen la operatividad de las bases de datos y su integridad.</li> <li>5. Mantener respaldos de las bases de datos, de tal manera que se garantice la operatividad de la misma en caso de siniestro.</li> <li>6. Mantener un plan de contingencia para recuperación y funcionamiento de la base de datos luego de un siniestro.</li> <li>7. Revisar los resultados de las Auditorías y controles establecidos en la base de datos y tomar acciones cuando sea necesario.</li> <li>8. Garantizar un adecuado nivel de eficiencia y productividad en las aplicaciones.</li> <li>9. Colaborar con su criterio técnico en las soluciones propuestas por la sección de desarrollo de aplicaciones y velar por que se cumplan los estándares.</li> <li>10. Diseñar, implantar y mantener las bases de datos de la institución.</li> <li>11. Desarrollar y administrar las políticas de acceso, estadísticas,</li> </ol>	



<p>encriptación, monitoreo, etc.</p> <p>12. Mantener un alto nivel de seguridad, rendimiento y utilización de las bases de datos y aplicaciones de la Institución.</p> <p>13. Implantar medidas de control que garanticen la operatividad de las bases de datos y su integridad.</p> <p>14. Mantener respaldos de las bases de datos, de tal manera que se garantice la operatividad de la misma en caso de siniestro.</p> <p>15. Mantener un plan de contingencia para recuperación y funcionamiento de la base de datos luego de un siniestro.</p> <p>16. Revisar los resultados de las Auditorías y controles establecidos en la base de datos y tomar acciones cuando sea necesario.</p> <p>17. Colaborar con su criterio técnico en las soluciones propuestas por la sección de desarrollo de aplicaciones y velar por que se cumplan los estándares.</p> <p>18. Optimizar el uso de recursos materiales de la institución en su área de labores.</p> <p>19. Presentar informes, que dentro de la naturaleza de sus funciones, solicitase su jefe inmediato.</p> <p>20. Cumplir con cualquier actividad que dentro de la naturaleza de su cargo solicitase su jefe inmediato.</p>	
<b>V. REQUISITOS PARA EL PUESTO</b>	
<b>Formación</b>	Título Universitario en el campo de la Informática, Sistemas.
<b>Conocimientos</b>	Cursos Administración de Base de datos.
<b>Experiencia</b>	2 años en cargos similares.
<b>Competencias</b>	Comprensión Oral, Detección de Averías, Diseño de Tecnología, Identificación de problemas, Juicio y Toma de Decisiones, Operación y Control, Organización de la Información, Recopilación de Información.
<b>Personalidad</b>	Alto espíritu de colaboración y de servicio, adaptarse a los cambios con facilidad ser líder, trabajo bajo presión.

<b>I. IDENTIFICACIÓN</b>	
<b>Nombre del Puesto</b>	<b>ASISTENTE DE SOPORTE TECNICO Y ADMINISTRADOR DE RESPALDOS</b>
<b>N° Personas a cargo</b>	1
<b>Ubicación</b>	Parque Industrial
<b>Ámbito de Operación</b>	Operativo
<b>II. RELACIONES DE AUTORIDAD</b>	
<b>Jefe Inmediato</b>	Director GTIC
<b>Subordinados directos</b>	No Aplica
<b>Dependencia Funcional</b>	Gerencia General
<b>III. PROPÓSITO DEL PUESTO</b>	
<p>1. Realizar constantes investigaciones que ayuden a estar al día en materia de seguridad informática, así como prevenir la infección de virus.</p> <p>2. Mantener el adecuado flujo de información en las redes de Voz y Datos.</p> <p>3. Mantener en perfecto funcionamiento todos los equipos de cómputo, de</p>	

<p>impresión y de copiado de la empresa.</p> <p>4. Planear la actualización del equipo informático y de diagramas de la red de cómputo y comunicación.</p> <p>5. Coordinar el mantenimiento preventivo y correctivo a equipos.</p>	
<b>IV. FUNCIONES Y RESPONSABILIDADES</b>	
<p>1. Diseñar, implantar y mantener las bases de datos de la institución.</p> <p>2. Procurar el perfecto estado físico de los equipos de cómputo, así como recomendar a los usuarios evitar prácticas que pudieran alterar su estado físico.</p> <p>3. Atender las peticiones de soporte técnico de los usuarios.</p> <p>4. Efectuar y coordinar los mantenimientos que se encuentren previamente calendarizados.</p> <p>5. Realizar los cableados de voz y datos y las configuraciones necesarias para agregar o actualizar los servicios de dicho tipo.</p> <p>6. Mantener en óptimas condiciones de operación los equipos de cómputo a fin de coadyuvar al cumplimiento de las funciones asignadas a las áreas usuarias.</p> <p>7. Administrar los respaldos de equipos críticos de la empresa.</p> <p>8. Elaborar informes mensuales de las actividades realizadas.</p> <p>9. Cumplir con cualquier actividad que dentro de la naturaleza de su cargo solicitase su jefe inmediato.</p>	
<b>V. REQUISITOS PARA EL PUESTO</b>	
<b>Formación</b>	Titulado en: Ingeniería en Informática, Ingeniería en Sistemas Computacionales, Administración en Sistemas Computacionales, o carreras afines.
<b>Conocimientos</b>	Altos conocimientos de paquetes Office, Sistemas Operativos, Manejo Routers Mikrotik, Conocimientos MAC, telefonía IP Elastix, alto desarrollo y mantenimiento de redes, básico de dibujo, diseño, ilustración.
<b>Experiencia</b>	2 años en cargos similares.
<b>Competencias</b>	Capacidad de coordinación, organización, analítico, creativo, facilidad de palabra/comunicación, trabajo bajo presión, iniciativa, trabajo en equipo, imparcialidad.
<b>Personalidad</b>	Alto espíritu de colaboración y de servicio, adaptarse a los cambios con facilidad ser líder, paciente.

Con el manual se ha procedido a describir las funciones y responsabilidades de los integrantes del Comité de Sistemas y Seguridad.

### **Comité de Sistemas y Seguridad**

- Mantener permanentemente actualizado el plan de contingencia.
- Evaluar el impacto de las contingencias que se presenten.
- Mantener actualizada la matriz de impacto, la matriz de probabilidad de ocurrencia y la matriz de riesgo asociado con Slego ERP.
- Elaborar los informes referidos al plan de contingencias

- Proponer incorporaciones de eventos al plan de contingencia al Comité de Contingencia.
- Proponer la capacitación al personal nuevo del servicio, sobre las actividades que deben ejecutar cuando se presente la contingencia.
- Velar que el personal se encuentre debidamente capacitado y preparado para ejecutar el plan de contingencia.
- Proponer reuniones periódicas sobre el plan de contingencia.

### **Comité de Control del Plan de Contingencia y Seguridad**

- Velar por el cumplimiento del plan de contingencia.
- Analizar el impacto de las contingencias que se presenten tanto internas como externas a la institución.
- Gestionar y verificar el uso de bitácoras, seguimientos y responsables de los cambios solicitados a la base de datos de Slego ERP.
- Revisar los informes referidos al plan de contingencias elaborado por el GTI.
- Controlar que usuarios solicitan cambios e identificar a que procesos afectan para proponer soluciones.
- Proponer la creación de súper usuarios en cada departamento asociado a la funcionalidad y procesos de Slego ERP y la empresa.
- Proponer reuniones periódicas en actividades relacionada al plan de contingencias.
- Auditar los cambios solicitados por los usuarios en Slego ERP tanto en datos como en procesos.

### **Comité de Ejecución del Plan**

- Velar por el cumplimiento del plan en caso que ocurra la contingencia.
- Realizar pruebas pilotos internas para ejecutar el plan y reunir a los responsables.
- Documentar los resultados de las pruebas y verificar que los procesos se encuentren claros e ilustrativos.

- Minimizar los tiempos de respuesta con respecto a la puesta en marcha del plan.
- Ejecutar el plan de contingencias.

Continuando con el proceso de levantamiento de información se anexa los diagramas de:

Anexo 1. Diagrama de Red – Enlaces

Anexo 2. Diagrama de Red PIA

Anexo 3. Hardware – Servidores

### **1.1.2.3 Procesamiento de Datos e Información**

Los datos recolectados se transforman siguiendo ciertos procedimientos:

- Revisión crítica de la información recogida; es decir, limpieza de la información defectuosa: contradictoria, incompleta, no pertinente, etc.
- Repetición de la recolección, en ciertos casos individuales, para corregir fallas de contestación.
- Manejo de información, reajuste de cuadros con casillas vacías o con datos tan reducidos cuantitativamente, que no influyen significativamente en los análisis.
- Estudio estadístico de datos para presentación de resultados.

