DESARROLLO DE UN PLAN DE RECUPERACIÓN DE DESASTRES PARA LA UNIDAD DE TECNOLOGÍA DE LA EMPRESA PÚBLICA MUNICIPAL DE AGUA POTABLE Y ALCANTARILLADO DE PORTOVIEJO

José Loor

Universidad de las Fuerzas Armadas, Sangolquí, Ecuador
failuresystem83@hotmail.com

Resumen: Este artículo se basa en el desarrollo de un DRP para la Unidad de Tecnología de la Empresa Pública Municipal de Agua Potable y Alcantarillado de Portoviejo (EPMAPAP), con el objetivo de asegurar la continuidad de los procesos tecnológicos que sostienen las actividades comerciales y de servicio en esta entidad. Para el efecto, se revisaron tres estándares: ISO 27001, ISO 22301 y British Standard BS 25999, referidos a la continuidad del negocio; a los cuáles se les aplicó criterios para su selección, a fin de escoger aquel con mayor flexibilidad de adaptación a la realidad institucional, así como a la normativa legal a la que están sujetas las entidades públicas, cumpliendo en mayor porcentaje estos requisitos la norma ISO 22301.

Utilizando el estándar ISO 22301:2012 escogido mediante el cumplimiento de criterios de selección tales como flexibilidad de adaptación, actualización disponible, escalabilidad, independencia, impacto, sostenibilidad, entre otros, se desarrolló el DRP con el nivel de detalle especificado en el mismo y se lo adaptó a la realidad de la EPMAPAP, generándose los documentos entregables personalizados.

Se realizó un estudio de factibilidad sobre la implementación del DRP en la organización, el mismo que involucró la factibilidad técnica, operativa, legal y económica, obteniendo resultados positivos como: 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 además de las herramientas informáticas necesarias para la administración y recuperación las principales actividades de la entidad; estructura orgánica funcional que permite la toma de decisiones de forma oportuna; la normativa legal obligatoria tales como el literal i del reglamento orgánico funcional de la misma entidad, el apartado 410-11 de las normas de control interno emitidas por la Contraloría General del Estado y el artículo 389 y 390 de la Constitución de la República de Ecuador, que exigen la implementación de planes de recuperación; y el costo total de inversión vs. el valor de la caída concurrente de todos los sistemas informáticos que sustentan las operaciones la organización, siendo este último mucho más elevado que el costo de inversión; por esta razón, tomando en cuenta el estudio de factibilidad se recomienda la implementación del DRP desarrollado.

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

Abstract: This article is based on the development of a DRP for Unity Technology Public Company Municipal Water and Sewer Portoviejo (EPMAPAP), in order to ensure continuity of technological processes that support the business and service in this entity. To this end, we reviewed three standards: ISO 27001, ISO 22301 and BS 25999 British Standard, they related to business continuity; to what criteria were applied for selection, to choose that with greater flexibility to adapt to the institutional reality, as well as legal regulations that are subject to public entities, fulfilling these requirements in greater percentage ISO 22301.
Using the standard ISO 22301:2012 chosen by meeting criteria such as flexibility to adapt, update available, scalability, independence, impact, sustainability, among others, the DRP was developed to the level of detail specified in the same and adapted it to the reality of EPMAPAP, generating custom deliverables.
A feasibility study on the implementation of the DRP in the organization was conducted involving the same technical, operational, legal and economic feasibility, positive results as it has both the knowledge and skills of senior level management administrative and operational management levels of the computing tasks of the institution in addition to necessary for the administration and recovery the main activities of the organization tools; functional organizational structure to facilitate decision making in a timely manner; mandatory legal regulations such as the literal i of organic functional regulation of the same entity, section 410-11 of the Internal Control Standards issued by the Comptroller General and Article 389 and 390 of the Constitution of the Republic of Ecuador which require the implementation of recovery plans; and the total investment cost vs. the value of concurrent drop all computer systems that support the organization's operations, the latter being much higher than the investment cost; therefore, taking into account the feasibility study DRP implementation developed is recommended.

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

I. Introducción

Un DRP es definido por el sitio web de inBest como “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).

Según el sitio web de Balarezo Consultores describe que los planes de continuidad del negocio “permiten 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.).

Analizadas estas definiciones se establece 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.

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, que ayude a establecer lo que se debe hacer para asegurar en todo momento la funcionalidad de los sistemas informáticos importantes dentro de las unidades de Tecnología, y con esto la continuidad de los procesos críticos de la organización.

II. Metodología

Para la realización del trabajo, se partió de una investigación documental que permitió establecer con el nivel de detalle pertinente el estado del arte sobre la temática de los DRP.

A continuación se realizó un proceso de síntesis que definió el DRP. Paralelamente, se empleó como técnicas de campo la entrevista y la observación directa para identificar los procesos que deben se consideraron dentro del DRP y se desarrollaron los documentos que sustentan la actuación ante la presencia de incidentes disruptivos. Finalmente se realizó un análisis que justificó la factibilidad del DRP desarrollado.

