ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

IV PROMOCIÓN

TESIS DE GRADO MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

TEMA: "DESARROLLO DE UN PLAN DE RECUPERACIÓN DE DESASTRES PARA LA UNIDAD DE TECNOLOGÍA DE LA EPMAPAP"

AUTOR: ING. LOOR ZAMBRANO JOSÉ LUIS

DIRECTOR: ING. MSc. MONTENEGRO ARMAS CARLOS ESTALESMIT

SANGOLQUÍ, JUNIO DEL 2014

UNIVERSIDAD DE LAS FUERZAS ARMADAS

ESPE

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

CERTIFICADO

Ing. Carlos Estalesmit Montenegro Armas MSc.
Ing. Rubén Darío Arroyo Chango MSc.

CERTIFICAN

Que el trabajo titulado DESARROLLO DE UN PLAN DE RECUPERACIÓN DE DESASTRES PARA LA UNIDAD DE TECNOLOGÍA DE LA EPMAPAP realizado por Ing. José Luis Loor Zambrano, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas de la Universidad de las Fuerzas Armadas-ESPE.

Debido a que constituye un trabajo que aporta de forma positiva a la gestión que se realiza en la EPMAPAP, contribuyendo a la mejora continua de los servicios que se ofrecen a la ciudadanía, motivo por el cual si recomendamos su publicación.

El mencionado trabajo consta de un documento empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan a José Luis Loor Zambrano que lo entregue a Cnel. Fidel Castro, en su calidad de Director de la Carrera.

Sangolquí, 12 de junio de 2014

Ing. Carlos Montenegro Armas MSc.	Ing. Rubén Darío Arroyo Chango MSc.
DIRECTOR	CODIRECTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

DECLARATORIA DE RESPONSABILIDAD

JOSE LUIS LOOR ZAMBRANO

DECLARO QUE:

El trabajo de investigación denominado "DESARROLLO DE UN PLAN DE RECUPERACIÓN DE DESASTRES PARA LA UNIDAD DE TECNOLOGÍA DE LA EPMAPAP", ha sido desarrollado respetando derechos intelectuales de terceros, conforme las citas cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

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

Sangolquí, junio 2014.

_____

Ing. José Luis Loor Zambrano
AUTOR

UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

AUTORIZACION

Yo, José Luis Loor Zambrano

Autorizo a la Universidad de las Fuerzas Armadas – ESPE la publicación, en la biblioteca virtual de la Institución del trabajo "DESARROLLO DE UN PLAN DE RECUPERACIÓN DE DESASTRES PARA LA UNIDAD DE TECNOLOGÍA DE LA EPMAPAP", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, junio 2014.

_____

Ing. José Luis Loor Zambrano
AUTOR

AGRADECIMIENTO

Porque más allá de la protocolaria expresión de una cortesía, me cumple dar expresamente y con profunda sinceridad las gracias a quienes tanto han ayudado a la feliz culminación de este trabajo.

Mi agradecimiento imperecedero a DIOS por permitirme finalizar y superar esta etapa de mi vida de la mejor manera posible, permitiéndome crecer como ser humano y también como profesional.

A mi familia directa e indirecta por el apoyo brindado y por demostrarme en todo momento el interés porque este trabajo diera la satisfacción esperada.

A la Universidad de las Fuerzas Armadas, y en especial a los catedráticos y catedráticas de la Facultad de Posgrado quienes aportaron con conocimientos y moldearon mi perfil profesional.

A mi director de tesis Ing. Carlos Estalesmit Montenegro Armas y los docentes miembros del tribunal Ing. Mario Ron Egas e Ing. Rubén Darío Arroyo, por sus valiosas aportaciones y sugerencias en el trabajo realizado.

José Luis Loor Zambrano

DEDICATORIA

Una persona triunfadora no debe su éxito a la suerte, sino al entusiasmo, dedicación, esfuerzo y al trabajo constante. Este trabajo quiero dedicarlo:

A DIOS el hacedor de todas las cosas por la gran oportunidad que me ha concedido al vivir.

A mi HIJO que está por nacer, quien es la muestra más clara del amor puro y sincero, él con su ternura es sin duda alguna mi mayor fuente de motivación.

A mi esposa KARLA MARÍA INTRIAGO ZAMBRANO, que con su amor me impulsó a seguir adelante y me apoyó para alcanzar una de las metas más importantes de mi vida.

A mis padres JOSÉ y FRANCISCA, por su contribución en mi formación humana y académica. Ellos han sido ejemplo de perseverancia, sencillez y humildad.

A mis hermanas y a toda mi familia política de la que siempre recibí apoyo incondicional y supieron acogerme entre ellos.

A todas aquellas personas que de una u otra forma contribuyeron a la feliz culminación de este trabajo, mi profunda admiración y respeto.

José Luis Loor Zambrano

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURAS

PRÓLOGO

El presente trabajo investigativo se basa en el desarrollo de un DRP para la Unidad de Tecnología de la EPMAPAP a fin de que pueda ser acogido por esta organización para asegurar la continuidad de los procesos tecnológicos que sostienen las actividades comerciales y de servicio de esta organización.

La investigación ha sido estructurada en seis capítulos:

En el capítulo I, se analizan los antecedentes investigativos planteando el tema y problema a investigar, se formula el problema, se justifica y se detalla la importancia del mismo, se plantea el objetivo general y los objetivos específicos.

En el capítulo II, se analizan los antecedentes investigativos, llegando a establecer la fundamentación filosófica de varios autores sobre el tema tratado, así mismo dicho capítulo está sustentado a través del marco conceptual con la definición de términos básicos que respaldan el desarrollo de la investigación y el planteamiento de los objetivos; se da una breve descripción del estado del arte y termina con una descripción del enfoque de la investigación.

El capítulo III, plantea la normativa y estándares a aplicar, definiendo mediante los criterios de selección el estándar que más se ajusta al presente trabajo investigativo, así como la normativa legal expedida a la que están sujetas las entidades públicas, como en el caso de la organización en estudio.

En el capítulo IV, se define el DRP para la Unidad de Tecnología de la EPMAPAP, describiendo primeramente la estructura orgánica de la institución y luego puntualizando el enfoque en la unidad de tecnología, los sistemas informáticos relacionados a los servicios institucionales, su diagrama de red organizacional, entrando al desarrollo del DRP basado en la norma seleccionada y realizando pruebas pilotos para su evaluación.

El capítulo V, define las factibilidades técnicas, operativas, legales y económicas del DRP desarrollado para su implementación en la unidad de tecnología de la EPMAPAP.

Finalmente en el capítulo VI, se detallan las conclusiones y recomendaciones del presente trabajo investigativo basadas en los objetivos propuestos.

RESUMEN

Esta investigación, se basa en el estudio del problema detectado en la Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo EPMAPAP, en la cual no se cuenta con planes de recuperación de desastres.

Al ser la EPMAPAP una entidad pública del estado ecuatoriano, son de cumplimiento obligatorio las disposiciones emitidas por la Contraloría General del Estado a través de sus normas de control interno 410-11 Plan de Contingencias la cual establece que: "…Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado…".

Es por esta razón la propuesta de diseño de un DRP basado en la norma ISO 22301:2012 que permita enfrentar desastres que puedan provocar discontinuidad en las operaciones que presta la Unidad de Tecnología de la EPMAPAP.

El estudio de factibilidad, así como las pruebas preliminares demuestran que el DRP desarrollado puede implementarse y operarse.

Palabras Claves: Plan de recuperación de desastres, Sistema de Gestión de la Continuidad del Negocio, ISO 22031, BS25999, Plan de contingencia.

ABSTRACT

This research is based on the study of the problem identified in the Municipal Public Company for Water and Wastewater Portoviejo EPMAPAP, in which there is no disaster recovery plans.

As the EPMAPAP a public entity of the Ecuadorian state, are binding provisions issued by the Comptroller General of the State through its internal control standards 410-11 Plan Contingency states: "…It is for the information technology unit the definition, adoption and implementation of a contingency plan detailing the actions to take in case of an emergency or suspension in the processing of information by equipment problems, or related personnel programs…".

For this reason the proposed design of a DRP based on the ISO 22301:2012 standard, allowing face disasters that may cause disruption of the operations provided by the Technology Unit EPMAPAP.

The feasibility study and preliminary tests show that the DRP developed can be implemented and operated.

Key words: Disaster Recovery Plan, Business Continuity Management System, ISO 22031, BS25999, Contingency plan.

CAPÍTULO I

INTRODUCCIÓN

1. Tema

"Desarrollo de un Plan de Recuperación de Desastres para la Unidad de Tecnología de la EPMAPAP"

1.1. Antecedentes

En virtud de la creciente dependencia que tienen las empresas a nivel mundial de la tecnología para realizar sus operaciones, se hace cada vez más necesario el contar con un plan de recuperación de desastres que permita estar preparados para incidentes que pudieran afectar el normal funcionamiento de la organización y la pérdida de sus datos, software o hardware. Es así que la adopción de los planes de recuperación de desastres se ha convertido en una herramienta indispensable que permite a las empresas su permanencia en el mercado en caso de disrupciones inesperadas.

En Ecuador este fenómeno se manifiesta en mayor proporción en el sector privado, que busca salvaguardar su inversión ante desastres inesperados o incidentes disruptivos que interrumpan las actividades organizacionales provocando desestabilización y hasta desaparición de las empresas.

En la provincia de Manabí muy pocas empresas cuentan con la protección de esta herramienta que les permita salvaguardar sus operaciones y datos, sin contemplar la ocurrencia de desastres inesperados que pueda significar pérdidas considerables y hasta el cierre de las organizaciones.

1.2. Planteamiento del Problema

No se dispone de un DRP para la Unidad de Tecnología de la EPMAPAP, por lo que se incumple la norma de control interno 410-11Plan de Contingencias emitida por la Contraloría General del Estado, la cual establece que:

Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado. (Contraloría General del Estado, 2009)

1.3. Alcance

El Plan de Recuperación de Desastres se desarrolló para sustentar las operaciones de los principales servicios ofrecidos por la Unidad de Servicios Informáticos de la EPMAPAP.

Dada la recurrencia de eventos eléctricos discontinuos y de inundaciones presentadas en la ciudad a causas de fuertes inviernos cada vez más frecuentes que amenazan la seguridad de los datos, los sistemas informáticos con los que cuenta la institución, sus consecuencias en la continuidad y calidad en la prestación de estos servicios, es evidente la necesidad de tomar acciones preventivas invitando a los directivos a la adopción de medidas que mitiguen los posibles impactos generados por los fenómenos naturales o errores humanos y las consecuencias que estos puedan tener.

1.4. Justificación e Importancia

El agua es un derecho Constitucional, según lo expresa la Constitución de la República del Ecuador en su Título II Derechos, Capítulo II Derechos del Buen Vivir, Sección Primera Agua y Alimentación, Art. 12 que establece que "El derecho humano al agua es fundamental e irrenunciable. El agua constituye patrimonio nacional estratégico de uso público, inalienable, imprescriptible, inembargable y esencial para la vida". (Asamblea Nacional Constituyente, 2008)

Razón por la cual los gobiernos Municipales a través de las empresas públicas de agua potable y alcantarillado garantizan el goce de este derecho. En este principio radica la importancia de contar con sistemas informáticos integrados, que sustenten las actividades comerciales y administrativas que le permita a la EPMAPAP brindar un servicio de calidad mediante una buena gestión y un correcto manejo de la información y los recursos con los que se cuentan.

La implementación del DRP permite salvaguardar la integridad de los equipos informáticos, realizar una adecuada gestión y administración de los recursos tecnológicos en la Unidad de Servicios Informáticos de la EPMAPAP, logrando la continuidad de los servicios que brindan las aplicaciones informáticas de la institución que sustentan las operaciones comerciales y administrativas, evitando la paralización de servicios institucionales que se ofrecen a la ciudadanía.

1.5. Objetivos

1.5.1. Objetivo General

Desarrollar un DRP para la Unidad de Tecnología de la EPMAPAP sobre la base de estándares y buenas prácticas, que permita afrontar desastres y mantener la continuidad de las operaciones del negocio.