### **1.1.3 Evaluación de Resultados y Discusión**

De acuerdo con el análisis realizado en el proyecto titulado: “Impacto de la Implantación de un ERP en la empresa TÉCNICOS AGROPECUARIOS DEL ECUADOR CIA. LTDA. TADEC”, en la tabla 1 se mencionan los niveles de riesgo a los cuales se encuentra expuesta la empresa en el área de TI asociado a Slego ERP.

**Tabla 1.**  
**Matriz de Probabilidad de Ocurrencia, Frecuencia, Pérdida y Riesgo**

Área	Preguntas	Probabilidad de Ocurrencia	Frecuencia	Pérdida (USD)	Riesgo
IN	13. ¿Cuántas veces en el año se ha caído el servidor de producción de base de datos?	Muy Probable (5)	4 veces en el año	más de 28 mil	Extremo
SI	16. ¿Cuántas veces en la semana se detectan bloqueos a la base de datos?	Incierto (2)	1 vez por semana	3 mil	Bajo
SI	18. ¿Cuántas veces en el mes se efectúan cambios en las tablas del usuario PRD?	Muy Probable (5)	más de diez veces en el mes	3 mil	Bajo
AG	3. ¿Con qué frecuencia realiza la planificación de nuevos proyectos el área de TI con la Gerencia?	Incierto (2)	1 vez por año	más de 28 mil	Extremo
SI	6. ¿Con qué frecuencia realiza respaldos a la base de datos del usuario PRD?	Improbable (1)	Diario	3 mil	Bajo
SI	7. ¿Con qué frecuencia válida y recupera los respaldos de la base de datos del usuario PRD?	Catastrófico (5)	1 vez por mes	más de 28 mil	Extremo
SI	8. ¿Con qué frecuencia realiza respaldos de los archivos CONTROL FILE, DATA FILE Y REDO LOGS de la base de datos?	Catastrófico (5)	Nunca	más de 28 mil	Extremo
AG	9. ¿Con qué frecuencia se ingresa a la consola de administración de la base de datos para determinar el consumo de los recursos de memoria y procesador?	Menor (2)	Diario	21 mil	Alto
AG	10. ¿Con qué frecuencia se ingresa a la consola de administración del servidor de aplicaciones para administrar los recursos de memoria y procesador?	Menor (2)	Diario	7 mil	Bajo
PP	11. ¿Con qué frecuencia realiza los respaldos del directorio Slego?	Catastrófico (5)	Anual	más de 28 mil	Extremo
PP	23. ¿Con qué frecuencia realiza el seguimiento de las pistas de auditoría?	Catastrófico (5)	Nunca	14 mil	Medio
<b>Riesgo Extremo</b>		<b>5</b>			
<b>Riesgo Alto</b>		<b>1</b>			
<b>Riesgo Medio</b>		<b>1</b>			
<b>Riesgo Bajo</b>		<b>3</b>			

Con esta información de acuerdo a la tabla 1 Matriz de Probabilidad de Ocurrencia, Frecuencia, Pérdida y Riesgo se evidencia que de 11 preguntas 5 corresponden a riesgo extremo, 1 a riesgo alto, 1 a riesgo medio y 3 a riesgo bajo, como se tabula en la tabla 2 Matriz de Riesgos.

**Tabla 2.**  
**Matriz de Riesgos**

1,00	<b>Muy Probable (5)</b>	<b>Bajo</b>		<b>Extremo</b>		
0,75	<b>Probable (4)</b>					
0,5	<b>Posible (3)</b>					
0,25	<b>Incierto (2)</b>	<b>Bajo</b>	<b>Bajo</b>			<b>Extremo</b>
0,01	<b>Improbable (1)</b>			<b>Medio</b>	<b>Alto</b>	<b>Extremo</b>
Probabilidad Anual		<b>Insignificante (1)</b>	<b>Menor (2)</b>	<b>Moderado (3)</b>	<b>Significativo (4)</b>	<b>Catastrófico (5)</b>
	Impacto en miles de USD	3	7	14	21	28 o más

En base a la tabla 2 Matriz de Riesgos se determinará los procesos críticos a ser considerados dentro de la propuesta del Plan de Contingencia del Área de TI asociado a Slego ERP.

## CAPITULO IV

### PLAN DE CONTINGENCIAS

#### 4.1 Objetivos

##### 4.1.1 General

Garantizar la disponibilidad del Software Slego ERP en la empresa Técnicos Agropecuarios del Ecuador Cia. Ltda. TADEC a través de la creación de un plan de contingencias que cubran los procesos críticos identificados en la Matriz de Riesgos.

##### 4.1.2 Específicos

- Levantar los procesos críticos de la matriz de riesgos y documentarlos aplicando metodología ISO 9001:2000.
- Definir los responsables de la ejecución del plan de contingencias con el fin de ubicarlos inmediatamente en caso que ocurra la contingencia.
- Elaborar bitácoras de gestión y control de respaldos y recuperación de la base de datos en torno al usuario PRD.

#### 4.2 Alcance


El plan de contingencia del área de TI se aplica a Slego ERP, tomando en cuenta los siguientes elementos: servidores, bases de datos, respaldo y recuperación del usuario PRD, infraestructura y personal responsable de minimizar los riesgos identificados en la matriz de riesgos que atentan contra el normal funcionamiento de Slego ERP.

### **4.3 Procesos Críticos**

A continuación se desarrollan los procesos críticos de la matriz de riesgos aplicando la metodología ISO 9001:2000.

- 4.3.1 Restauración del Servidor la Base de Datos
- 4.3.2 Restauración del Servidor de Aplicaciones
- 4.3.3 Restauración del Usuario de la Base de Datos PRD
- 4.3.4 Gestión de Respaldo y Recuperación del Usuario PRD
- 4.3.5 Restauración del Modelo Analítico de Ventas
- 4.3.6 Restauración del Modelo de Documentos Electrónicos
- 4.3.7 Restauración del Modelo Notas de Pedido para la Web



	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-001</b>
	<b>Restauración del Servidor la Base de Datos</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

### **1. OBJETIVO**

Habilitar el servidor de base datos de contingencia que se encuentre instalado en un sistema operativo Linux.

### **2. DEFINICIONES Y ABREVIATURAS**

**Administrador de la base de datos:** Es la persona encargada de definir y controlar las bases de datos corporativas, además proporciona asesoría a los desarrolladores, usuarios y ejecutivos que la requieran.

**SQLPlus:** Es un programa de línea de comandos de Oracle que puede ejecutar comandos SQL y PL/SQL de forma interactiva o mediante un script.

**Usuario DBA:** Usuario de una base de datos Oracle, el cual tiene los máximos privilegios de manipular una base de datos.

**SID:** Nombre de una instancia de base de datos, con la cual se identifica a una base de datos.


### **3. RESPONSABLES**

#### **3.1 POLÍTICAS**

- El servidor de contingencia de base de datos debe estar ubicado en un área restringida fuera del área de TI.
- El servidor de contingencia de base de datos debe estar encendido para validar su funcionalidad.
- El responsable de TI debe contar con el acta de instalación y configuración del servidor de bases de datos, en donde se describan los usuarios, contraseñas y demás información técnica del equipo, base de datos y sistema operativo.
- La versión de la base de datos y del SOS debe ser la misma que del servidor de producción.

#### **3.2 CONTROLES**

- Verificar el correcto funcionamiento servidor en lo que a hardware se refiere.

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-001</b>
	<b>Restauración del Servidor la Base de Datos</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

- Verificar el funcionamiento del sistema operativo.
- Verificar el reloj del equipo que se encuentre consistente de acuerdo con la fecha que entra en funcionamiento.

### 3.2.1 DOCUMENTOS DE ENTRADA

- Claves de acceso de usuario propietario del software Oracle. (Acta de configuración)
- Manuales de configuración de las bases de datos que se encuentran instaladas en ese servidor.