A. Selección de la normativa a ser aplicada

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. Se evaluaron los siguientes estándares:

- British Standard BS 25999
- ISO 22301:2012 Seguridad de la sociedad – Sistemas de gestión de la continuidad de negocio. (ISO 22301, 2012)
- ISO 27001 Tecnología de la Información – Técnicas de Seguridad – Sistema de la Seguridad de la Información (SGSI). (ISO 27001, 2011)

B. Criterios de selección

Los criterios de selección que se utilizaron en el presente trabajo, ver Tabla 1, cumplen con la tarea de demostrar que norma se ajusta a la realidad institucional de la Unidad de Tecnología de la EPMAPAP, analizando entre otros factores su aplicabilidad y flexibilidad de implementación. Es necesario comprender los conceptos de aplicabilidad y flexibilidad, tal como los manifiesta la RAE, definiendo aplicar como “Emplear, administrar o poner en práctica un conocimiento, medida o principio, a fin de obtener un determinado efecto o rendimiento en alguien o algo” y flexible como “Susceptible de cambios o variaciones según las circunstancias o necesidades”, las fuentes de información utilizadas en las

definiciones fueron recuperadas desde Real Academia Española. (2001).Diccionario de la lengua española (DRAE)(22.ª ed.)

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%**

III. Evaluación de resultados

A. Documentación del DRP

En base a la norma seleccionada se desarrolló el DRP para la Unidad de tecnología de la EPMAPAP, cuyo contenido documental se lista a continuación:

- Política de continuidad de servicios tecnológicos
- Análisis del impacto en el negocio
- Cuestionario de análisis de impacto – Disponibilidad del servicio de comunicación
- Cuestionario de análisis de impacto – Disponibilidad del sistema comercial
- Cuestionario de análisis de impacto – Disponibilidad del sistema administrativo
- Cuestionario de análisis de impacto – Disponibilidad del sistema financiero
- Cuestionario de análisis de impacto – Seguridad de los sistemas de información
- Estrategia de continuidad de los servicios tecnológicos
- Prioridades de recuperación
- Objetivos de tiempo de recuperación
- Escenarios de incidentes disruptivos
- Plan de preparación para la continuidad de los servicios tecnológicos
- Estrategia de recuperación - Disponibilidad del servicio de comunicación
- Estrategia de recuperación - Disponibilidad del sistema comercial
- Estrategia de recuperación - Disponibilidad del sistema administrativo
- Estrategia de recuperación - Disponibilidad del sistema financiero

- Cuestionario de evaluación de control interno
- Calificación de la evaluación de control interno
- Matriz de evaluación de riesgos
- Matriz de tratamiento de riesgos
- Plan de continuidad
- Plan de respuesta a incidentes generales
- Registro de incidentes
- Ubicaciones estratégicas de continuidad
- Plan de transporte
- Registro de contactos
- Plan de recuperación - Disponibilidad del servicio de comunicación
- Plan de recuperación - Disponibilidad del sistema comercial
- Plan de recuperación - Disponibilidad del sistema administrativo
- Plan de recuperación - Disponibilidad del sistema financiero
- Formulario de informe de pruebas
- Plan de capacitación
- Formulario medidas correctivas
- Matriz RACI de responsabilidades

B. Pruebas pilotos

Con el desarrollo del DRP se realizaron los simulacros o pruebas pilotos a la unidad de servicios informáticos, con tres escenarios seleccionados para medir el grado de eficacia y aplicabilidad del plan.

Los escenarios aplicados fueron seleccionados de forma discrecional por el autor, en base a que la propuesta de diseño del DRP aún no se encuentra implementada.

Las pruebas pilotos realizadas fueron documentadas siguiendo el esquema que manda la norma ISO 22301:2012, mostrando un resumen en la Tabla 2.

Las pruebas pilotos se realizaron con éxito, 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.

TABLA 2: Detalle de las pruebas pilotos desarrolladas

#	Escenario	Acciones	Objetivos	Unidad afectada	Prueba anunciada	Medidas correctivas	Recomendaciones
1	Fallas en las telecomunicaciones	Seguimiento de acciones del DRP	Recuperar los servicios de telecomunicaciones dentro del menor tiempo	TIC y áreas usuarias	Sí	• Etiquetar los cables • Enlistar personal para mensajería	Adquisición de herramientas de monitoreo para los equipos de comunicación
2	Ataque de código malicioso	Seguimiento de acciones del DRP	Eliminación del código malicioso de los computadores	TIC y áreas usuarias	Sí	Se realiza el trámite para la renovación de las licencias del software antivirus	Colocar los sistemas informáticos en un servidor aparte para evitar infecciones que

							ingresen desde el internet
3	Interrupción del suministro eléctrico	Seguimiento de acciones del DRP	Recuperar el suministro de energía eléctrica en el menor tiempo	Toda la entidad	Sí	• Línea directa y números celulares de los contactos del proveedor	Mejorar el proceso de ejecución alternativa de actividades a fin agilizar los mismos.