1.5.2. Objetivos Específicos

1. Seleccionar los estándares y buenas prácticas aplicables a la recuperación de desastres en la Unidad de Tecnología de la EPMAPAP.
2. Aplicar los estándares y buenas prácticas seleccionados, para definir y probar, en forma piloto, el DRP
3. Realizar un análisis de factibilidad para la implementación del DRP.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes Investigativos

Según la definición de varios autores se establece la continuidad del negocio como:

"Un proyecto estratégico de toda la organización involucrando a todos los departamentos y divisiones para que la información necesaria fluya de forma continuada en la medida de las necesidades de los responsables de llevarlo adelante. Su desarrollo, implementación y mantenimiento, propiciará a la organización beneficios, tales como: minimizar potenciales pérdidas económicas, reducir riesgos, reducir interrupciones, asegurar la estabilidad en la organización, entre otras". (Gaspar Martínez, Planes de contingencia la continuidad del negocio en las organizaciones, 2004) (p. 1)

"Un instrumento de gestión que contiene las medidas (tecnológicas y humanas y de organización) que garanticen la continuidad del negocio protegiendo al sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto" (Aguilera, 2010) (p. 23)

"Conjunto de estrategias, acciones, procedimientos planificados y responsabilidades definidas para minimizar el impacto de una interrupción imprevista de las funciones críticas y conseguir la continuidad de las operaciones del negocio". (Gaspar Martínez, El plan de continuidad de negocio Una guía práctica para su elaboración, 2010) (p. 205)

"Se cree que algunas empresas gastan hasta el 25 % de su presupuesto en proyectos de recuperación de desastre, sin embargo, esto lo hacen para evitar pérdidas más grandes. De las empresas que tenían una pérdida principal de registros automatizados el 43 % nunca vuelve a abrir, el 51 % cierra en menos de dos años, y sólo el 6 % sobrevivirá a largo plazo". (Hoffer, 2001)

Una vez analizadas estas definiciones se puede concluir que un DRP como parte de la continuidad del negocio constituye una herramienta que permite a las organizaciones estar preparadas para afrontar eventualidades que pudieran presentarse y poner en riesgo las operaciones tecnológicas y la permanencia del negocio a través del tiempo, estableciendo las acciones a tomar en cada caso y las personas responsables de ejecutarlas.

2.2. Marco Conceptual

Para el desarrollo de esta tesis se utilizaron los siguientes conceptos básicos:

Sistemas de información, son un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos, teniendo como elementos: recursos, equipo humano, información y actividades. (Aguilera, 2010) (p. 8)

Sistema informático, está constituido de un conjunto de elementos físicos (hardware, dispositivos periféricos y conexiones) lógicos (sistemas operativos, aplicaciones) y con frecuencia se incluye también los elementos humanos (personal experto que maneja el software y el hardware) Un sistema informático puede ser un subconjunto del sistema de información, pero en principio un sistema de información no tiene por qué contener elementos informáticos. (Aguilera, 2010) (p. 8)

Seguridad informática, es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de información seguro y confiable. (Aguilera, 2010) (p. 9)

Plan de contingencia, determinadas amenazas a cualquiera de los activos del sistema de información pueden poner en peligro la continuidad del negocio. El plan de contingencia es un instrumento de gestión que contiene las medidas (tecnológicas y humanas y de organización) que garanticen la continuidad del negocio protegiendo al sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto.

El plan de contingencia consta de tres subplanes independientes:

- Plan de respaldo, ante una amenaza se aplican medidas preventivas para evitar que se produzca un daño
- Plan de emergencia, Contempla qué medidas tomar cuando se está materializando una amenaza cuando acaba de producirse.
- Plan de recuperación, indica las medidas que se aplicarán cuando ha ocurrido un desastre. El objetivo es evaluar el impacto y regresar lo antes posible a un estado normal de funcionamiento de la organización y del sistema.

La elaboración del plan de contingencia no puede descuidar al personal de la organización que estará informado del plan y entrenado para actuar en las funciones que le hayan sido encomendadas en caso de producirse una amenaza o un impacto. (Aguilera, 2010) (p. 23)

Gobierno de TI, es una disciplina de trabajo, no una solución en sí misma. Está orientado a proveer las estructuras que unen los procesos de TI, recursos de TI e información con las estrategias y los objetivos de la empresa. Además, el Gobierno de TI integra e institucionaliza las mejores prácticas de planificación y organización, adquisición e implementación, entrega de servicios y soporte, y monitoriza el rendimiento de TI para asegurar que la información de la empresa y las tecnologías relacionadas soportan los objetivos del negocio. (sitio Web de Grupo Pragma Consultores)

Plan de Continuidad, permite de modo planificado, sistemático y organizado resguardar la capacidad de la empresa de proveer un nivel aceptable de servicios en la eventualidad de una falla grave, una emergencia o una contingencia que comprometa de modo significativo la continuidad de las operaciones. (sitio Web de Balarezo Consultores CIA. LTDA.)

DRP – Plan de Recuperación de Desastres, un DRP (*Disaster Recovery Plan* o Plan de recuperación de desastres) es la estrategia que se seguirá para restablecer los servicios de TI (*Hardware y Software*) después de haber sufrido una afectación por una catástrofe natural, epidemiológica, falla masiva, daño premeditado, ataque de cualquier tipo, el cual atente contra la continuidad del negocio.

Cuando las compañías no cuentan con un DRP implementado y se tiene una eventualidad, éstas lo tratan de recuperar a cualquier costo ya que dependen del funcionamiento de sus sistemas de información. (Sitio Web de inBest)

2.3. Estado del Arte

Actualmente los DRP´s se desarrollan bajo los estándares de buenas prácticas internacionales tales como: Norma Británica BS-25999 e ISO 22301:2012.

BS 25999-2.- Es una norma Británica emitida en el 2007 utilizada en muchos países como referente para gestionar la continuidad del negocio. La BS 25999-2 define cuatro fases de gestión: planificación, implementación, revisión y supervisión, además de mejora; ya que con las primeras fases se pretende que el sistema se actualice y mejore permanentemente para que sea de utilidad en caso de producirse desastres. (sitio web de EPPS *Service*s Ltd.)

Como base histórica se puede mencionar que la norma ha sido publicada en dos partes.

- BS 25999-1:2006 Parte 1: se trata de un documento orientativo que proporciona las recomendaciones prácticas para las el BCM.
- BS 25999-2:2007 Parte 2: establece los requisitos para un Sistema de Gestión de la Continuidad (BCM). Esta es la parte de la norma que se certifica a través de una etapa de implementación, de auditoría y posterior certificación.

Se detallan una lista de los principales procedimientos y documentos requeridos por la BS 25999-2:

- Alcance del SGCN: identificación precisa del área de la organización donde se aplicará la gestión de la continuidad del negocio.
- Política de GCN: definición de objetivos, responsabilidades, etc.
- Gestión de recursos humanos.
- Análisis de impactos en el negocio y evaluación de riesgos.
- Definición de estrategia de continuidad del negocio.
- Planes de continuidad del negocio.
- Mantenimiento de planes y sistemas (mejora continua).

La norma BS 25999-2 requiere los siguientes documentos:

- El alcance de GCN;
- La política de GCN;
- Responsabilidades específicas para la GCN;
- Procedimientos para gestionar documentos y registros y para medidas correctivas y preventivas;
- Metodología para el análisis de impactos en el negocio y resultados del análisis;
- Metodología de evaluación de riesgos;
- Estrategia de continuidad del negocio;

- Plan de continuidad del negocio que incluya planes de respuesta a los incidentes y planes de recuperación;
- Registros.

Norma ISO 22301:2012 Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio - Requisitos.- Es una norma Internacional para sistemas de gestión de la continuidad del negocio (SGCN), diseñada para ayudar a las organizaciones a minimizar el riesgo de interrupciones. Fue lanzada por ISO reemplazando a la actual norma británica BS 25999-2.

Esta norma específica requisitos para planificar, establecer, implantar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión documentado para prepararse, responder y recuperarse de interrupciones cuando estas ocurran, brindando la confianza de negocio a negocio y de negocio a cliente.

La norma proporciona a las organizaciones un marco que asegura que ellos pueden continuar trabajando durante las circunstancias más difíciles e inesperadas – protegiendo a sus empleados, manteniendo su reputación y proporcionando la capacidad de continuar trabajando y comercializando.

Los requisitos especificados en la ISO 22301 son de tipo genérico con el afán de ser aplicados de forma general a cualquier organización sin importar el tipo, tamaño y naturaleza.

La estandarización de la continuidad del negocio con ISO 22301 agrega:

- Mayor énfasis en el establecimiento de objetivos, seguimiento del desempeño y de los indicadores;
- Expectativas más claras sobre la dirección

- Planificación y preparación más cuidadosas de recursos para el aseguramiento de la continuidad del negocio.

Las clausulas principales de la norma ISO 22301 son:

- Clausula 4.- Contexto de la organización
- Clausula 5.- Liderazgo
- Clausula 6.- Planificación
- Clausula 7.- Soporte
- Clausula 8.- Operación
- Clausula 9.- Evaluación del desempeño
- Clausula 10.- Mejora

Un sistema de gestión de la continuidad del negocio alineado con la norma ISO 22301 se adapta y es adecuado para cualquier organización, sin importar su tamaño y en todos los sectores, tanto del sector público como privado y tanto para empresas de producción como de servicios. (ISO 22301, 2012)

2.4. Enfoque de la Investigación

En este trabajo se parte de una investigación documental que permita establecer con el nivel de detalle pertinente el estado del arte sobre la temática de los DRPs. A continuación se realizará un proceso de Síntesis para definir el DRP. Paralelamente, se emplearan como técnicas de campo la Entrevista y la Observación directa para identificar los procesos que deben ser considerados dentro del DRP. Finalmente se utilizará un Análisis que justifique la factibilidad del DRP desarrollado.

CAPITULO III
SELECCIÓN DE LA NORMATIVA Y ESTÁNDARES A APLICAR

Los estándares, normas y buenas prácticas implementadas en diversas organizaciones a nivel mundial, surgen ante la necesidad de gestionar los riesgos y estandarizar las políticas de seguridad en las organizaciones a fin de garantizar la continuidad de los productos y servicios que se ofrecen a la colectividad, a través de la correcta selección y aplicación de las normas de acuerdo a las necesidades organizacionales.

3.1. Estándares, buenas prácticas y normativas acerca de los DPR´s.

Constantemente las empresas experimentan situaciones de emergencia que necesitan respuestas inmediatas, es así que en los últimos años los estándares y buenas prácticas han sido aceptados por las organizaciones para asegurar la continuidad de sus operaciones mediante la implementación de mecanismos y/o técnicas que mitiguen los riesgos a los que están expuestas.

Ante esta situación se plantea como solución la implementación de un DRP, el cual ayude a establecer lo que se debe hacer para asegurar en todo momento la funcionalidad de los sistemas importantes dentro de la Unidad de Tecnología, y con esto la continuidad de los procesos críticos de la organización.

En adelante se encuentra una descripción y análisis de los principales estándares acogidos por las organizaciones para asegurar la continuidad de sus negocios:

3.1.1. Estándares

Los estándares son un conjunto de especificaciones técnicas o mejores prácticas, aprobadas por organismos reconocidos, aplicables a cualquier tipo de organización cuyo objetivo es la mejora continua de los procesos y su permanencia a través del tiempo.

3.1.1.1. BS-25999

Es un estándar británico de mejores prácticas, recomendaciones y actividades específicas, para lograr la continuidad de las operaciones de negocio, considerando los riesgos a los que se enfrenta la organización. Este estándar se basa en el Plan de Continuidad el Negocio o BCP por sus siglas en inglés (*Business Continuity Planning*), el mismo que al implementarlo en una organización se le debe hacer seguimiento a fin de conocer su evolución de mejora permanente en los procesos de la empresa. (Rodríguez Edith & Correa)

La publicación de esta norma fue realizada en 2 partes:

- BS 25999-1:2006 Parte 1: Se trata de un documento orientativo que proporciona las recomendaciones prácticas para el BCM.
- BS 25999-2:2007 Parte 2: Establece los requisitos para un Sistema de Gestión de la Continuidad (BCM). Esta es la parte de la norma que se certifica a través de una etapa de implementación, auditoría y posterior certificación.

A continuación se detallan los componentes de cada parte de la norma BS-25999:

3.1.1.1.1. BS 25999-1:2006 – Código de Práctica

- Gestión de Continuidad del Negocio.
- Política de Gestión de Continuidad del Negocio.
- Gestión del Programa de Continuidad del Negocio.