### 3.2.2 DOCUMENTOS DE SALIDA


- Acta de configuración

## 4. PARAMETROS

- Usuarios:
  - root
  - oracle
  - sys
  - prd
- IP del servidor
- SID de la base de datos
- Directorio de instalación de product y de instancia
- Ver SOS Linux Red Hat Enterprise 6.0
- Ver base de datos 11gR2
- Claves

## 5. DESARROLLO DE ACTIVIDADES

Responsable	No.	Actividades
Administrador del Servidor de Base de Datos.	1	Enciende el equipo con usuario root.
Administrador del Servidor de Base de Datos.	2	Inicie una sesión en el servidor de bases de datos Oracle como el propietario del software Oracle.

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-001</b>
	<b>Restauración del Servidor la Base de Datos</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

Administrador del Servidor de Base de Datos.	3	Inicie una sesión en la instancia de Oracle con SQLPlus como usuario administrador de base de datos (SYS). Con un SID de Oracle para conseguir una instalación limpia.
Administrador del Servidor de Base de Datos.	4	Establezca la variable de entorno en la línea de mandatos.
Administrador del Servidor de Base de Datos.	5	Inicie SQLPlus desde la línea de mandatos.
Administrador del Servidor de Base de Datos.	6	Inicie una sesión en SQLPlus como un usuario DBA.
Administrador del Servidor de Base de Datos.	7	Suprima el usuario de base de datos (máximo, de forma predeterminada) con un comando SQL.
Administrador del Servidor de Base de Datos.	8	Dar de baja e iniciar nuevamente la base de datos, esto sin desconectarse de SQLPlus.
Administrador del Servidor de Base de Datos.	9	Vuelva a crear manualmente la base de datos.
<b>Sugerencias:</b> Mientras usted esté realizando algún proceso en el SQLPlus no se desconecte.		

## 6. ANEXOS

- Acta de Configuración Servidor de Contingencia de Base de Datos
- Manual de configuración de la Base de Datos en Linux

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-002</b>
	<b>Restauración del Servidor de Aplicaciones</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

## **1. OBJETIVO**

Habilitar el servidor de aplicaciones de contingencia para el correcto funcionamiento de Slego ERP en caso de existir caídas con el servidor de producción.

## **2. DEFINICIONES Y ABREVIATURAS**

**Ambiente:** Configuración de ciertos parámetros únicos para determinadas empresas.

**Parámetro:** Valor propio de configuración que se mantendrá en un determinado ambiente.

**Domino:** Un dominio se define como un conjunto de caracteres alfanuméricos que conforman un nombre único el cual está ligado y define a un sitio web.

**Path virtual:** Ubicación de un archivo o directorio en un determinado servidor.

**Servidor de Reportes:** Se encarga de proveer a los usuarios una manera fácil de crear y generar reportes, utilizar reportes previamente parametrizados y diseñados, además de permitir hacerlo rápidamente y de manera segura.

**Consola de Administración:** es un interfaz que provee acceso a las funciones del servidor de administración, de manera local o remotamente a través de la red.

**Usuario Administrador de WebLogic:** es un usuario para que tiene acceso de administrador. Un usuario con acceso de administrador tendrá los mismos permisos que el creador de la cuenta, con la única diferencia de que este tipo de usuario se puede eliminar y cambiar.

**Instancias:** es la aplicación de un esquema a un conjunto finito de datos. En palabras no tan técnicas, se puede definir como el contenido de una tabla en un momento dado, pero también es válido referirnos a una instancia cuando trabajamos o mostramos únicamente un subconjunto de la información contenida en una relación o tabla.

**Colas de Impresión:** La cola de impresión te permite enviar documentos de gran tamaño, o varios documentos, a una impresora sin tener que esperar que se complete la impresión para seguir con tu siguiente tarea.

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-002</b>
	<b>Restauración del Servidor de Aplicaciones</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

### **3. RESPONSABLES**

#### **3.1 POLÍTICAS**

- El servidor de contingencia de base de datos debe estar ubicado en un área restringida fuera del área de TI.

#### **3.2 CONTROLES**

- Verificar el correcto funcionamiento servidor en lo que a hardware se refiere.
- Verificar el funcionamiento del sistema operativo Linux Red Hat ver 6.0.
- Verificar el reloj del equipo que se encuentre consistente de acuerdo con la fecha que entra en funcionamiento.
- Verificar el arranque por la consola del servidor.
- Verificación por consola que estén arriba los servidores y la instancia OHS.
- Verificar que el ambiente de trabajo funcione correctamente.

##### **3.2.1 DOCUMENTOS DE ENTRADA**

- Archivo formsweb.cfg
- Archivo de Configuración del Ambiente .env
- Archivo rwservlet.config y rwservlet.properties
- Directorios de Instalación.
- Acta Configuración e Instalación Servidor de Aplicaciones.

##### **3.2.2 DOCUMENTOS DE SALIDA**

- Acta Configuración e Instalación Servidor de Aplicaciones

### **4. PARAMETROS**

- envFile: Archivo punto env del ambiente.
- Form: Formulario punto fmx con el que arranque la aplicación.
- background: Fondo con el que arranque la aplicación.
- pageTitle: Título de la página de la aplicación.
- Height: Alto de la ventana de la aplicación.
- Width: Ancho de la ventana de la aplicación.

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-002</b>
	<b>Restauración del Servidor de Aplicaciones</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya


- FORMS\_PATH: Directorio donde estén ubicados los formularios y librerías compiladas.
- REPORTS\_PATH: Directorio donde este ubicados los reportes.
- ORACLE\_PATH: Directorio de los formularios y librerías compiladas.

## **5. DESARROLLO DE ACTIVIDADES**

<b>Responsable</b>	<b>No.</b>	<b>Actividades</b>
Administrador del Servidor de Aplicaciones	1	Instalar Weblogic y Forms and Reports 11g. Archivo Manual de instalación y configuración de Weblogic forms y Reports.
Administrador del Servidor de Aplicaciones	2	Configurar dominio en Weblogic.
Administrador del Servidor de Aplicaciones	3	Configurar los path virtuales necesarios.
Administrador del Servidor de Aplicaciones	4	Configurar el archivo formweb.cfg con los parámetros del ambiente.
Administrador del Servidor de Aplicaciones	5	Crear el archivo .env del ambiente.
Administrador del Servidor de Aplicaciones	6	Verificar los jars que ocupa el ambiente.
Administrador del Servidor de Aplicaciones	7	Crear el Report Server Component de acuerdo.
Administrador del Servidor de Aplicaciones	8	Configurar el archivo rwserver.config y rwservlet.properties con los valores necesarios para que el servidor de reportes pueda trabajar correctamente.
Administrador del Servidor de Aplicaciones	9	Arrancar el opmnctl y levantar todos los componentes del servidor.
Administrador del Servidor de Aplicaciones	10	Verificar que los componentes estén levantados.

## **6. ANEXOS**

- Acta de Configuración del Servidor de Aplicaciones
- Manual de instalación y configuración de Weblogic Forms y Reports.

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-003</b>
	<b>Restauración del usuario de la Base de Datos PRD</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

### **1. OBJETIVO**

Recuperar el usuario PRD en la instancia TDC para el correcto funcionamiento de Slego ERP en caso de existir caídas con el Servidor de Producción.

### **2. DEFINICIONES Y ABREVIATURAS**

**Import:** Es una utilidad de Oracle para realizar backups lógicos de Oracle y luego poderlos restaurar. Copian el contenido de la BD pero sin almacenar la posición física de los datos.

### **3. RESPONSABLES**

#### **3.1 POLÍTICAS**

- Realizar la restauración del usuario de base de datos si existe algún evento de contingencia o pruebas.

#### **3.2 CONTROLES**


- Verificar contraseñas de usuario.

#### **3.2.1 DOCUMENTOS DE ENTRADA**

- Archivo formsweb.cfg
- Archivo dmp (Backups lógicos de Oracle)
- Archivo crea\_prd.sql (Crear usuario PRD)
- Archivo grtusu (Grants para el usuario PRD).
- Archivo prcsys (Permisos, funciones, paquetes para el PRD)

### **4. PARAMETROS**

- Usuario.
- Contraseña.
- Ruta archivo dmp.
- Tamaño buffer.
- Permisos.
- Instancia.