C. Estudio de factibilidad

a. Factibilidad técnica

Una vez desarrollado el diseño del DRP para la Unidad de Servicios informáticos de la EPMAPAP se pudo determinar que si 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

b. Factibilidad operativa

La Unidad de Servicios Informáticos de 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, debido a su gran experiencia y empoderamiento de los procesos organizacionales que manejan; esta efectiva operabilidad coordinada con los procesos definidos en el manual de procesos organizacionales de la EPMAPAP permite la viabilidad operativa del DRP desarrollado.

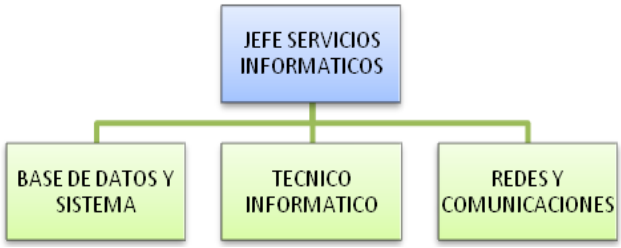

FIGURA 1: Estructura Orgánica Unidad de Servicios Informáticos EPMAPAP
Fuente: Reglamento de la Estructura Orgánica Funcional de la EPMAPAP 2013

c. Factibilidad legal

El literal i del Reglamento de la Estructura Orgánica y Funcional de la EPMAPAP 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 410-11de 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)

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…".

"**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…" (Asamblea Nacional Constituyente, 2008)

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.

d. 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 2, que refleja claramente la factibilidad económica del DRP desarrollado para la organización.

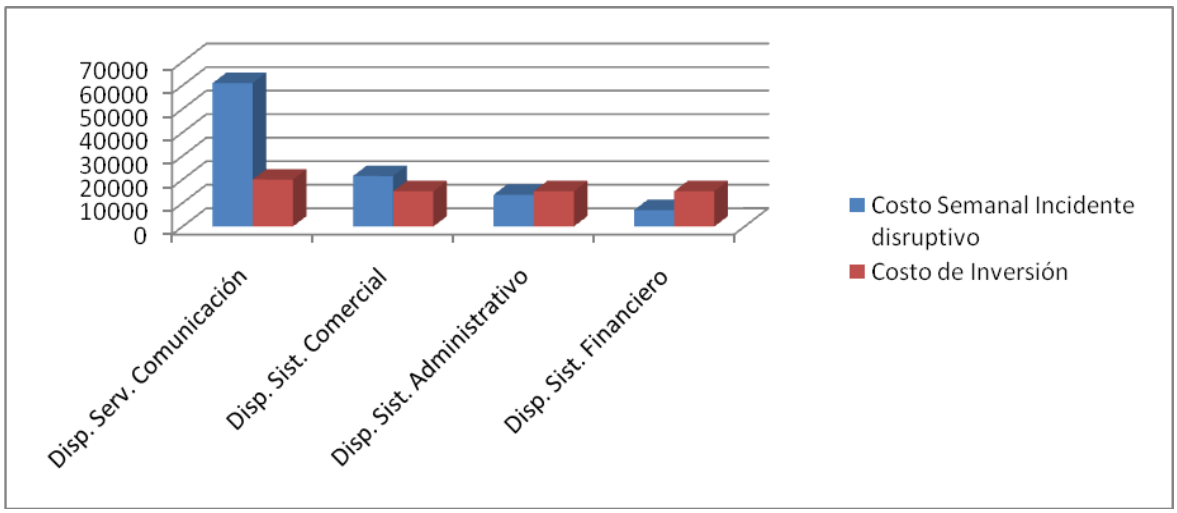

FIGURA 2: Cuadro estadístico comparativo de costo de pérdida vs. costo de inversión

IV. Trabajos relacionados

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.

El presente artículo pretende difundir este tipo de recurso en entidades estatales a fin de que sirva como iniciativa para el resto de instituciones públicas de la provincia y del país, a la vez de cumplir con la normativa legal vigente impuesta por los entes de control.

V. Conclusiones y trabajo futuro

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, fue la mejor opción (solución) para desarrollar el plan de recuperación de desastres para la unidad de servicios informáticos de la EPMAPAP, por haber cumplido con el mayor puntaje en cuanto a los criterios de selección aplicados durante el desarrollo del estudio, 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, tales como: el bajo costo de inversión vs. el valor de la caída concurrente de todos los sistemas informáticos que sustentan las actividades de la entidad, la normativa legal entre las que se puede mencionar la constitución de la República del Ecuador, las normas de control interno de la Contraloría General del Estado y el propio reglamento interno de la institución, que obliga la implementación de planes de recuperación, entre otras, 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.

Como trabajo futuro se sugiere el seguimiento como caso de estudio la implementación tanto del DRP como de la continuidad del negocio en toda la organización. Además se sugiere la implementación total de la norma ISO 22301:2012 seleccionada y de ser posible su combinación con otras normas o estándares tales como la ISO 27001, en todas las direcciones departamentales, para conseguir continuidad del negocio en la organización.

Referencias Bibliográficas

(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 inBest: http://inbest.me/que-es-un-drp

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. 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.

Española, R. A. (2001). Diccionario de la lengua española (DRAE)(22.a ed.). Madrid, España.

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