- Entendiendo la Organización.
- Desarrollo e Implementación de Respuestas a BCM.
- Determinando Estrategias de Continuidad del Negocio.
- Ejercitando, Manteniendo y Analizando el plan de BCM.
- Fijando el BCM en la Cultura de la Organización.

3.1.1.1.2. BS 25999-2:2007 – Especificación

- Planeación del Sistema de Gestión de BCM.
- Implementando y Operando el Sistema.
- Monitoreo y Revisión del Sistema.
- Mantenimiento y Mejora del Sistema.

3.1.1.1.2.1 Cláusulas

3.1.1.1.2.1.1 Alcance

En el alcance se deben identificar los procesos productivos que se incluirán en la gestión de continuidad del negocio. Es decir que se seleccionarán los procesos que suponen son de mayor importancia para la organización y en la cual se basa fundamentalmente su operación productiva de negocio. Dejando de lado los productos y servicios que se realicen de forma minoritaria o en menor medida, o la opción de incluir todos los productos y servicios que ofrece la organización, esta será la primera decisión que se debe tomar en la organización frente a la implementación de esta norma.

3.1.1.1.2.1.2 Términos y definiciones

BS 25999-1:2006 tiene su propia lista de términos y definiciones que pertenecen al estándar mismo y los usuarios deberían tenerlos en cuenta. Como cualquier industria, el BCM tiene su propia terminología, definiciones y siglas.

3.1.1.1.2.1.3 Planear el BCMS

La etapa de planificación incluye la definición de políticas y la asignación apropiada de recursos para la correcta implementación de los BCMS, además del desarrollo de documentación que sirva de soporte para el sistema tales como: políticas, procedimientos, etc. Asimismo esta cláusula incluye los requisitos para el control de la documentación generada y los registros asociados al sistema de gestión.

3.1.1.1.2.1.4 Implementar y operar el BCMS

Esta cláusula requiere que se entienda más a fondo la organización, ya que es el punto de partida para el desarrollo del sistema de gestión para la continuidad del negocio, este primer paso consiste en la realización de análisis de impacto en el negocio – BIA, el mismo que deberá incluir:

- Actividades críticas, las cuáles dan soporte a los procesos productivos de la organización.
- El impacto que producen la interrupción de dichas actividades.
- Establecer el período máximo tolerable de interrupción de cada actividad, que es el tiempo máximo que la organización puede soportar sin que sus productos o servicios sufran un daño grave.
- Identificar las dependencias entre actividades.
- Identificación de los acuerdos con contratistas que nos suministran servicios para las actividades críticas.
- Establecer los objetivos de tiempo de recuperación para cada actividad.

Como segundo paso se debe realizar un análisis de riesgos para evaluar la probabilidad de ocurrencia de las posibles interrupciones identificadas en el BIA. Es aquí donde se identifican las amenazas y vulnerabilidades asociadas a las actividades críticas del negocio.

Asimismo se debe definir el tratamiento que se les darán a estos riesgos identificados los cuáles pueden ser: reducir los riesgos, disminuir el tiempo de interrupción y limitar el impacto de una interrupción que afecte a los productos y servicios de la organización.

En esta etapa se debe también definir la estructura documental a implementar en caso de una interrupción real, lo cual incluye: planes de gestión de incidentes, planes de gestión de recuperación, etc.

Aquí también se desarrollan los planes de gestión de la continuidad del negocio para responder de forma eficaz en caso de una interrupción que pueda afectar el negocio.

Como en todos los casos la documentación y los procedimientos desarrollados deben ser revisados y validados periódicamente y en intervalos definidos, mediante ejercicios de autoevaluación y auditorías.

3.1.1.1.2.1.5 Monitorear y revisar el BCMS

Una vez realizada la implementación de los requisitos especificados en las cláusulas anteriores la BS 25999 requiere de una serie de actividades de seguimiento y revisión como son:

- Auditorías internas.
- Revisión por parte de la dirección.

3.1.1.1.2.1.6 Mantener y mejorar el BCMS

Finalmente esta norma propone acciones preventivas y correctivas como métodos para encaminar a la organización hacia la mejora continua del sistema de gestión de la continuidad del negocio.

A pesar de que la norma Británica no es internacional tuvo gran demanda mundial por la eficiente propuesta de sus buenas prácticas y su implementación se extendió mucho a nivel internacional, es así que como consecuencia a esta fuerte demanda que se crea la Norma Internacional ISO 22301:2012, para cubrir la necesidad actual de las empresas, de tener asegurado su negocio ante interrupciones y poder ofrecer la continuidad de las operaciones más críticas. (Bello, 2008)

3.1.1.2. ISO 22301"Seguridad de la sociedad – Sistemas de gestión de la continuidad de negocio – Requisitos".

Es la primera norma internacional para la gestión de la continuidad del negocio, desarrollada para ayudar a las organizaciones a minimizar el riesgo de las interrupciones que puedan presentarse. Esta norma reemplaza a la norma británica BS-25999.

La norma ISO 22301 especifica requisitos para planificar, establecer, implantar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión documentado para prepararse, responder y recuperarse de eventos que generan interrupciones, cuando éstos ocurren.

Los requisitos que se especifican en la norma ISO 22301 son genéricos y pueden ser aplicados a todas las organizaciones o parte de ellas, sin importar su tipo, tamaño y naturaleza, su grado de aplicación depende del ambiente operativo y de la complejidad de la organización.

La estandarización de la continuidad de negocio evoluciona con ISO 22301, agregando:

- Mayor énfasis en el establecimiento de objetivos, seguimiento del desempeño y de los indicadores;
- Expectativas más claras sobre la Dirección;
- Planificación y preparación más cuidadosas de recursos requeridos para el aseguramiento de la continuidad de negocio.

La norma ISO 22301 puede ser aplicada a todo tipo y tamaño de organizaciones que quieran:

- Establecer, implantar, mantener y mejorar un SGCN;
- Asegurar conformidad con la política establecida de la continuidad de negocio de la organización;
- Demostrar conformidad a los demás;
- Buscar certificación/registro de su SGCN por un organismo externo de certificación; o
- Realizar una autodeterminación y auto declaración de conformidad con esta norma internacional.

3.1.1.2.1. Cláusulas (ISO 22301, 2012-06-15)

3.1.1.2.1.1 Alcance

Esta norma internacional para la gestión de la continuidad del negocio especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión documentado que permita: reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de perjudiciales incidentes que puedan surgir.

Los requisitos de esta norma son genéricos ya que la misma pretende ser implementada en cualquier organización independientemente de su tamaño, tipo y naturaleza; su alcance y aplicación de estos requisitos depende del entorno operativo de la organización y su complejidad.

Esta norma no pretende proporcionar uniformidad en la estructura de un sistema de gestión de continuidad del negocio, pero pretende cubrir las necesidades de las partes interesadas de la organización, estas necesidades están determinadas por: lo legal, normativo, organizacional y requerimientos de industriales, los productos y servicios, los procesos de empleados, el tamaño y estructura de la organización y los requerimientos de las partes interesadas de la organización. (ISO 22301, 2012)

3.1.1.2.1.2 Referencias normativas

Esta norma constituye un documento indispensable para su aplicación en cualquier organización. Para las referencias sin fecha se aplica la última edición del documento referenciado (incluye cualquier modificación); para las referencias fichadas se aplica únicamente la edición citada. No existen referencias normativas. (ISO 22301, 2012)

3.1.1.2.1.3 Términos y definiciones

Para la aplicación del presente estándar se presentan los términos definiciones de los que se hablan en el documento BS 25999-2:2007 *Specifications* en su apartado "*3 Term and definitions*". (ISO 22301, 2012)

3.1.1.2.1.4 Requerimientos generales

La organización deberá definir los aspectos internos y externos que afecten su capacidad de alcanzar los objetivos especificados en su Sistema de Gestión de

Continuidad del Negocio, definir las partes interesadas que intervienen y la normativa legal y reglamentaria aplicable que se debe observar al momento de establecer, implementar y mantener su SGCN.

Es necesario también identificar los límites y aplicabilidad del SGCN, así como las partes de la organización a ser incluidos y su personal para así definir su alcance y una vez implementado mantener y mejorar continuamente conforme a los requisitos de esta norma. (ISO 22301, 2012)

3.1.1.2.1.5 Liderazgo

Esta norma se refiere mucho al liderazgo y compromiso que debe demostrar la alta gerencia y las personas que desempeñan funciones de gestión con respecto a los BCMS, además de asegurarse de proporcionar los recursos necesarios, establecer políticas y definir a las personas que implementan y mantienen el BCMS y que estas asignación de responsabilidades son debidamente comunicadas dentro de la organización. (ISO 22301, 2012)

3.1.1.2.1.6 Planeación

Requiere que la organización identifique sus riesgos para la implementación del sistema de gestión y establezca objetivos y criterios que puedan ser utilizados para medir su éxito. Es así que una vez que la organización define sus objetivos sobre la continuidad del negocio debe también desarrollar los proyectos para alcanzarlos. Estos objetivos deben estar ligados a la política de continuidad del negocio y deben ser medibles.

Al establecer estos objetivos se debe considerar el nivel mínimo de productos y servicios que la organización puede ofrecer para alcanzar sus objetivos globales de negocio. (ISO 22301, 2012)

3.1.1.2.1.7 Soporte

Dado que los recursos son necesarios para la implementación, esta cláusula introduce el importante concepto de competencia. Para tener éxito en la continuidad del negocio, se debe contar con las personas con los conocimientos, las habilidades y la experiencia adecuada, para que contribuyan al BCMS y respondan a los incidentes cuando éstos se producen.

También es importante que todo el personal esté consciente de su propio papel en la respuesta a incidentes y es lo que también se define en esta cláusula. La parte de comunicación de esta cláusula incluye las comunicaciones internas y externas que sean relevantes para la implementación y mejora continua de los BCMS.

La necesidad de comunicación relativa a los BCMS - por ejemplo, comunicar a los clientes que la organización tiene implementado un SGCN apropiado - y también se incluye aquí la preparación para comunicar un incidente después de su ocurrencia (cuando los canales normales pueden ser interrumpidos). (ISO 22301, 2012)

3.1.1.2.1.8 Operación

La organización debe planificar, ejecutar y controlar procesos para cumplir con requisitos necesarios, estableciendo criterios para los procesos y aplicando los mismos, mediante el control y la documentación de la información para asegurar la confianza de que los procesos se están cumpliendo según lo previsto. Además de controlar los cambios efectuados y revisar sus consecuencias, mitigando efectos adversos si es que los hubieran. Es necesario que la organización tenga el control de los procesos externalizados o manejados por terceros.

La organización debe realizar un análisis de impacto y evaluación de riesgos que establezca un marco de evaluación, defina criterios y evalúe el impacto potencial de

incidentes perturbadores. Adicionalmente la organización debe preocuparse de comunicar estos riesgos con los niveles de detalle suficientes y apropiados, para luego determinar las estrategias necesarias que servirán para estabilizar, reanudar y recuperar las actividades priorizadas, teniendo en cuenta los plazos priorizados para la reanudación de cada actividad determinada. (ISO 22301, 2012)

3.1.1.2.1.9 Evaluación del desempeño

La alta gerencia debe medir y evaluar todo tipo de acción o correctivo tomado en la organización, medir procesos, estado de problemas internos y externos, procesos de auditorías, oportunidades de mejora continua, necesidades de cambio, opiniones de proveedores y socios y cualquier cambio que pudiera afectar el BCMS sea este interno o externo. Estas evaluaciones deben ser planificadas a intervalos para asegurarse de su conveniencia, educación y eficacia. (ISO 22301, 2012)

3.1.1.2.1.10 Mejora

En las organizaciones siempre se observarán no conformidades que ayudarán a mejorar de forma sistemática la implementación de un BCMS, estas acciones correctivas se derivan de las auditorías, revisiones y ejercicios que significarán cambios en los BCMS en caso de ser necesarios. La organización puede utilizar los procesos de las BCMS como el liderazgo, la planificación, la evaluación y el rendimiento para lograr una mejora de las operaciones. (ISO 22301, 2012)

3.1.1.3. ISO 27001 – Tecnología de la Información – Técnicas de Seguridad – Sistema de la Seguridad de la Información (SGSI) – Requisitos.