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-003</b>
	<b>Restauración del usuario de la Base de Datos PRD</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya


### **5. DESARROLLO DE ACTIVIDADES**

<b>Responsable</b>	<b>No.</b>	<b>Actividades</b>
Administrador del Slego	1	Identificar la ubicación del respaldo del archivo .dmp
Administrador del Slego	2	Identificar las claves de usuarios.
Administrador del Slego	3	Copiar el archivo .dmp en el servidor de base de datos.
Administrador del Slego	4	Crear usuario PRD con su tablespace. Archivo crea_prd.sql
Administrador del Slego	5	Ejecutar grants al usuario PRD. Archivo grtusu.sql
Administrador del Slego	6	Conectar con usuario Oracle.
Administrador del Slego	7	Instanciar el ORACLE_HOME.
Administrador del Slego	8	Instanciar el ORACLE_SID.
Administrador del Slego	9	Ejecutar import de Oracle.
Administrador del Slego	10	Ingresar los parámetros que solicita la utilidad del import.
Administrador del Slego	11	Subir seguridades ejecutando el archivo PRCSYS.SQL
<b>Sugerencia:</b> Ejecutar individualmente cada link del archivo PRCSYS.SQL.		

### **6. ANEXOS**

- No aplica



	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-004</b>
	<b>Gestión de Respaldo y Recuperación del Usuario PRD</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

### **1. OBJETIVO**

Realizar una adecuada gestión del respaldo y recuperación del usuario PRD en la base de datos TDC para la empresa TADEC CIA. LTDA.

### **2. DEFINICION Y ABREVIATURAS**

**Import:** Es una utilidad de Oracle para realizar backups lógicos de Oracle y luego poderlos restaurar. Copian el contenido de la BD pero sin almacenar la posición física de los datos.


**Export:** Es una utilidad que genera un archivo binario con toda la información de estructura y contenido de una base de datos. Estos archivos sólo pueden ser leídos por la utilidad de importación de Oracle (IMPORT). Incluye todas las definiciones de objetos y los datos que se deseen dentro de una base de datos.

**Bitácoras:** Herramienta que permite registrar, analizar, detectar y notificar eventos que sucedan en cualquier sistema de información utilizado en las organizaciones.

### **3. RESPONSABLES**

#### **3.1 POLÍTICAS**

- Realizar la restauración del usuario de base de datos si existe algún evento de contingencia o pruebas.
- Se debe realizar el respaldo diario del usuario PRD a las 6 am y a las 11 pm de los 7 días de la semana.
- Se debe realizar la verificación del archivo creado TDCPRDddmmaahh.dmp en forma automática en el directorio \Slego\Respaldos
- Pasar los archivos del directorio \Slego\Respaldos a un disco externo diariamente para garantizar la independencia del servidor con el respaldo.
- Se signará un responsable de respaldo por semana entre el administrador de Slego y el responsable de infraestructura.
- Registrar diariamente la bitácora de control de acuerdo al responsable y a la validación de los archivos.dmp

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-004</b>
	<b>Gestión de Respaldo y Recuperación del Usuario PRD</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

- Una vez por semana se debe realizar la validación del import con un export del respaldo del día 7 en la base de datos de pruebas para validar la integridad de la información.
- Se debe cambiar la contraseña del usuario PRD el último día del mes.

### 3.2 CONTROLES

- Verificar contraseñas de usuario.

#### 3.2.1 DOCUMENTOS DE ENTRADA


- Bitácora de respaldo
- Bitácora de recuperación

### 4. PARAMETROS


- Usuario.
- Usuario de respaldo.
  - Prd
- Contraseña.
  - xxxxxx
- Ruta archivo dmp.
  - \u01\slego\respaldos
- Nombre del archivo
  - TDCPRDddmmyyy.dmp
- Nombre de la instancia de la BD
  - 1.TDC
  - 2. PTDC.

### 5. DESARROLLO DE ACTIVIDADES

Responsable	No.	Actividades para del respaldo de prd
Administrador de Slego	1	Verificar que la tarea se encuentre programada automáticamente en el Cronanb en el servidor de SRVTDCPRD ip 192.168.1.2 con SOS Linux
Administrador de Slego	2	Ubicarse en el \u01\slego\respaldos y verificar que el archivo TDCPRDddmmyyy.dmp exista y comparar el tamaño del archivo del día anterior que mantenga una consistencia de crecimiento del 1 al 5% diario.

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-004</b>
	<b>Gestión de Respaldo y Recuperación del Usuario PRD</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

Administrador de Slego	3	Copiar TDCPRDddmmyyy.dmp en un disco externo en una carpeta nombrada por aaaa y mes
Administrador de Slego	4	Llenar la bitácora de registro que se muestra en la tabla 3. Bitácora de Registro de Control de Respaldos Diarios del usuario PRD
Administrador de Slego	5	Guardar el disco externo en la caja fuerte de la empresa.
Administrador de Slego	6	Ejecutar import de Oracle.
Administrador de Slego	7	Ingresar los parámetros que solicita la utilidad del Import.
<b>Responsable</b>	<b>No.</b>	<b>Actividades para del respaldo de prd</b>
Administrador de Slego	1	Verificar la instancia de datos a recuperar PTDC
Administrador de Slego	2	Identificar el archivo TDCPRDddmmyyy.dmp del acuerdo a la política establecida por la empresa.
Administrador de Slego	3	Copiar el archivo en el Servidor SRVTDCPRD \u01\slego\recuperacion
Administrador de Slego	4	Crear el usuario PRD
Administrador de Slego	5	Ejecutar el comando: Import usuario/clave@instancia archivo.dmp
Administrador de Slego	6	Seguir las instrucciones de la importación de datos, dar las opciones por defecto excepto importar esquema a N Import toda el área a Yes, el resto de opciones a N. Para más información seguir el PEC03.
Administrador de Slego	7	Ejecutar subir seguridades.
Contador General	8	Conectarse al Slego ERP como usuario de CONTABILIDAD, ingresar al módulo de contabilidad y generar los siguientes Reportes: Balance General Balance de Resultados Estado de Cuenta de Clientes Estado de Cuenta de Proveedores SalDOS de Bancos

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-004</b>
	<b>Gestión de Respaldo y Recuperación del Usuario PRD</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

		Y comparar con el sistema en línea de acuerdo a la fecha que recupero el respaldo. Si existen inconsistencias notificar al área sistemas para la correspondiente verificación del respaldo.
Administrador de Slego	9	Realizar el respectivo Check List en la tabla 4. Bitácora de Registro de Control de Recuperación del usuario PRD.

## 6. ANEXOS

- Tabla 4. Bitácora de Registro de Control de Recuperación

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-005</b>
	<b>Restauración del Modelo Analítico de Ventas</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

### **1. OBJETIVO**

Proporcionar una guía de restauración en caso de que el modelo analítico de ventas deje de funcionar ya sea por falla de software o hardware.

### **2. DEFINICIÓN Y ABREVIATURAS**

**Business Intelligence (BI):** Es la habilidad para transformar los datos en información, y la información en conocimiento, de forma que se pueda optimizar el proceso de toma de decisiones en los negocios.

**Datawarehouse (DWH):** Es la base de datos que se modela y construye en la fase de análisis del proyecto y es poblado con procesos ETL, una vez disponible la herramienta lee la información, de acuerdo al modelo construido, para elaborar los informes, consultas, cuadros de mando, cubos, etc. que requiera el cliente.

**Metadata (MD):** Son las tablas internas de Microstrategy donde se guarda toda la información del modelo de datos que se define y contiene todos los objetos que se construye utilizando la herramienta (filtros, informes, indicadores, etc.).

**MicroStrategy Intelligence Server:** Es el motor de procesamiento y gestión de los trabajos de las aplicaciones de informes, análisis y monitorización. Utiliza una arquitectura orientada al servicio (SOA), y estandariza en una única plataforma todas las necesidades de análisis y reporting, a través de varios canales de acceso: Web browsers, Microsoft® Office, Desktop clients, y email. En este paso de la configuración se asocia al Intelligence Server el esquema de base de datos del METADATA y permite indicar parámetros adicionales de configuración.

### **3. RESPONSABLES**

#### **3.1 POLÍTICAS**

- Se procederá aplicar este plan de contingencia cuando:
- **HARDWARE:** En caso de que el equipo sufra un daño irreversible físicamente y por lo cual se proceda a cambiarlo total o parcialmente

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-005</b>
	<b>Restauración del Modelo Analítico de Ventas</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

(disco duro) por lo cual se requiere volver a instalar.