Esta norma mediante el enfoque por procesos proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de la Seguridad de la Información (SGSI), lo cual debe ser fruto de una decisión estratégica dentro de una organización.

El diseño y la implementación del SGSI dependen de las necesidades y objetivos de cada organización, por lo que consecuentemente la implementación de un SGSI debe ajustarse a estas mismas necesidades organizacionales. (Normas BCM – Plan de Continuidad de Operaciones, 2009).

3.1.1.3.1 Cláusulas de la Norma ISO 27001 (ISO/IEC 27001-2005, 2011):

- 0 Introducción
- 1 Alcance
- 2 Referencia Normativa
- 3 Términos y definiciones
- 4 Sistema de gestión de seguridad de la información
- 5 Responsabilidad de la Dirección
- 6 Auditoría interna del SGSI
- 7 Revisión por la Dirección del SGSI
- 8 Mejora del SGSI
- Anexo A (Normativo) – Objetivos de Control y Controles
- Anexo B y C (informativos) y Bibliografía

3.1.2. Normativa

La normativa es todo el cuerpo legal que en el marco de su jurisdicción es aplicable para cada organización de acuerdo a su actividad y lugar donde desarrollan sus actividades.

3.1.2.1. Constitución de la República del Ecuador

La Constitución de la República del Ecuador establece en su Título VII Régimen Del Buen Vivir, Capítulo Primero Inclusión y Equidad, Sección Novena, Gestión del Riesgo, que:

> **Art. 389.-** El Estado protegerá a las personas, las colectividades y la naturaleza frente a los efectos negativos de los desastres de origen natural o antrópico mediante la prevención ante el riesgo, la mitigación de desastres, la recuperación y mejoramiento de las condiciones sociales, económicas y ambientales, con el objetivo de minimizar la condición de vulnerabilidad.
>
> El sistema nacional descentralizado de gestión de riesgo está compuesto por las unidades de gestión de riesgo de todas las instituciones públicas y privadas en los ámbitos local, regional y nacional. El Estado ejercerá la rectoría a través del organismo técnico establecido en la ley. Tendrá como funciones principales, entre otras:
>
> 1. Identificar los riesgos existentes y potenciales, internos y externos que afecten al territorio ecuatoriano.
> 2. Generar, democratizar el acceso y difundir información suficiente y oportuna para gestionar adecuadamente el riesgo.
> 3. Asegurar que todas las instituciones públicas y privadas incorporen obligatoriamente, y en forma transversal, la gestión de riesgo en su planificación y gestión.

4. Fortalecer en la ciudadanía y en las entidades públicas y privadas capacidades para identificar los riesgos inherentes a sus respectivos ámbitos de acción, informar sobre ellos, e incorporar acciones tendientes a reducirlos.
5. Articular las instituciones para que coordinen acciones a fin de prevenir y mitigar los riesgos, así como para enfrentarlos, recuperar y mejorar las condiciones anteriores a la ocurrencia de una emergencia o desastre.
6. Realizar y coordinar las acciones necesarias para reducir vulnerabilidad es y prevenir, mitigar, atender y recuperar eventuales efectos negativos derivados de desastres o emergencias en el territorio nacional.
7. Garantizar financiamiento suficiente y oportuno para el funcionamiento del Sistema, y coordinar la cooperación internacional dirigida a la gestión de riesgo.

Art. 390.- Los riesgos se gestionarán bajo el principio de descentralización subsidiaria, que implicará la responsabilidad directa de las instituciones dentro de su ámbito geográfico. Cuando sus capacidades para la gestión del riesgo sean insuficientes, las instancias de mayor ámbito territorial y mayor capacidad técnica y financiera brindarán el apoyo necesario con respeto a su autoridad en el territorio y sin relevarlos de su responsabilidad. (Asamblea Nacional Constituyente, 2008)

Así queda evidenciado que por mandato Constitucional las Organizaciones públicas deben gestionar los riesgos mediante la implementación de planes de continuidad del negocio para la recuperación de sus actividades en caso de interrupciones, que provoquen paralizaciones de los servicios institucionales y que afecte a las personas, las colectividades y la naturaleza.

El marco jurídico normativo del Ecuador regula dentro de sus normas la gestión que deben dar a los riesgos las Instituciones Públicas que regulan la implementación de acciones que permitan gestionar los riesgos inherentes.

3.1.2.2. Normas de Control Interno

Al ser la Contraloría General del Estado el órgano rector encargado del control de los recursos públicos para precautelar su uso efectivo, en beneficio de la sociedad, es la Institución responsable de la emisión de las normas de control interno, que son de cumplimiento obligatorio en las instituciones del Estado, siendo así que: la norma 410-11 Plan de Contingencias establece:

Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado**.** (Contraloría General del Estado, 2009)

Por lo antes expuesto se propone el Desarrollo de un Plan de recuperación ante Desastres para la Unidad de Tecnología de la EPMAPAP, que permita enfrentar interrupciones que puedan provocar discontinuidad de las operaciones informáticas de la mencionada institución.

3.2. Selección del estándar, buenas prácticas y la normativa para la definición del DRP, aplicable al presente trabajo.

Para el presente trabajo se realizó la selección de la norma que cumplió con los criterios establecidos que mejor se ajustaron a la realidad y necesidad de la Unidad de Tecnología de la EPMAPAP a fin obtener mejores resultados durante su desarrollo y en su posterior implementación para mitigar en lo posible los riesgos a los que está expuesta la organización, adoptando de mejor manera las recomendaciones sugeridas en el estándar seleccionado.

3.2.1 Criterios de selección

Los criterios de selección que se utilizaron en el presente trabajo cumplen con la tarea de demostrar que norma se ajusta a la realidad institucional de la Unidad de Tecnología de la EPMAPAP. Las fuentes de información utilizadas en las definiciones fueron recuperadas desde Real Academia Española. (2001).Diccionario de la lengua española (DRAE)(22.ª ed.); estos criterios se definen como:

A. **Contribución a la continuidad del negocio**.- Este criterio se basa en el aporte que puede brindar la norma o el estándar para garantizar la efectividad de las operaciones a través de la implementación de mecanismos que permitan asegurar la continuidad de las operaciones tecnológicas y del negocio.

B. **Flexibilidad de adaptación**.- Es la capacidad o facilidad que posee la norma para ajustarse a cambios o variaciones según las circunstancias o necesidades, que puede ser la realidad institucional de la organización, independientemente de la implementación de sistemas, procesos y políticas que estas mantengan.

C. **Norma internacional (alcance internacional)**.- Se refiere a la estandarización internacional o aplicación global que puede tener una norma, lo cual ayudará a obtener mejores resultados en su implementación.

D. **Actualización disponible**.- Esto es la facilidad y disponibilidad de actualizaciones a la cual se pueda acceder de forma periódica, lo cual se ve reflejado por medio del respaldo de un organismo internacional que se preocupe de la optimización y mejora continua de las buenas prácticas de implementación que ayuden a la continuidad del negocio.

E. **Escalabilidad**.- Se refiere a la capacidad que puede tener la norma de adaptarse, es decir de que su aplicación sea en menor o mayor escala sin afectar la

efectividad de sus procesos al ser implementados y funcionen independientemente del tamaño de la organización.

F. **Independencia**.- Que no depende de otro, este criterio se refiere a la independencia que pueda tener la norma con respecto de otras, es decir que no dependa de la implementación previa de un estándar adicional para su aplicación.

G. **Impacto**.- Se refiere al cambio brusco que pueda tener la norma una vez implementada en la organización, ya sea de carácter laboral entre el personal o de la repercusión entre la disponibilidad de los sistemas de información disponibles dentro de la empresa.

H. **Sostenibilidad**.- las normas deben garantizar que su aplicación será favorable para la organización y perdurarán en el tiempo.

I. **Aplicabilidad sector público/privado**.- es necesario conocer que normas son aplicadas por las organizaciones en el sector público y privado y cuáles se ajustan al tipo de organización que se está analizando y de esta manera asegurar que la norma utilizada es la más idónea.

J. **Certificable**.- las buenas prácticas y estándares internacionales deben certificar a las organizaciones una vez que cumplen con los requisitos establecidos, dándoles así la certeza a los consumidores de que los servicios y/o productos brindados cumplen con normas de calidad.

K. **Experiencias exitosas de implementación**.- es necesario recopilar las experiencias de organizaciones similares al implementar los estándares internacionales y de esta manera corregir posibles errores y optimizar recursos garantizando la continuidad del negocio.

3.2.2 Selección

Los criterios de selección expuestos en el apartado 3.2.1 han sido agrupados en la Tabla 1, con la finalidad de calificarlos, basándose en un criterio personal, luego de revisadas las normas y estándares expuestos.

En la Tabla 1, se listan 11 criterios los cuales representan el 100% de la ponderación de la norma a utilizar, dividiendo el 100% de dicha puntuación para el número de criterios utilizados, obteniendo un total de 9,09% en 10 de los criterios listados, con la excepción del primer criterio "Contribución a la continuidad de negocio" al que se le asignó el peso de 9,10% por efectos de redondeo. Posteriormente se realizó la calificación del cumplimiento de cada una de las normas con relación a los criterios de selección.

Tabla 1: Criterios para la selección de estándares

Peso %	**Criterios de Selección**	**Alternativas**		
		BS-25999	**ISO 22301**	**ISO 27001**
9,10%	Contribución a la continuidad de negocio	100,00%	100,00%	40,00%
9,09%	Flexibilidad de adaptación	100,00%	100,00%	90,00%
9,09%	Norma Internacional	50,00%	100,00%	100,00%
9,09%	Actualización disponible	80,00%	100,00%	90,00%
9,09%	Escalabilidad	90,00%	100,00%	80,00%
9,09%	Independencia	95,00%	97,00%	80,00%
9,09%	Impacto	80,00%	80,00%	80,00%
9,09%	Sostenibilidad	80,00%	100,00%	80,00%
9,09%	Aplicabilidad sector público/ privado	100,00%	100,00%	90,00%
9,09%	Certificable	100,00%	100,00%	100,00%
9,09%	Experiencias exitosas de implementación	98,00%	95,00%	100,00%
100,00%	**TOTAL PONDERACIÓN**	**88,46%**	**97,45%**	**84,54%**

Para obtener el porcentaje total de cumplimiento de las normas se procedió a multiplicar cada una de las calificaciones dadas a las mismas por el peso asignado a los criterios, para luego realizar la sumatoria.

Del análisis realizado en la Tabla 1, se selecciona el estándar ISO 22301 por ser el que cuenta con la mayor puntuación de cumplimiento de los criterios analizados, también se utilizarán las normas de control interno de la Contraloría General del Estado.

CAPÍTULO IV
DEFINICIÓN DEL DRP PARA LA UNIDAD DE TECNOLOGÍA DE LA EPMAPAP.

4.1. Descripción de la Unidad de Tecnología de la EPMAPAP.

La Unidad de Tecnología de la EPMAPAP, es un área de asesoría tecnológica que brinda servicios de soporte y administración de los sistemas informáticos a las áreas administrativas de la EPMAPAP.

4.1.1. Estructura orgánica de la EPMAPAP

La composición de la estructura Orgánica funcional está determinada en forma piramidal jerárquica como se muestra en la Figura 1, donde las Direcciones Ejecutivas se encuentran en la base y los Departamentos Operativos en el borde de su extremo externo, vínculo directo con el consumidor.

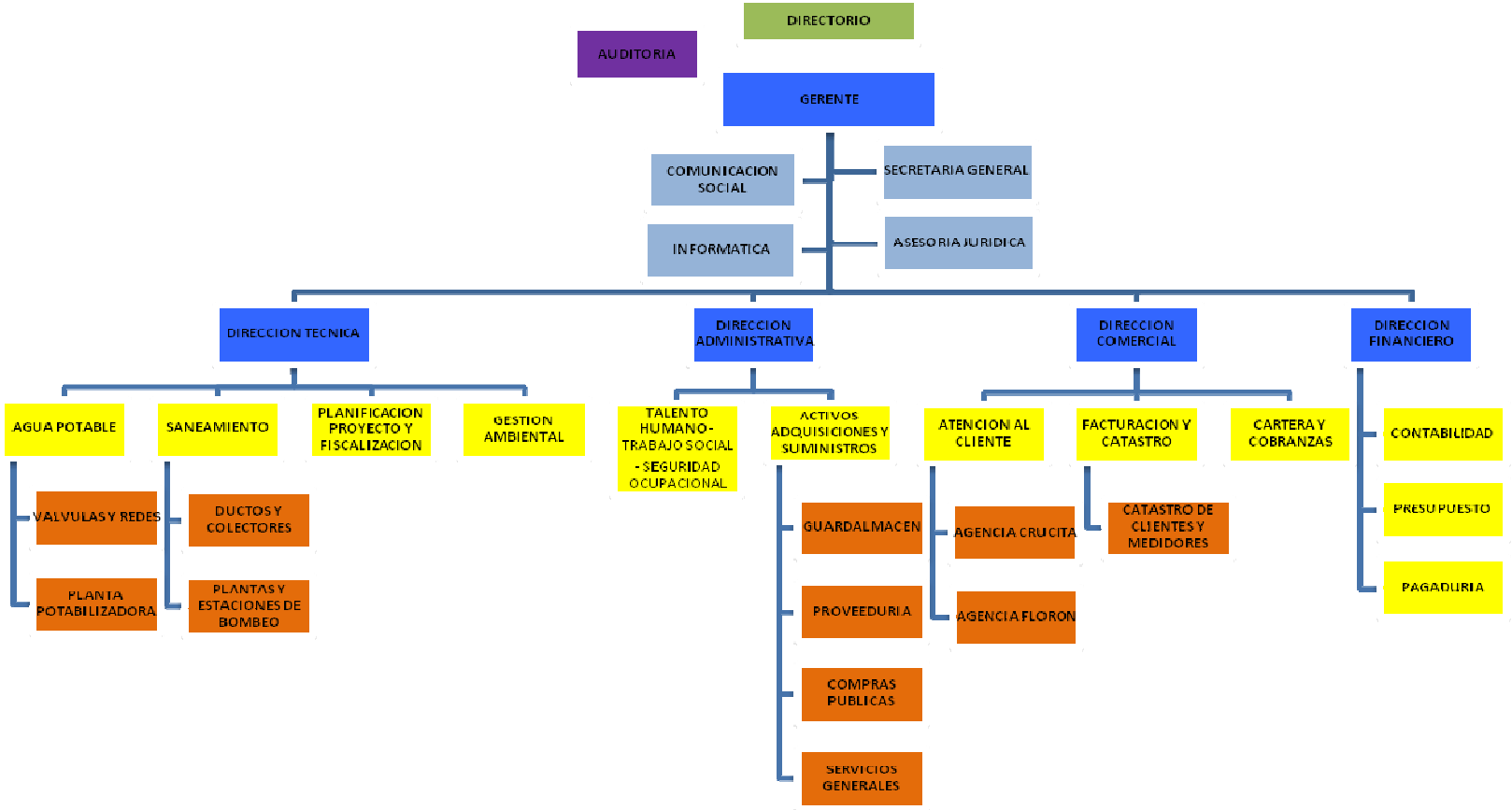

Figura 1: Estructura Orgánica Funcional EPMAPAP

Fuente: Reglamento de la Estructura Orgánica Funcional de la EPMAPAP 2013

4.1.2. Servicios Informáticos – Unidad de Tecnología

Este departamento operativo se encuentra posicionado dentro del Orgánico funcional, como un área de asesoría a la Gerencia General, brindando la asesoría tecnológica dentro de las gestiones administrativas, alineadas siempre a los objetivos institucionales.

4.1.2.1. Misión

Desarrollar e implementar soluciones tecnológicas acordes a las necesidades de la Empresa y que puestas al servicio de los funcionarios de la Institución permitan alcanzar la excelencia en todos sus ámbitos. (Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo, 2013)

4.1.2.2. Productos

- Brindar a Gerencia asesoría integral sobre la tecnología informática aplicada a las políticas operativas y administrativas de la Empresa;
- Definir lineamientos y características para la adquisición de recursos tecnológicos;
- Conciliar el inventario tecnológico de la Empresa;
- Supervisar el buen uso de los activos tecnológicos;
- Definir y controlar las políticas de uso de los recursos tecnológicos de la empresa;
- Definir los procedimientos de contingencia o planes de recuperación de desastre;

- Informar a la Gerencia de las eventualidades presentadas respecto al departamento y recursos tecnológicos de la Empresa. (Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo, 2013)

4.1.2.3. Estructura Orgánica Unidad de Servicios Informáticos EPMAPAP

La Unidad de Servicios Informáticos de la EPMAPAP consta de una pequeña estructura jerárquica de 3 departamentos básicos (base de datos y sistemas, técnico informático y redes y comunicaciones), que dependen del Jefe de Servicios Informáticos quien es la cabeza principal de esta unidad, ver Figura 2.

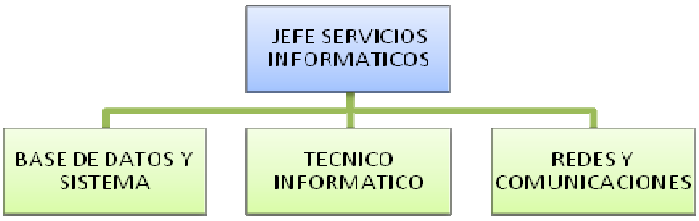

Figura 2: Estructura Orgánica Unidad de Servicios Informáticos EPMAPAP
Fuente: Reglamento de la Estructura Orgánica Funcional de la EPMAPAP 2013

4.1.2.4. Estructura Funcional

4.1.2.4.1. Jefe Departamento de Servicios Informáticos

a) Brindar a la Gerencia la asesorar integral sobre la tecnología informática aplicada a las políticas operativas y administrativas de la Empresa;

b) Realizar las gestiones administrativas del departamento;

c) Supervisar y coordinar las funciones y trabajos del recurso humano del departamento;

d) Coordinar y asesorar en la integración de nuevos procesos automatizados;

e) Definir lineamientos y características para la adquisición de recursos tecnológicos;

f) Conciliar el inventario tecnológico de la Empresa;

g) Supervisar el buen uso de los activos tecnológicos;

h) Definir y controlar las políticas de uso de los recursos tecnológicos de la empresa;

i) Definir los procedimientos de contingencia o planes de recuperación de desastre;

j) Informar a la Gerencia de las eventualidades presentadas respecto al departamento y recursos tecnológicos de la Empresa. (Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo, 2013)

4.1.2.4.2. Administrador de Base de Datos y Sistemas

a) Administrar y controlar los Sistemas Manejadores de Base de Datos (DBMS);

b) Administrar la actividad de los datos almacenados;

c) Responsable de definir y documentar(diccionario de datos) el diseño y estructura de las Bases de Datos que serán utilizadas en el desarrollo o reingeniería de aplicaciones;

d) Asegurar la confiabilidad, integridad y disponibilidad de la Base de Datos en producción;

e) Gestionar y custodiar los respaldos de información (*backup*);

f) Administrar la seguridad de los servidores de base de datos y de los DBMS;

g) Presentar estadísticas de la actividad y procesos de las bases de datos en todas sus dimensiones y de todos los sucesos;

h) Registrar e informar al Jefe, los eventos que se presenten en las Bases de Datos y las acciones tomadas para su resolución;

i) Desarrollar reportes y aplicaciones que consulten y procesen información de las bases de datos. (Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo, 2013)

4.1.2.4.3. Administrador de Redes y Comunicaciones

a) Configurar y proporcionar seguridad a los servidores;

b) Controlar las redes de voz y datos y proporcionar las seguridades de acceso y disponibilidad de las mismas;

c) Implementar y/o desarrollar herramientas de monitoreo de tráfico y vulnerabilidades en las redes de voz y datos;

d) Mantenimiento e implementación de cableado estructurado en todas las oficinas de la EPMAPAP;

e) Asignar claves a usuarios de los sistemas en producción;

f) Gestionar el Plan de Seguridad Informática y mantenerlo actualizado;

g) Gestionar el direccionamiento IP a todos los equipos informáticos de la Empresa;

h) Proponer y coordinar cambios para el mejoramiento de la calidad de servicio (QoS) en la comunicación de datos del parque informático de la Empresa;

i) Presentar estadísticas de la actividad y sucesos evidenciados en las redes de voz y datos;

j) Registrar e informar al Jefe, los eventos que se presenten en las redes de voz y datos y las acciones tomadas para su resolución. (Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo, 2013)

4.1.2.4.4. Técnico Informático

a) Instalación y configuración de equipos y sistemas informáticos;

b) Elaboración y ejecución del plan de mantenimiento preventivo y correctivo de los equipos del parque informático y de los sistemas de información de la EPMAPAP;

c) Brindar soporte oportuno y capacitación a los usuarios sobre los sistemas y equipos informáticos para que pueda ejecutarlos y operarlos de forma segura y adecuada;

d) Mantener actualizada la documentación técnica y usuaria para cada uno de los sistemas informáticos y en caso de un futuro mantenimiento a los mismos se hagan las correcciones o incorporaciones adicionales a dicha documentación;

e) Elaborar los manuales de procedimientos de instalación de los equipos y aplicativos de las estaciones de trabajos;

f) Llevar el inventarios de equipos, aplicativos instalados, licencias, garantías;

g) Creación y configuración de las cuentas de correo electrónico;

h) Coordinación de trabajo, colaboración y aportes de ideas y soluciones a problemas o necesidades presentadas;

i) Registrar e informar al Jefe, de las eventualidades presentadas en el funcionamiento de los equipos existentes en el parque informático de la Empresa y las acciones tomadas para su resolución. (Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo, 2013)

4.1.3. Sistemas informáticos relacionados a los servicios organizacionales

La EPMAPAP cuenta con sistemas informáticos integrados dentro de sus principales áreas, tales como la Dirección comercial, la Dirección administrativa, la Dirección financiera y la Dirección de Talento Humano, los cuáles interactúan entre

sí para brindar a sus abonados los diferentes servicios institucionales que ofrece la entidad.

En conjunto con el Jefe de Servicios Informáticos de la EPMAPAP, Ing. Iván González, se definieron las funciones y principales características de los sistemas informáticos utilizados en la EPMAPAP, los cuáles se detallan en los siguientes numerales: 4.1.3.1, 4.1.3.2, 4.1.3.3, 4.1.3.4, 4.1.3.5.

4.1.3.1. Sistema informático financiero – AFINANCIAL

Sistema informático financiero que permite la gestión contable de la Institución, se basa en una arquitectura cliente – servidor de 3 capas, de interfaces visuales, instalado como aplicación del sistema operativo en cada equipo. Utiliza el gestor de base de datos Oracle 10g y sus interfaces de usuario se encuentran desarrolladas en java script. Aún no se encuentra en producción debido a que la empresa no ha migrado totalmente la base contable y sus estados financieros a este sistema.

4.1.3.2. Sistema informático contable OLYMPO

Sistema informático financiero que permite la gestión contable de la Institución, está basado en interfaces visuales de fácil manejo. Es un sistema de arquitectura cliente – servidor de 2 capas, utiliza el gestor de base de datos SQL Server 2005 y sus interfaces de usuario se encuentran desarrolladas en C # y C Sharp.

4.1.3.3. Sistema informático de talento humano – ATHIE

Sistema informático que permite la gestión del Talento humano, el cual se encuentra ligado a los equipos de marcación biométrica de la empresa; el sistema está basado en una arquitectura cliente – servidor de 3 capas, utiliza el gestor de base

de datos Oracle 10.g y sus interfaces de usuario se encuentran desarrolladas en java script. Este sistema no se encuentra aún en producción.

4.1.3.4. Sistema informático administrativo – AFLOW

Sistema informático utilizado para la gestión documental y administrativa de la Institución, permite la administración de pedidos y reclamos de clientes, además de la gestión de campo generada por el personal técnico; este sistema está basado en una arquitectura cliente – servidor de 3 capas, utiliza el gestor de base de datos SQL Server 2005 y sus interfaces de usuario se encuentran desarrolladas en java script.

4.1.3.5 Sistema informático comercial – ABILLING

Sistema informático comercial, utilizado para los procesos de facturación y posterior recaudación de los valores generados por servicios institucionales brindados a la ciudadanía; este sistema está basado en una arquitectura cliente – servidor de 3 capas, utiliza el gestor de base de datos Oracle 10g. y sus interfaces de usuario se encuentran desarrolladas en java script.