- SOFTWARE: En caso de que el equipo sufra un daño irreversible lógicamente y por lo cual se requiera formatear el disco. Si requiere actualizar la versión de Microstrategy o si requiere actualizar la versión del modelo analítico.

### 3.2 CONTROLES

- Verificación del funcionamiento del equipo habilitado.

#### 3.2.1 DOCUMENTOS DE ENTRADA

- Archivo formsweb.cfg
- Respalos de base de datos DWH\_BLT
- Respalos de base de datos MD\_BLT

#### 3.2.2 DOCUMENTOS DE SALIDA

- Acta de configuración del equipo

### 4. PARAMETROS

- Monto Máximo: 500 por mes
- Plazo Máximo: 6 meses.

### 5. DESARROLLO DE ACTIVIDADES

#### 5.1 Daño irreversible en el sistema operativo del servidor asignado para BI MicroStrategy

Responsable	No.	Actividades instalación base de datos Oracle
Administrador de BI	1	Obtener el respaldo de la base de datos del DWH_BLT
Administrador de BI	2	Obtener el respaldo de la base de datos del MD_BLT
Administrador de BI	3	Respaldo los instaladores y archivos de configuración de MSTR
Administrador de BI	4	Formatear el servidor.
Administrador de BI	5	Instalar sistema operativo Windows 2008 server de 64 bits con dos particiones C y D, asignar.
Administrador de BI i	6	Instalar base de datos ORACLE 11g.

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-005</b>
	<b>Restauración del Modelo Analítico de Ventas</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

Administrador de BI	7	Crear base de datos tipo almacén de datos con el SID: BIMSTR y password: BIMSTR+año_en_curso.
Administrador de BI	8	Crear instancias de base de datos DWH_BLT y MD_BLT
Administrador de BI	9	Recuperar e importar base de datos DWH_BLT
Administrador de BI	10	Recuperar e importar base de datos MD_BLT

**Sugerencias:** Para los punto 6, 7 y 8 ver manual de instalación y configuración de base de datos.

#### 5.1.1 Instalación MicroStrategy

Responsable	No.	Actividades
Administrador de BI	1	Instalar software de Microstrategy
Administrador de BI	2	Crear odbc para DWH
Administrador de BI	3	Crear odbc para MD
Administrador de BI	4	Configuración del itelligence server

**Sugerencias:** Para realizar estas actividades ver manual de instalación y configuración de Microstrategy.

#### 5.2 Subir base de datos de BI


Responsable	No.	Actividades
Administrador de BI	1	Obtener el respaldo de la base de datos del DWH_BLT
Administrador de BI	2	Obtener el respaldo de la base de datos del MD_BLT
Administrador de BI	3	Recuperar e importar base de datos DWH_BLT
Administrador de BI	4	Recuperar e importar base de datos MD_BLT

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-005</b>
	<b>Restauración del Modelo Analítico de Ventas</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

## 6. ANEXOS

- Manual de instalación y configuración de base de datos.
- Manual de instalación y configuración de Microstrategy



	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-006</b>
	<b>Restauración del Modelo de Documentos Electrónicos</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

### **1. OBJETIVO**

Proporcionar una guía de restauración en caso de que el modelo de facturación electrónica deje de funcionar.

### **2. DEFINICIÓN Y ABREVIATURAS**

**Archivo de configuración:** Es un archivo .txt el cual contiene todos los parámetros para que funcione el software.

**Directorio de archivos:** Es un archivo común al cual se le asignado una estructura particular.

**Framework 4.0:** Es un componente de software que provee soluciones precodificadas y gestiona la ejecución de programas escritos específicamente escritos para este framework.

### **3. RESPONSABLES**

#### **3.1 POLÍTICAS**

- Se procederá aplicar este plan de contingencia cuando:
- **HARDWARE:** En caso de que el equipo sufra un daño irreversible físicamente y por lo cual se proceda a cambiarlo total o parcialmente (disco duro) por lo cual se requiere volver a instalar.
- **SOFTWARE:** En caso de que el equipo sufra un daño irreversible y por lo cual se requiera formatear el disco.

#### **3.2 CONTROLES**


- Verificación del funcionamiento del equipo habilitado.

##### **3.2.1 DOCUMENTOS DE ENTRADA**

- Resaldos de archivo de configuración
- Resaldos de estructura de directorio de archivos

##### **3.2.2 DOCUMENTOS DE SALIDA**

- Acta de configuración del equipo


	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-006</b>
	<b>Restauración del Modelo de Documentos Electrónicos</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

#### **4. DESARROLLO DE ACTIVIDADES**

<b>Responsable</b>	<b>No.</b>	<b>Actividades</b>
Administrador de SDocE	1	Obtener el respaldo del archivo de configuración de facturación electrónica
Administrador de SDocE	2	Obtener el respaldo del archivo de la estructura del directorio de archivos.
Administrador de SDocE	3	Instalar Windows 7
Administrador de SDocE	4	Instalar Framework 4.0
Administrador de SDocE	5	Instalar software de facturación electrónica
Administrador de SDocE	6	Configurar software de facturación electrónica
Administrador de SDocE	7	Creación de la lista de control de acceso – acl
Administrador de SDocE	8	Configuración de parámetros del paquete smtp_out_serverd
Administrador de SDocE	9	Definición de parámetros en Slego
<b>Sugerencias:</b> Para las actividades descritas remitirse al manual de instalación y configuración de facturación electrónica.		

#### **5. ANEXOS**

- Manual de instalación y configuración de facturación electrónica.

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-007</b>
	<b>Restauración del Modelo de Notas de Pedido para la Web</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

## **1. OBJETIVO**

Proporcionar una guía de restauración en caso de que el modelo de notas de pedido deje de funcionar.

## **2. DEFINICIÓN Y ABREVIATURAS**

**Archivo de configuración:** Es un archivo .txt el cual contiene todos los parámetros para que funcione el software.

**Directorio de archivos:** Es un archivo común al cual se le asignado una estructura particular.

## **3. RESPONSABLES**

### **3.1 POLÍTICAS**

- Se procederá aplicar este plan de contingencia cuando:
- **HARDWARE:** En caso de que el equipo sufra un daño irreversible físicamente y por lo cual se proceda a cambiarlo total o parcialmente (disco duro) por lo cual se requiere volver a instalar.
- **SOFTWARE:** En caso de que el equipo sufra un daño irreversible lógicamente y por lo cual se requiera formatear el disco.

### **3.2 CONTROLES**

- Verificación del funcionamiento del equipo habilitado.

#### **3.2.1 DOCUMENTOS DE ENTRADA**


- Resaldos de archivo de configuración
- Resaldos de estructura de directorio de archivos.

#### **3.2.2 DOCUMENTOS DE SALIDA**

- Acta de configuración del equipo

## **4. PARAMETROS**

- Clave


	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-007</b>
	<b>Restauración del Modelo de Notas de Pedido para la Web</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

## 5. DESARROLLO DE ACTIVIDADES


### 5.1 habilitar el sistema de notas de pedido

Responsable	No.	Actividades si el equipo de notas de pedido se encuentra configurado (equipo de contingencia)
Administrador de Pedidos en la Web	1.	Ubicar el equipo de contingencia de notas de pedido en el rack de servidores.
Administrador de Pedidos en la Web	2.	Verificación de IP del equipo.
Administrador de Pedidos en la Web	3.	Verificación de nombre de equipo.
Administrador de Pedidos en la Web	4.	Verificación de la configuración del IIS 7.5
Administrador de Pedidos en la Web	5.	Verificación de la conexión a la base de datos Oracle por el Net Manager.
Administrador de Pedidos en la Web	6.	Verificación de la configuración del web config
Administrador de Pedidos en la Web	7.	Subir el respaldo de la aplicación de notas de pedido a la carpeta del sistema "Notas de Pedido" en un directorio seguro para la publicación web IIS, se puede utilizar la carpeta predefinida %windir%:\inetpub\wwwroot (%windir% partición donde se aloja el S.O.)
Administrador de Pedidos en la Web	8.	Realizar pruebas de funcionamiento con al menos 100 conexiones externas.
Administrador de Pedidos en la Web	9.	Puesta en marcha del equipo de contingencia de notas de pedido

**Sugerencia:** Para las actividades descritas remitirse al manual de contingencia de notas de pedido.

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-007</b>
	<b>Restauración del Modelo de Notas de Pedido para la Web</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

<b>Responsable</b>	<b>No.</b>	<b>Actividades si el equipo de notas de pedido no se encuentra configurado (nuevo hardware)</b>
Administrador de Pedidos en la Web	1.	Ubicar el equipo asignado para notas de pedido en el rack de servidores.
Administrador de Pedidos en la Web	2.	Instalación del sistema operativo Windows XP, 2003 Server, Win 7, 2008 Server o versiones superiores
Administrador de Pedidos en la Web	3.	Asignación de IP del equipo.
Administrador de Pedidos en la Web	4.	Asignación de nombre de equipo.
Administrador de Pedidos en la Web	5.	Asignación de la configuración del IIS 7.5
Administrador de Pedidos en la Web	6.	Instalación del oracle client 11.2.3
Administrador de Pedidos en la Web	7.	Instalación el Oracle NetConector 11.2.3
Administrador de Pedidos en la Web	8.	Copiar la carpeta del sistema "NotasdePedido" en un directorio seguro para la publicación web IIS, se puede utilizar la carpeta predefinida %windir%\inetpub\wwwroot (%windir% partición donde se aloja el S.O.)
Administrador de Pedidos en la Web	9.	Editar el archivo conexion.xml que se encuentra dentro de la carpeta del sistema Notas de Pedido y editar la cadena de conexión para conectar el sistema con la base de datos que se va a utilizar.
Administrador de Pedidos en la Web	10.	Dependiendo del S.O. instalado se debe de ir a la pantalla de Administración de IIS, para poder crear un nuevo directorio virtual que haga referencia a la carpeta Notas de Pedido
Administrador de Pedidos en la Web	11.	Realizar pruebas de funcionamiento con al menos 100 conexiones externas.

	<b>PLAN DE CONTINGENCIAS</b>	<b>PCTI-007</b>
	<b>Restauración del Modelo de Notas de Pedido para la Web</b>	Fecha: 15/05/2014 Versión: 01
Revisado por: Juan Diego León		Aprobado por: Gioconda Moya

Administrador de Pedidos en la Web	12.	Puesta en marcha del equipo de notas de pedido.
<b>Sugerencias:</b> Para las actividades descritas remitirse al manual de instalación y configuración de notas de pedido		

## 6. ANEXOS

- Manual de instalación y configuración de notas de pedido

#### 4.4 Bitácoras de Control

En la tabla 3 y 4 se muestran las bitácoras para el registro y control de los respaldos y recuperación diaria de la base de datos y del usuario PRD.

**Tabla 3.**  
*Bitácora de Registro de Control de Respaldo Diarios*

BITACORA No. 1										
<b>TEMA:</b>		REGISTRO DE CONTROL DE RESPALDO DIARIO								
<b>Cargo:</b>		Administrador de Slego ERP								
<b>Responsable:</b>		Ing. Cristian Cobo								
Fecha	Responsable	Nombre del Archivo	Tamaño del Archivo	Hora del Respaldo	Directorio	Disco Externo	Tamaño del Disco	Disponible	Firma del Responsable	ESTADO
										SOLICITADO/ PROCESADO



**Tabla 4.**  
*Bitácora de Registro de Control de Recuperación*

BITACORA No. 2										
<b>TEMA:</b>		REGISTRO DE CONTROL DE RECUPERACION								
<b>Cargo:</b>		Administrador de Slego ERP								
<b>Responsable:</b>		Ing. Cristian Cobo								
Fecha	Responsable	Nombre del Archivo	Tamaño del Archivo	Hora del Respaldo	Directorio	Disco Externo	Tamaño del Disco	Disponible	Firma del Responsable	ESTADO
										SOLICITADO/ PROCESADO



En la tabla 5 se muestra un modelo de bitácoras para los cambios solicitados del usuario administrador de Slego ERP.

**Tabla 5.**  
**Bitácora de Registro de Control de Cambios**

**BITACORA No. 3**

**TEMA:** REGISTRO DE CONTROL DE CAMBIOS EN SLEGO



**Cargo:** Administrador de Slego ERP

**Responsable:** Ing. Cristian Cobo

Ticked ID	Fecha Solicitud	Solicitado por	Descripción	Módulo	Tipo	Nombre del objeto	Prioridad del cambio	Asignado a:	Estado	Procesado por	Fecha de proceso	Solución
				VENTAS	PANTALLA/ REPORTE/ DATOS/ PROCESO	RHH430203	ALTO / MEDIO / BAJO		SOLICITADO/ EN PROCESO PROCESADO/ CERRADO/ DE BAJA			



## 4.5 Responsables

A continuación en la tabla 6 se muestra la información necesaria del recurso humano responsable para la prueba y ejecución del plan de contingencias.

**Tabla 6.**  
**Matriz de Responsables de Plan de Contingencias**

Responsables Plan de Contingencias									
No.	Agencia	Nombre del Recurso	Cargo	Ciudad	Dirección de correo	Dirección del Domicilio	Teléfonos de Contacto Casa	Telefono Celular Personal	Telefono Celular Oficina
1	Matriz-Pachanlica	Ing. Patricio Acosta	Vicepresidente Financiero	Ambato	<a href="mailto:patricio.acosta@tadec.com.ec">patricio.acosta@tadec.com.ec</a>	Av. Atahualpa y Victor Hugo casa#21	3 2419129	0987842834	0987842754
2	Matriz-Pachanlica	Ing. Belén Armas	Contador Geeneral	Ambato	<a href="mailto:belen.armas@tadec.com.ec">belen.armas@tadec.com.ec</a>	Machangara y Jácome Clavijo	3 2854678	0992668186	0999232351
2	Matriz-Pachanlica	Ing. Juan Diego León	Director de GTI	Ambato	<a href="mailto:juan.leon@tadec.com.ec">juan.leon@tadec.com.ec</a>	Urbanización la Rioja casa #93 / frente al ex	3 2436425	0985888934	0985888436
2	Matriz-Pachanlica	Ing. Cristian Cobo	Administrador de Slego ERP	Ambato	<a href="mailto:christian.cobo@tadec.com.ec">christian.cobo@tadec.com.ec</a>	Urbanización la Rioja casa #93 / frente al ex	3 2436425	0985888934	0985888436
2	Matriz-Pachanlica	Ing. Henry Flores	Administrador de Infraestructura	Ambato	<a href="mailto:henry.flores@tadec.com.ec">henry.flores@tadec.com.ec</a>	Antonio Clavijo y Ernesto Minio casa #10	3 2829787	0984187060	0984187199
	S-INNOVATE C	Ing. Gioconda Moya	Consultor Externo S-INNOVATEC	Ambato	<a href="mailto:gmoiva@s-innovatec.com">gmoiva@s-innovatec.com</a>	Urbanización la Rioja casa #91 / frente al ex	3 2436425	0999232358	0995039273
	S-INNOVATE C	Ing. Daniel Noroña	Consultor Externo S-INNOVATEC	Ambato	<a href="mailto:dnorona@s-innovatec.com">dnorona@s-innovatec.com</a>	Av. Indoamérica Km a41/2	3 2436425	0999232358	0995039273

## 4.6 Recursos

### Recurso Humano

El recurso humano responsable para la prueba y ejecución del plan de contingencias se muestra en la tabla 6.

### Recursos de Infraestructura

Ver anexos:

Anexo 1. Diagrama de Red – Enlaces

Anexo 2. Diagrama de Red PIA


Anexo 3. Hardware – Servidores

#### **4.7 Períodos Plazos de Prueba**

De acuerdo con la planificación realizada con el comité de la organización para la dar seguimiento y control al plan de contingencia se ha establecido que se valide dos veces en el año de la siguiente manera: la última semana del mes de abril y la última semana del mes de Septiembre con el fin de actualizar el plan de contingencias cada vez que existan cambios o en caso de que los resultados no sean los esperados.