4.1.4. Diagrama de red Organizacional

En la Figura 3, se puede apreciar el diagrama de red organizacional con el que cuenta la EPMAPAP, el cual consta de 2 nodos principales: las oficinas centro (en la cual se basará el presente trabajo) y las oficinas matriz ubicadas en la Cdla. El Maestro, los 2 nodos ubicados dentro de la ciudad de Portoviejo. Adicionalmente cuenta de 4 nodos secundarios, agencia el Florón, agencia Crucita, PTAR y Planta de bombeo de 4 esquinas.

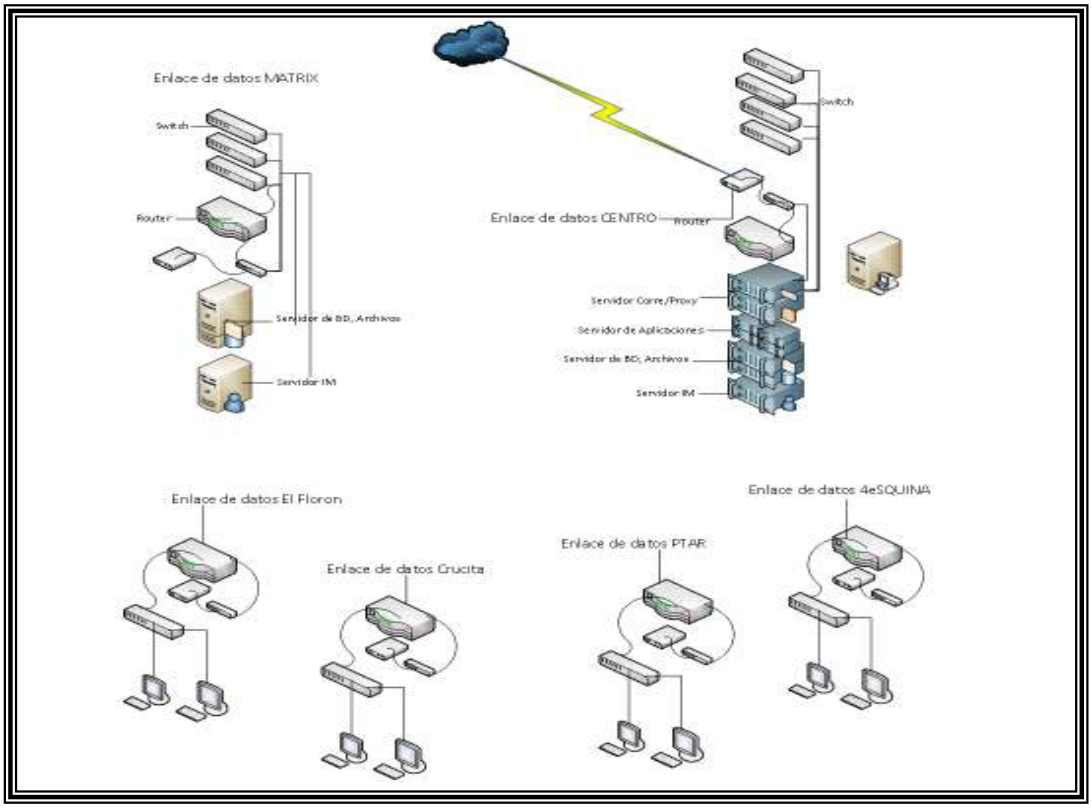

Figura 3: Diagrama de Red Organizacional
Fuente: Unidad de Servicios Informáticos EPMAPAP

4.2. Desarrollo del DRP

La norma ISO 22301:2012, abarca un campo muy amplio como es la continuidad del negocio que comprende la recuperación de todo el engranaje de procesos de las operaciones que se llevan a cabo en la organización; lo cual para la aplicabilidad de esta tesis se tomó lo más importante y complementario para el desarrollo del DRP, enfocándose en la recuperación de las actividades tecnológicas de mayor relevancia que mantienen los procesos comerciales de la EPMAPAP.

El DRP se basa en la continuidad de las operaciones de los sistemas informáticos y procesos tecnológicos que mantiene la Unidad de Servicios informáticos de la EPMAPAP para sustentar las principales actividades que se desarrollan en la

organización; estos servicios que ofrece la Unidad de tecnología a las áreas usuarias, deben estar siempre disponibles para poder asegurar la estabilidad económica y financiera de la institución y su permanencia en el mercado, sin caer en violaciones de las leyes y de observancias de los organismos de control que así lo exigen.

El DRP para la Unidad de Tecnología de la EPMAPAP se desarrolla bajo el estándar ISO 22301:2012. Este DRP consta de una serie de documentos formulados a partir de las necesidades y objetivos institucionales que espera cumplir la organización. Estos documentos se detallan en la Tabla 2, los cuáles se adjuntan como anexos de esta tesis.

Tabla 2: Documentos del plan de recuperación de desastres

Ubicación del Documento	Nombre del Documento
ANEXO 1	Control de información documentada
ANEXO 2	Requisitos legales, normativos y reglamentarios
ANEXO 2.1	Lista de requisitos legales, normativos y reglamentarios
ANEXO 3	Política de continuidad de servicios tecnológicos
ANEXO 4	Análisis de impacto en el negocio
ANEXO 4.1	Cuestionario de análisis de impacto– Disponibilidad del servicio de comunicación
ANEXO 4.2	Cuestionario de análisis de impacto– Disponibilidad del sistema comercial
ANEXO 4.3	Cuestionario de análisis de impacto– Disponibilidad del sistema administrativo
ANEXO 4.4	Cuestionario de análisis de impacto– Disponibilidad del sistema financiero
ANEXO 5	Estrategia de continuidad de los servicios tecnológicos
ANEXO 5.1	Lista de actividades
ANEXO 5.2	Prioridades de recuperación
ANEXO 5.3	Objetivos de tiempo de recuperación
ANEXO 5.4	Escenarios de incidentes disruptivos
ANEXO 5.5	Plan de preparación para la continuidad de los servicios tecnológicos
ANEXO 5.6	Estrategia de recuperación - Disponibilidad del servicio de comunicación
ANEXO 5.7	Estrategia de recuperación - Disponibilidad del sistema comercial

ANEXO 5.8	Estrategia de recuperación - Disponibilidad del sistema administrativo
ANEXO 5.9	Estrategia de recuperación - Disponibilidad del sistema financiero
ANEXO 5.10	Cuestionario de evaluación de control interno
ANEXO 5.11	Calificación de la evaluación de control interno
ANEXO 5.12	Matriz de evaluación de riesgos
ANEXO 5.13	Matriz de tratamiento de riesgos
ANEXO 5.14	Plan de evacuación
ANEXO 6	Plan de continuidad
ANEXO 6.1	Plan de respuesta a incidentes generales
ANEXO 6.2	Registro de incidentes
ANEXO 6.3	Ubicaciones estratégicas de continuidad
ANEXO 6.4	Plan de transporte
ANEXO 6.5	Registro de contactos
ANEXO 6.6	Plan de recuperación - Disponibilidad del servicio de comunicación
ANEXO 6.7	Plan de recuperación - Disponibilidad del sistema comercial
ANEXO 6.8	Plan de recuperación - Disponibilidad del sistema administrativo
ANEXO 6.9	Plan de recuperación - Disponibilidad del sistema financiero
ANEXO 7	Formulario de informe de pruebas
ANEXO 8	Plan de capacitación
ANEXO 9.1	Programa de auditoría
ANEXO 9.2	Informe de auditoría
ANEXO 10	Formulario de medidas correctivas
ANEXO 11	Matriz RACI de responsabilidades

- **Control de información documentada**

Este documento tiene como objetivo el de asegurar el control de la información documentada con respecto a la creación, actualización, distribución, acceso, recuperación y uso de los documentos utilizados en el Plan de Recuperación de Desastres (DRP), ver Anexo 1.

- **Requisitos legales, normativos y reglamentarios**

El presente documento tiene como objetivo determinar las partes interesadas que son relevantes para la organización y los requisitos de estas partes interesadas, además de los requisitos legales, normativos y reglamentarios aplicables a la organización, ver Anexo 2.

- **Lista de requisitos legales, normativos y reglamentarios**

En este documento se listan todos los requisitos legales, normativos, y reglamentarios que hacen necesario el desarrollo del plan de recuperación de desastres y su posterior implementación, ver Anexo 2.1.

- **Política de continuidad de servicios tecnológicos**

El presente documento tiene como objetivo definir el alcance y reglas básicas para la gestión de la continuidad de los servicios tecnológicos, ver Anexo 3.

- **Análisis de impacto en el negocio**

El presente documento tiene como objetivo definir el proceso de evaluación que se aplicará a los principales servicios que ofrece la unidad de tecnología y determinar el impacto de interrupción en el negocio, para priorizar objetivos de recuperación, ver Anexo 4.

- **Cuestionario de análisis de impacto – Disponibilidad del servicio de comunicación**

En este documento se detallan las tareas, recursos y datos necesarios para la recuperación de la actividad de Disponibilidad del servicio de comunicación, ver Anexo 4.1.

- **Cuestionario de análisis de impacto – Disponibilidad del sistema comercial**

En este documento se detallan las tareas, recursos y datos necesarios para la recuperación de la actividad de Disponibilidad del sistema comercial, ver Anexo 4.2.

- **Cuestionario de análisis de impacto – Disponibilidad del sistema administrativo**

En este documento se detallan las tareas, recursos y datos necesarios para la recuperación de la actividad de Disponibilidad del sistema administrativo, ver Anexo 4.3.

- **Cuestionario de análisis de impacto – Disponibilidad del sistema financiero**

En este documento se detallan las tareas, recursos y datos necesarios para la recuperación de la actividad de Disponibilidad del sistema financiero, ver Anexo 4.4.

- **Estrategia de continuidad de los servicios tecnológicos**

El presente documento tiene como objetivo determinar una estrategia de recuperación apropiada para asegurar la protección de las actividades priorizadas, sus dependencias y el apoyo de recursos, sirviendo de base para la continuidad y recuperación de los servicios tecnológicos que sustentan el negocio, ver Anexo 5.

- **Lista de actividades**

Este documento detalla las actividades principales y complementarias de recuperación que garantizan la continuidad de las operaciones organizacionales que dependen de la Unidad de servicios informáticos, ver Anexo 5.1.

- **Prioridades de recuperación**

Este documento define los períodos máximos tolerables de interrupción para cada actividad y establece prioridades en consecuencia, ver Anexo 5.2.

- **Objetivos de tiempo de recuperación**

Este documento define los objetivos de tiempo de recuperación para cada actividad a recuperar considerada dentro del DRP, ver Anexo 5.3.

- **Escenarios de incidentes disruptivos**

Este documento define escenarios comunes de incidentes disruptivos, ver Anexo 5.4.

- **Plan de preparación para la continuidad de los servicios tecnológicos**

Este documento define los preparativos para cumplir con las condiciones necesarias y poder retomar en forma satisfactoria las actividades comerciales luego de un incidente disruptivo, ver Anexo 5.5.

- **Estrategia de recuperación - Disponibilidad del servicio de comunicación**

Este documento define las responsabilidades claves, el tratamiento de los recursos y el procedimiento aplicable a las copias de seguridad de los datos para la recuperación de la actividad actual, ver Anexo 5.6.

- **Estrategia de recuperación - Disponibilidad del sistema comercial**

Este documento define las responsabilidades claves, el tratamiento de los recursos y el procedimiento aplicable a las copias de seguridad de los datos para la recuperación de la actividad actual, ver Anexo 5.7.

- **Estrategia de recuperación - Disponibilidad del sistema administrativo**

Este documento define las responsabilidades claves, el tratamiento de los recursos y el procedimiento aplicable a las copias de seguridad de los datos para la recuperación de la actividad actual, ver Anexo 5.8.

- **Estrategia de recuperación - Disponibilidad del sistema financiero**

Este documento define las responsabilidades claves, el tratamiento de los recursos y el procedimiento aplicable a las copias de seguridad de los datos para la recuperación de la actividad actual, ver Anexo 5.9.

- **Cuestionario de evaluación de control interno**

Este documento describe el cuestionario de control interno realizado a la Unidad de servicios informáticos de la EPMAPAP para la evaluación y verificación de los controles implementados o la falta de estos, ver Anexo 5.10.

- **Calificación de la evaluación de control interno**

Este documento contiene la evaluación realizada a la Unidad de servicios informáticos mediante el cuestionario de control interno, ver Anexo 5.11.

- **Matriz de evaluación de riesgos**

Este documento contiene la matiz de evaluación y respuesta a los riesgos luego de realizada la calificación mediante el cuestionario de control interno, ver Anexo 5.12.

- **Matriz de tratamiento de riesgos**

Este documento contiene la respuesta y las instrucciones de auditoría de cómo tratar los riesgos una vez identificados, ver Anexo 5.13.

- **Plan de evacuación**

Este documento define el plan de evacuación del edificio y los procedimientos básicos a seguir en casos de emergencia por circunstancias de esta naturaleza, ver Anexo 5.14.

- **Plan de continuidad**

El presente documento tiene como objetivo determinar procedimientos documentados para responder a incidentes perturbadores y como continuar o recuperar sus principales actividades tecnológicas dentro de un marco de tiempo predeterminado, ver Anexo 6.

- **Plan de respuesta a incidentes generales**

El presente documento tiene como objetivo asegurar la protección y bienestar de los individuos ante la ocurrencia de desastres, así como también contener el incidente, reduciendo al mínimo posible el daño sobre el negocio, sus empleados y sus partes interesadas, ver Anexo 6.1.

- **Registro de incidentes**

Este documento clasifica los incidentes disruptivos y presenta un formato para el registro de estos cuando se presentan, ver Anexo 6.2.

- **Ubicaciones estratégicas de continuidad**

Este documento proporciona las ubicaciones disponibles alternativas para asegurar la continuidad de las operaciones tecnológicas en caso de incidentes disruptivos, ver Anexo 6.3.

- **Plan de transporte**

Este documento presenta la forma en que se organizará el transporte en caso de que se activen los planes de recuperación, ver Anexo 6.4.

- **Registro de contactos**

Este documento lista los principales datos de los empleados que se encuentran vinculados a las acciones de recuperación o involucrados dentro de las actividades del DRP, ver Anexo 6.5.

- **Plan de recuperación - Disponibilidad del servicio de comunicación**

El presente documento tiene como objetivo definir de forma precisa la recuperación de las actividades críticas dentro de plazos establecidos ante la ocurrencia de desastres o de incidentes disruptivos, ver Anexo 6.6.

- **Plan de recuperación - Disponibilidad del sistema comercial**

El presente documento tiene como objetivo definir de forma precisa la recuperación de las actividades críticas dentro de plazos establecidos ante la ocurrencia de desastres o de incidentes disruptivos, ver Anexo 6.7.

- **Plan de recuperación - Disponibilidad del sistema administrativo**

El presente documento tiene como objetivo definir de forma precisa la recuperación de las actividades críticas dentro de plazos establecidos ante la ocurrencia de desastres o de incidentes disruptivos, ver Anexo 6.8

- **Plan de recuperación - Disponibilidad del sistema financiero**

El presente documento tiene como objetivo definir de forma precisa la recuperación de las actividades críticas dentro de plazos establecidos ante la ocurrencia de desastres o de incidentes disruptivos, ver Anexo 6.9.

- **Formulario de informe de pruebas**

Este documento es un formato que se usará para el registro de las pruebas y verificaciones periódicas o imprevistas con el fin de evaluar y detectar problemas que se presenten al momento de aplicar el DRP, para luego tomar las medidas correctivas necesarias, ver Anexo 7.

- **Plan de capacitación**

Este documento detalla la capacitación necesaria para preparar al personal para que pueda cumplir su función dentro del plan de recuperación de desastres, ver Anexo 8.

- **Programa de auditoría**

Este documento es un formato para redactar el programa anual de auditoría interna sobre el marco de la norma ISO 22301:2012, ver Anexo 9.1.

- **Informe de auditoría**

Formato básico para el registro de las auditorías internas realizadas al DRP desarrollado luego de su implementación, ver Anexo 9.2.

- **Formulario de medidas correctivas**

Este documento es un formato para el registro de las acciones correctivas detectadas durante incidentes disruptivos al aplicar los procedimientos del DRP, con el objetivo de implementar la mejora continua al presente plan de recuperación de desastres, ver Anexo 10.

- **Matriz RACI de responsabilidades**

Es una matriz de asignación de responsabilidades, en la cual se especifica el rol de cada persona dentro de la gestión del DRP para la continuidad del negocio. En la matriz se detalla quien ejecuta cada actividad, a quien se consulta, quien autoriza y a quien se informa, ver Anexo 11.

4.3. Pruebas piloto

Una vez desarrollado el documento del plan de continuidad ver Anexo 6, como parte del DRP para la Unidad de Servicios Informáticos de la EPMAPAP y siguiendo la norma ISO 22301:2012, se realizaron los simulacros o pruebas piloto a esta unidad organizativa con tres escenarios seleccionados para medir el grado de eficacia y aplicabilidad del plan desarrollado.

Los escenarios aplicados fueron seleccionados de forma discrecional por el autor debido a que la actual tesis es una propuesta de diseño de un DRP pero el mismo no se encuentra implementado, por esta razón la falta de recursos materiales, humanos y logísticos impidieron probar escenarios de mayor complejidad.

Las pruebas pilotos realizadas fueron documentadas siguiendo el esquema que manda la norma ISO 22301:2012, dichos documentos se detallan en el Anexo 12.

Las pruebas pilotos se realizaron con éxito, obteniéndose los resultados esperados en cada una de las pruebas, demostrando el beneficio de contar con procedimientos ordenados en un plan de respuesta a incidentes, donde cada persona sabe cómo actuar y los recursos de los que dispone.

CAPITULO V

ESTUDIO DE FACTIBILIDAD

5.1 Factibilidad Técnica

Una vez desarrollado el diseño del DRP para la Unidad de Servicios informáticos de la EPMAPAP se pudo determinar que existe la factibilidad técnica en la implementación del mencionado DRP, ya que se cuenta con los conocimientos y habilidades tanto de los niveles directivos para la gestión administrativa y de los niveles de gestión operativa de las tareas informáticas de la institución, necesarios para la recuperación de actividades que involucran en su gran mayoría el manejo de equipos informáticos y de comunicación, comprobando esto mediante los perfiles y habilidades del personal que labora en este departamento tecnológico, tal como se muestra en la Tabla 3.

Tabla 3: Perfiles del personal de TIC de la EPMAPAP

Apellidos y Nombres	Título de tercer nivel	Experiencia Áreas	# Años de experiencia
José Iván Alcívar Moreira	Ingeniero en sistemas informáticos	• Seguridad y base de datos. • Telecomunicaciones • Desarrollo de software	3
Javier Hernán López Zambrano	Ingeniero en sistemas computacionales	• Seguridad y base de datos. • Telecomunicaciones • Desarrollo de software	4
Eglice Renán Ross Villavicencio	Técnico informático	• Soporte técnico. • Instalación y mantenimiento de hardware y software	3

Así mismo se establece que se cuentan con las herramientas informáticas necesarias para la administración y recuperación de actividades que exige el DRP

desarrollado, entre estas herramientas podemos mencionar las que se muestran en la Tabla 4.

Tabla 4: Herramientas informáticas de administración

Aplicación	Tipo de software	Tipo licencia	Plataforma
WhatsUp Gold	Monitoreo de red	Propietario	Windows
Consolas de comandos integradas en el sistema operativo	Consola de comandos	GLP – Software libre	Linux

Adicionalmente los recursos técnicos actuales deben ser complementados mediante capacitaciones especializadas en temas específicos, dirigidas al personal involucrado dentro de las acciones del DRP tal como se muestra en la Tabla 102. Así como también campañas de concientización a todo el personal de la EPMAPAP sobre la prevención y mitigación de riesgos, aplicación de medidas de seguridad y colaboración en la implementación de acciones correctivas que contribuyan al desarrollo institucional.

5.2 Factibilidad Operativa

La EPMAPAP posee una estructura orgánica funcional, ver Figura 1, que permite la toma de decisiones de forma oportuna, brindando disponibilidad en la vinculación del talento humano del que dispone la organización, esta efectiva operabilidad coordinada con los procesos definidos en el manual de procesos organizacionales de la EPMAPAP permite la viabilidad operativa del DRP desarrollado.

El personal seleccionado una vez que reciba la capacitación propuesta, ver Tabla 102, puede hacer un uso efectivo y garantizado del DRP, debido a su gran

experiencia y empoderamiento de los procesos organizacionales que manejan. La viabilidad operativa del DRP desarrollado se basa en la tecnología alcanzable para la realización de dicho proyecto y con el personal operativo como lo son los usuarios operacionales de los sistemas informáticos; el personal técnico que realizará las operaciones informáticas avanzadas de configuración y resolución de los incidentes relacionados a tecnología de la información y por último el personal de gestión que se compone de los directivos de la institución.

5.3 Factibilidad Legal

En el literal i) del Reglamento de la Estructura Orgánica y Funcional de la EPMAPAP se establece que es función del jefe del departamento de servicios informáticos: "Definir los procedimientos de contingencia o planes de recuperación de desastre" (Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo, 2013)

En la norma de control interno 410-11 de la Contraloría General del Estado dice que: "Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado"**.** (Contraloría General del Estado, 2009)

(Asamblea Nacional Constituyente, 2008) la Constitución de la República del Ecuador en sus Art. 389 y 390 menciona:

> **Art. 389.-** El Estado protegerá a las personas, las colectividades y la naturaleza frente a los efectos negativos de los desastres de origen natural o antrópico mediante la prevención ante el riesgo, la mitigación de desastres, la

recuperación y mejoramiento de las condiciones sociales, económicas y ambientales, con el objetivo de minimizar la condición de vulnerabilidad.

El sistema nacional descentralizado de gestión de riesgo está compuesto por las unidades de gestión de riesgo de todas las instituciones públicas y privadas en los ámbitos local, regional y nacional. El Estado ejercerá la rectoría a través del organismo técnico establecido en la ley. Tendrá como funciones principales, entre otras:

1. Identificar los riesgos existentes y potenciales, internos y externos que afecten al territorio ecuatoriano.
2. Generar, democratizar el acceso y difundir información suficiente y oportuna para gestionar adecuadamente el riesgo.
3. Asegurar que todas las instituciones públicas y privadas incorporen obligatoriamente, y en forma transversal, la gestión de riesgo en su planificación y gestión.
4. Fortalecer en la ciudadanía y en las entidades públicas y privadas capacidades para identificar los riesgos inherentes a sus respectivos ámbitos de acción, informar sobre ellos, e incorporar acciones tendientes a reducirlos.
5. Articular las instituciones para que coordinen acciones a fin de prevenir y mitigar los riesgos, así como para enfrentarlos, recuperar y mejorar las condiciones anteriores a la ocurrencia de una emergencia o desastre.
6. Realizar y coordinar las acciones necesarias para reducir vulnerabilidad es y prevenir, mitigar, atender y recuperar eventuales efectos negativos derivados de desastres o emergencias en el territorio nacional.
7. Garantizar financiamiento suficiente y oportuno para el funcionamiento del Sistema, y coordinar la cooperación internacional dirigida a la gestión de riesgo.

Art. 390.- Los riesgos se gestionarán bajo el principio de descentralización subsidiaria, que implicará la responsabilidad directa de las instituciones dentro de su ámbito geográfico. Cuando sus capacidades para la gestión del riesgo sean

insuficientes, las instancias de mayor ámbito territorial y mayor capacidad técnica y financiera brindarán el apoyo necesario con respeto a su autoridad en el territorio y sin relevarlos de su responsabilidad.

Las citas anteriores demuestran la factibilidad legal que presenta el DRP desarrollado, estos documentos legales obligan a la implementación de planes de recuperación que incluyan la mitigación de riesgos dentro de la organización.

5.4 Factibilidad Económica

De acuerdo al estudio realizado se estableció el costo de la caída concurrente de todos los sistemas informáticos que sustentan las operaciones de la EPMAPAP. De la misma manera se estableció también el valor a invertir en los recursos necesarios para la recuperación de las actividades contempladas en el DRP desarrollado y que son las que sustentan las operaciones de la organización, ver Tabla 5.