#### 4.8 Cronograma de Actividades para la Ejecución del Plan

Tabla 7.  
Cronograma de Ejecución del Plan de Contingencias

CRONOGRAMA DE EJECUCION DEL PLAN DE CONTINGENCIAS								
Fecha:								
Coordinador por : Ing. Patricio Acosta								
No.	ACTIVIDADES	INDICAD ORES	Nombre del Responsable	FECHAS CUMPLIMIENTO		Tiempo Estimad o min	Firma de Responsab le	Check del proceso
				Hora de Inicio	Hora Fin.			
1	Concentrar a los responsables de la ejecución del plan de contingencias		Ing. Patricio Acosta			1,00		
2	Habilitar servidor de contingencia para SLEGO ERP		Ing. Henry Flores			1,00		
3	Encender el servidor de contingencia		Ing. Henry Flores			1,00		
4	Verificar el funcionamiento del equipo con el Sistema Operativo Oracle Linux 6.5 en servidor Dell PowerEdge R720 con IP 192.168.1.4		Ing. Henry Flores			1,00		

CONTINÚA 

5	Verificar que el listener y la consola se encuentren los servicios arriba.	Ing. Cristian Cobo	1,00
6	Verificar el tamaño de los tablespaces (SLNFX, SLNFO)	Ing. Cristian Cobo	1,00
7	Importación de base de datos PRD	Ing. Cristian Cobo	15,00
8	Subir seguridades	Ing. Cristian Cobo	15,00
9	Verificar la conexión con el usuario PRD a la base de datos	Ing. Juan Diego León / Ing. Belén Armas	1,00
10	Verificar que las colas de impresión se encuentren habilitadas	Ing. Henry Flores	5,00
11	Verificar que los servicios de Forms, Reports y el Gestionador de Reportes se encuentren disponibles	Ing. Cristian Cobo	5,00
12	Verificar que el Servidor de SDocE se encuentre disponible	Ing. Henry Flores	1,00
13	Pruebas de funcionamiento nuevo servidor	Ing. Juan Diego León	5,00
14	Conexión de usuarios a Slego ERP	Ing. Juan Diego León / Ing. Belén Armas / Usuarios	2,00

CONTINÚA



15	Verificación de datos a través de los reportes más utilizados como: Balance General, Balance de Resultados, Estados de Cuenta de todos los módulos.	Ing. Juan Diego León / Ing. Belén Armas	5
16	Generación de Documentos a diferentes destinos, RTF, PDF, TXT, XML, SpreadSheat	Ing. Juan Diego León / Ing. Belén Armas / Usuarios	5
17	Verificación del servidor de notas de pedido a través de la Web	Ing. Juan Diego León	2
18	Conexión de al menos uno o dos de los distribuidores con claves genéricas	Ing. Juan Diego León	5
19	Comunicación a todos los usuarios internos y externos del uso del sistema		5
<b>Total tiempo estimado en minutos</b>			<b>77</b>

**Firmas de Responsabilidad**

#### **4.9 Conclusiones de la Propuesta**

Se desarrollaron siete procedimientos (PECS) de acuerdo a los procesos críticos identificados en la Matriz de Riesgo, utilizando metodología ISO 9001:2000.

Con respecto a los responsables de la ejecución del plan de contingencia se formó el Comité de Sistemas y Seguridad, el Comité de Ejecución del Plan y el Comité de Control del plan de contingencias con funciones y responsabilidades.

Se elaboró una matriz con los responsables plan de contingencias con toda la información necesaria para su localización como es: direcciones domiciliarias, teléfonos de la compañía y personal, dirección de correo y lugar de residencia.

Se diseñaron bitácoras para el registro de control de respaldo diario, registro de validación y recuperación del usuario PRD y registro del control de cambios en Slego solicitados por los usuarios.

#### **4.10 Recomendaciones de la Propuesta**

Dar cumplimiento, seguimiento y actualización a los a los PECS para garantizar que sus contenidos realicen la tarea para lo cual fueron creados.

Socializar el contenido del presente plan de contingencias con la finalidad de instruir adecuadamente al personal de la empresa.

Adicionalmente al plan de contingencias se deben desarrollar reglas de control y pruebas para verificar la efectividad de las acciones en caso de la ocurrencia y de esta forma tener la seguridad de que se cuenta con un método efectivo para la recuperación de Slego ERP.

## BIBLIOGRAFÍA

- Repositorio Digital Universidad Politécnica Salesiana. (s.f.). *Realización de matrices de riesgo*. Obtenido de [http://dspace.ups.edu.ec/bitstream/123456789/982/4/Capitulo\\_3.pdf](http://dspace.ups.edu.ec/bitstream/123456789/982/4/Capitulo_3.pdf)
- Academia Latinoamericana de Seguridad Informática . (2000). Seguridad Informática.
- Aiteco Consultores. (2013). *El ciclo PDCA de Mejora Continua*. Obtenido de <http://www.aiteco.com/ciclo-pdca-de-mejora-continua/>
- Alegsa, L. (s.f.). *Diccionario de Informática*. Obtenido de <http://www.alegsa.com.ar/Dic/validacion%20de%20datos.php>
- Amendolia , D., & Cendagorta, J. (s.f.). *Políticas de Seguridad Informática*. Obtenido de <http://www.slideshare.net/bellaroagui/politicas-deseguridad-13610538>
- Baldeón Garzón, M., & Coronel Guerrero, C. (s.f.). *Plan maestro de seguridad informática*. Obtenido de <http://repositorio.espe.edu.ec/bitstream/21000/6026/1/AC-GS-ESPE-034491.pdf>
- Biblioteca Juridica Virtual. (s.f.). *Riesgos Informáticos*. Obtenido de <http://biblio.juridicas.unam.mx/libros/2/909/5.pdf>
- BuenasTareas.com. (s.f.). *Implantación*. Obtenido de <http://www.buenastareas.com/ensayos/Logica/7412997.html>
- Cauqueva, J. R. (2007). *Guía de elaboración de diagnósticos*. Obtenido de <http://www.cauqueva.org.ar/archivos/gu%C3%ADa-de-diagn%C3%B3stico.pdf>
- Chimbopatinm. (2009). *slideshare: Definicion de WEBLOG*. Obtenido de <http://www.slideshare.net/chimbopatinm/bitacora-1696113>
- Concept up technology. (s.f.). *Implementación informática*. Obtenido de <http://www.conceptup.com/es/consultoria-informatica.php?x=Consultor%EDa+Hardware&y=Implementaci%F3n%20inform%Etica>
- Contec IT Services. (s.f.). *Servicios>Plan de Contingencia*. Obtenido de <http://contec-itservices.com/servicios/plan-de-contingencia.php>
- Dangel, A. D. (s.f.). *Capítulo 2: Sistemas de Información*. Obtenido de <http://www.econlink.com.ar/sistemas-informacion/definicion>

- elegirERP. (s.f.). *Definición de ERP*. Obtenido de <http://www.elegirerp.com/ERP-Definicion.php>
- EPM Microdata Ltda. (s.f.). *Planes de Contingencias*. Obtenido de <http://epmmicrodata.com/web1/index.php/servicios/plan-contingencia>
- Escuela Técnica Superior de Ingeniería Informática. (2012). *Blog sobre Historia de la Informática*. Obtenido de <http://histinf.blogs.upv.es/2012/12/18/el-efecto-2000/>
- Gaspar Martínez, J. (2004). *Planes de Contingencia - La continuidad del negocio en las organizaciones*. Madrid: Ediciones Díaz de Santos, S.A. Obtenido de *La continuidad del negocio en las organizaciones*.
- González Seco, J. A. (s.f.). *Eventos*. Obtenido de <http://www.devjoker.com/contenidos/articulos/160/Eventos.aspx>
- González, M. (s.f.). *Costos estimados*. Obtenido de <http://www.gerencie.com/costos-estimados.html>
- Gordillo, E. (s.f.). *Riesgos informáticos*. Obtenido de <http://www.calameo.com/books/00292630810462d5f8c15>
- Informatica Moderna. (s.f.). *Respaldo de información - Backup*. Obtenido de <http://www.informaticamoderna.com/Backup.htm>
- Instituto del Mar del Perú IMARPE. (2012). *Plan de Contingencia Informático 2012-2015*. Obtenido de [http://www.imarpe.pe/imarpe/archivos/informes/imarpe\\_resol\\_de\\_158\\_2012\\_conting.pdf](http://www.imarpe.pe/imarpe/archivos/informes/imarpe_resol_de_158_2012_conting.pdf)
- Libertad Digital INTERNET. (s.f.). *El efecto 2000 diez años después*. Obtenido de <http://www.libertaddigital.com/internet/el-efecto-2000-diez-anos-despues-1276380327/>
- Massella Rivas, F., Maldonado Rivera, J., Ortíz Castro, L., Bardales Duarte, R., & Massella Rivas, V. (1999). *Planes de Contingencia*. Obtenido de <http://www.tesis.ufm.edu.gt/pdf/2742.pdf>
- Meltom Technologies. (s.f.). *Tecnología de Información*. Obtenido de *Tecnología de Información*
- Microsoft. (2013). *Crear y definir un plan de pruebas*. Obtenido de [http://msdn.microsoft.com/es-es/library/dd286583\(v=vs.110\).aspx](http://msdn.microsoft.com/es-es/library/dd286583(v=vs.110).aspx)
- Mimi Economía. (s.f.). *Recursos*. Obtenido de <http://es.mimi.hu/economia/recurso.html>
- Módulo Security Solutions S. A. (2000). *Encuesta sobre amenazas más frecuentes en Brasil*.



- N, E. (2012). *Business Continuity Plan*. Obtenido de <http://www.workplaza.es/>
- Osorio Osorio, M. (2013). *Riesgos Informáticos*. Obtenido de <http://www.calameo.com/books/00295160564197287a9c6>
- Pinto Molina, M. (2009). *Busqueda y Recuperación de Información*. Obtenido de [http://www.mariapinto.es/e-coms/recu\\_infor.htm#ri11SALVADOR](http://www.mariapinto.es/e-coms/recu_infor.htm#ri11SALVADOR)  
OLIVÁN
- Posada, M. A. (2010). *BUSINESS CONTINUITY MANAGEMENT (BCM)*.  
Obtenido de <http://auditoriauc20102miju02.wikispaces.com/file/view/BCM201021700521854.pdf>
- SolucionesenTI. (s.f.). *Dirección Estratégica de las Tecnologías de la Información y la Comunicación*. Obtenido de <http://solucionesenti.wordpress.com/tag/recuperacion-de-desastres/>
- Trelles Araujo , P. (Febrero de 2010). *Seguridad Informática*. Obtenido de <http://www.slideshare.net/Tcherino/seguridad-informatica-3143924>

## SIGLAS

**B2B** son las siglas de Business-to-business, Negocio entre Empresas. Es la transmisión de información referente a transacciones comerciales electrónicamente, normalmente utilizando tecnología como la Electronic Data Interchange (EDI), presentada a finales de los años 1970 para enviar electrónicamente documentos tales como pedidos de compra o facturas.

**B2C** es la abreviatura de la expresión Business-to-Consumer, Del Negocio al Consumidor. Se refiere a la estrategia que desarrollan las empresas comerciales para llegar directamente al cliente o consumidor final.

**BCE** Banco Central Europeo, es el Banco Central de la Unión Europea, la administración encargada de manejar la política monetaria de los 17 estados miembros de la Eurozona.

**BD** Abreviatura de Data Base, Base de Datos. Es una colección de datos estructurada y organizada para permitir el rápido acceso a la información de interés. Los elementos que la forman se denominan registros, los cuales, a su vez, están compuestos por campos. Las bases de datos pueden relacionarse entre sí para realizar búsquedas o informes complejos. La información se guarda en bibliotecas de datos, y lo más importante de una base de datos es la manera en que posibilita la recuperación de información y las operaciones con ella.

**BPM** significa Buenas Prácticas de Manufactura. Son una herramienta básica para la obtención de productos seguros para el consumo humano, que se centralizan en la higiene y forma de manipulación.

**CRM** de la sigla del término en inglés Customer Relationship Management. La administración basada en la relación con los clientes. Es un modelo de gestión de toda la organización, basada en la orientación al cliente u orientación al mercado según otros autores, el concepto más cercano es marketing relacional según se usa en España y tiene mucha

relación con otros conceptos como: cliente, marketing 1x1, marketing directo de base de datos, etcétera.

**DBA** de la sigla del término en inglés Data Base Administrator. Nombre que recibe el administrador de la base de datos.

**EDI** son las siglas de Electronic Data Interchange, Intercambio Electrónico de Datos. El sistema EDI permite el intercambio, envío y recepción, de documentos comerciales por vía telemática, albaranes, facturas, órdenes de compra y otros documentos comerciales electrónicos pueden tramitarse directamente desde el ordenador de la empresa emisora al de la empresa receptora, con gran ahorro de tiempo y evitando muchos errores, propios de la comunicación tradicional en papel.

**EDIFACT** es un estándar de la Organización de las Naciones Unidas para el intercambio de documentos comerciales en el ámbito mundial. Existiendo subestándares para cada entorno de negocio (distribución, automoción, transporte, aduanero, etc.) o para cada país. Así, por ejemplo, AECOC regula el estándar EDI del sector de distribución. Para el intercambio de este tipo de información se suelen utilizar las redes de valor añadido. Además del intercambio de la información, estas redes permiten su registro.

**EOQ** Cantidad Económica de Pedido conocida en inglés como Economic Order Quantity. Es el modelo fundamental para el control de inventarios. Es un método que, tomando en cuenta la demanda determinística de un producto, es decir, una demanda conocida y constante, el costo de mantener el inventario, y el costo de ordenar un pedido, produce como salida la cantidad óptima de unidades a pedir para minimizar costos por mantenimiento del producto. El principio del EOQ es simple, y se basa en encontrar el punto en el que los costos por ordenar un producto y los costos por mantenerlo en inventario son iguales.

**ERP** Los sistemas de Planificación de Recursos Empresariales, o ERP por sus siglas en inglés, Enterprise Resource Planning. Son 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 en la producción de bienes o servicios.

**FI** Gestión Financiera describe la herramienta básica del sistema para registrar la información económica de la compañía.

**HR** Human Resources, en español Recursos Humanos. Este módulo apoya la gestión del área de recursos humanos; inclusive, se puede realizar la gestión de turnos, horarios de fábrica, gestión de candidatos, calendarios de fábrica, etc.

**IT** Son las siglas de Information Technology, significa Tecnología de la Información. El conjunto de procesos y productos derivados de las nuevas herramientas. hardware y software, soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión digitalizados de la información.

**ITIL** Information Technology Infrastructure Library en español Biblioteca de Infraestructura de Tecnologías de Información. Es un conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general. ITIL da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

**IVA** Impuesto al Valor Agregado. Grava al valor de la transferencia de dominio o a la importación de bienes muebles de naturaleza corporal, en todas sus etapas de comercialización, así como a los derechos de autor, de propiedad industrial y derechos conexos; y al valor de los servicios prestados. Existen básicamente dos tarifas para este impuesto que son 12% y tarifa 0%.

**MBA3** Master Business Administrator ERP, en español Software administrativo ERP dirigido a la mediana y grande empresa, con requerimiento desde 20 a 500 usuarios.

**MRP** Material Requirements Planning, en español Planificación de Necesidades de Materiales. Es un sistema de planificación de la producción y de gestión de stocks.

**ODBC** Open Data Base Connectivity. Es un estándar de acceso a las bases de datos desarrollado por SQL Access Group en 1992. El objetivo de ODBC es hacer posible el acceder a cualquier dato desde cualquier aplicación, sin importar qué sistema de gestión de bases de datos (DBMS) almacene los datos.

**PYME** Abreviatura que significa Pequeña y Mediana Empresa, habitualmente son inferiores a 250 trabajadores.

**SCM** La administración de redes de suministro, en inglés Supply Chain Management. Es el proceso de planificación, puesta en ejecución y control de las operaciones de la red de suministro con el propósito de satisfacer las necesidades del cliente con tanta eficacia como sea posible. La gerencia de la cadena de suministro atraviesa todo el movimiento y almacenaje de materias primas, el correspondiente inventario que resulta del proceso, y las mercancías acabadas desde el punto de origen al punto de consumo. La correcta administración de la cadena de suministro debe considerar todos los acontecimientos y factores posibles que puedan causar una interrupción.

**SRI** significa Servicio de Rentas Internas. Es una entidad técnica y autónoma que tiene la responsabilidad de recaudar los tributos internos establecidos por ley mediante la aplicación de la normativa vigente. Su finalidad es la de consolidar la cultura tributaria en el país a efectos de incrementar sostenidamente el cumplimiento voluntario de las obligaciones tributarias por parte de los contribuyentes.

# ANEXOS

Anexo 1: Diagrama de Red – Enlaces

Anexo 2: Diagrama de Red PIA

Anexo 3: Hardware – Servidores

Anexo 4: Manual BI Ventas

Anexo 5: Manual Facturación Electrónica

Anexo 6: Manual Instalación Microstrategy

Anexo 7: Manual Usuario Notas Pedido