Tabla 5: Presentación de factibilidad económica

Actividad	Costo Semanal Incidente disruptivo	Costo de Inversión
Disponibilidad del servicio de comunicación	61000,00	20000,00
Disponibilidad del sistema comercial	21500,00	15000,00
Disponibilidad del sistema administrativo	13500,00	15000,00
Disponibilidad del sistema financiero	7000,00	15000,00
Total	**103000,00**	**65000,00**

La relación entre el valor a invertir en el DRP y el costo de la interrupción que pudieran sufrir las operaciones principales de la EPMAPAP se presenta en el gráfico estadístico comparativo, ver Figura 4, que refleja claramente la factibilidad económica del DRP desarrollado para la organización.

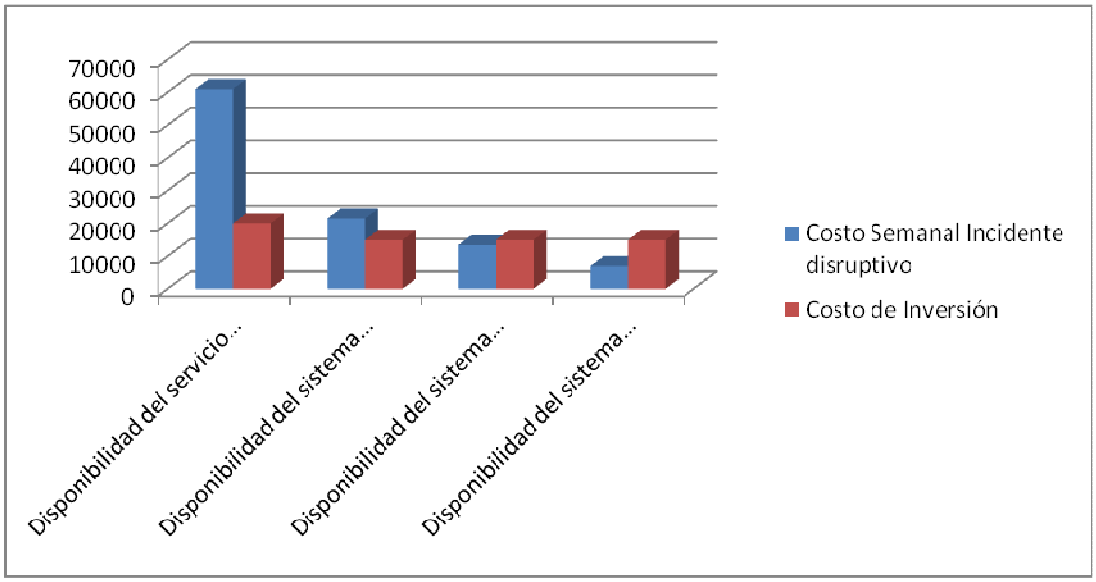

Figura 4: Cuadro estadístico comparativo costo de pérdida vs costo de inversión

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. Conclusiones

Una vez finalizado el presente trabajo de desarrollo de un plan de recuperación de desastres para la Unidad de Tecnología de la EPMAPAP se concluye lo siguiente:

- La norma ISO 22301:2012 se ajusta a las necesidades institucionales de la EPMAPAP debido a su flexibilidad de adaptación a cualquier organización sin importar su tipo, tamaño y naturaleza, lo que permitió la culminación del presente plan de recuperación de desastres.

- La norma ISO 22301:2012 aplicada en el presente trabajo, fue la mejor opción (solución) para desarrollar el plan de recuperación de desastres para la unidad de servicios informáticos de la EPMAPAP, quedando así demostrado mediante las pruebas pilotos que se realizaron con el objetivo de probar su eficacia y la flexibilidad de acoplamiento que brinda la norma.

- Después del análisis realizado se demuestra que existe la viabilidad técnica, operativa, legal y económica del DRP desarrollado, considerando los beneficios y prestaciones que motivan su implementación dentro de la Unidad de servicios informáticos de la organización.

- Las pruebas preliminares del DRP desarrollado corroboran el estudio de su factibilidad así como, permiten afirmar que es posible su implementación y operación en el marco organizacional de la EPMAPAP.

- El diseño desarrollado del DRP basado en la norma ISO 22301:2012, ha sido una solución demostrada mediante las pruebas pilotos y los estudios de factibilidad realizados que demuestran su viabilidad de implementación dentro del marco estructural y organizacional de la EPMAPAP.

6.2. Recomendaciones

Luego de haber analizado la aplicación del estándar ISO 22301:2012 en el desarrollo del DRP para la Unidad de servicios informáticos de la EPMAPAP se recomienda lo siguiente:

- Implementar el plan de recuperación de desastres desarrollado para la unidad de servicios informáticos de la EPMAPAP, para asegurar la continuidad de las operaciones tecnológicas y de los servicios informáticos que brinda este departamento, que son la base sustentable para llevar a cabo las principales actividades de la organización.

- Realizar la socialización del presente plan de recuperación de desastres a todo el personal de la institución para concientizar las acciones y medidas correctivas que se puedan tomar sin haber implementado el mismo, además de brindar una idea más clara y de prevención ante desastres o incidentes disruptivos que se pudieran presentar.

- Dotar al personal de la debida capacitación que ayude a adquirir las habilidades básicas necesarias para la integración del personal dentro del DRP desarrollado que complemente las habilidades y destrezas inmersas en el perfil de cada empleado.

- Acoger la norma ISO 22301:2012 en el resto de unidades organizativas de la EPMAPAP para asegurar la continuidad del negocio mediante un completo Sistema de Gestión de Continuidad del Negocio.

- Realizar un convenio de alianza estratégica con la Empresa homónima de servicio básico de agua potable de la ciudad de Manta denominada Empresa Pública Aguas de Manta, a fin de unir esfuerzos y servir de centros de recuperación remoto de forma bilateral, tal como se especifica en el desarrollo del presente DRP.

BIBLIOGRAFÍA

(s.f.). Recuperado el 13 de Agosto de 2013, de Sitio Web de inBest: http://inbest.me/que-es-un-drp

(s.f.). Recuperado el 13 de Agosto de 2013, de sitio Web de Grupo Pragma Consultores: http://www.pragmaconsultores.com/servicios/consultoria/Paginas/herramientas_gobierno_y_gestion.aspx

(s.f.). Recuperado el 12 de Agosto de 2013, de sitio Web de Balarezo Consultores CIA. LTDA.: http://www.bconsultores.com/index.php?option=com_content&view=article&id=31&Itemid=80

(s.f.). Recuperado el 13 de Agosto de 2013, de sitio web de EPPS *Services* Ltd.: http://www.iso27001standard.com/es/que-es-la-norma-bs-25999-2

Aguilera, P. (2010). *Seguridad Informática.* Recuperado el 12 de Agosto de 2013, de books.google.com.ec: http://books.google.com.ec/books?id=Mgvm3AYIT64C&pg=PA23&dq=Un+instrumento+de+gesti%C3%B3n+que+contiene+las+medidas+%28tecnol%C3%B3gicas+y+humanas+y+de+organizaci%C3%B3n%29+que+garanticen&hl=es&sa=X&ei=U0xTU4eLNYbLsATni4LwDg&ved=0CCsQ6AEwAA#v=onepage&q=Un

Asamblea Nacional Constituyente. (2008). Constitución de la República del Ecuador. Montecristi, Manabí, Ecuador: Registro Oficial 449 del 20 de octubre de 2008.

Bello, J. L. (Octubre de 2008). *sitio web de la Asosciación Española para la Calidad.* Recuperado el 13 de Agosto de 2013, de http://www.aec.es/c/document_library/get_file?uuid=99c086c1-9c20-4389-a9db-682ddbedc3c8&groupId=10128

Contraloría General del Estado. (14 de Diciembre de 2009). Normas Técnicas de Control Interno. *Normas Técnicas de Control Interno* . Quito, Pichincha, Ecuador: Registro Oficial Suplemento 87.

Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo. (2013). Reglamento de la Estructura Orgánica y Funcial de la EPMAPAP. Portoviejo, Manabí, Ecuador.

EPPS_*Services*_Ltd. (29 de Septiembre de 2013). Documentos sobre ISO 22301 BS 25999.

Gaspar Martínez, J. (2010). *El plan de continuidad de negocio Una guía práctica para su elaboración.* Recuperado el 12 de Agosto de 2013, de books.google.com.ec: http://books.google.com.ec/books?id=um1V2jADP78C&pg=PR2&dq=El+plan+de+continuidad+de+negocio+Una+gu%C3%ADa+pr%C3%A1ctica+para+su+elaboraci%C3%B3n&hl=es&sa=X&ei=D1JTU5uoA4G-sQSm6YDQCQ&ved=0CC0Q6AEwAA#v=onepage&q=Conjunto%20de%20estrategias%2C%20acciones%2C

Gaspar Martínez, J. (2004). *Planes de contingencia la continuidad del negocio en las organizaciones.* Recuperado el 12 de Agosto de 2013, de books.google.com.ec: http://books.google.com.ec/books?id=K_UMxjjB5gUC&printsec=frontcover&dq=Planes+de+contingencia+la+continuidad+del+negocio+en+las+organizaciones&hl=es&sa=X&ei=_k9TU8jOE8umsQT_jYHYAQ&ved=0CDYQ6AEwAA#v=onepage&q&f=false

Hoffer, J. (Enero de 2001). Recuperado el 12 de Agosto de 2013, de sitio Web de CBS Interactive Business Network Resoruce Library: http://archive.today/20120629133345/findarticles.com/p/articles/mi_m0DUD/is_1_22/ai_68864006

ISO 22301. (2012). Societal security - Business continuity management systems - Requirements.

ISO 27001. (Julio de 2011). Tecnología de la Información - Técnicas de Seguridad - Sistema de Gestión de la Seguridad de la Información (SGSI) - Requisitos.

Rodríguez Edith & Correa, D. (s.f.). *sitio web de Sisteseg.* Recuperado el 13 de Agosto de 2013, de http://www.sisteseg.com/files/Microsoft_Word_-_Articulo_BS_25999_DEF1.pdf

ABREVIATURAS Y ACRÓNIMOS

EPMAPAP	Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo
DRP	Plan de recuperación de desastres
SGCN	Sistema de Gestión de Continuidad del Negocio
TIC	Tecnología de la Información y Comunicaciones
TI	Tecnología de la Información
ISO	*International Organization for Standardization*
BS	*British Standard*
BCM	*Business Continuity Management*
BCMS	*Business Continuity Management System*
BIA	*Business Impact Analysis*
SGSI	Sistema de Gestión de Seguridad de la Información
DRAE	Diccionario de la Real Academia Española
DBMS	*Data Base Management System*
AFINANCIAL	Sistema informático contable – financiero
OLYMPO	Sistema informático contable - financiero
SQL	*Structure Query Language*
C#	Lenguaje informático de Programación
C Sharp	Lenguaje informático de Programación
ATHIE	Sistema informático de talento humano
AFLOW	Sistema informático administrativo
ABILLING	Sistema informático de facturación - comercial
RACI	*Responsible Accountable Consulted Informed*
GLP	*General Public License*
AIN	Análisis de Impacto al Negocio
R.O	Registro Oficial
MAO	*Maximum aceptable outage*
LCD	*Liquid Crystal Display*

GB	*GigaByte*
GHz	*GigaHertz*
POE	*Power Over Ethernet*
IP	*Internet Protocol*
AM	*Analog Modulation*
FM	*Frequency Modulation*
CAT	*Category*
CNEL	Corporación Nacional de Electricidad
TELCONET	
CNT	Corporación Nacional de Telecomunicaciones
ALTURA	
PETI	Plan Estratégico de Tecnología de la Información
USD	*United States Dollar*
ECU911	Servicio Integrado de Seguridad
SNGR	Sistema Nacional de Gestión de Riesgo
MSP	Ministerio Salud Pública
PROTELCOTELSA	Proveedor del sistema OLYMPO
MANTAREYS	Proveedor de páginas web
P/T	Ponderación / Total
UPS	*Uninterruptible Power Supply*
WEB	*Web Easy Builder*
CT	Calificación Total
PT	Ponderación Total
NC	Nivel de Confianza
RI	Riesgo Inherente
COSO	*Committee of Sponsoring Organizations*
CO2	Dióxido de Carbono
S/N	Sin / Número
RF	Rol Funcional
N/A	No / Aplica

MBCO	*Minimum Business Continuity Objective*
PTAR	Planta de Tratamiento de Aguas Residuales