ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

PROCEDIMIENTO DE IMPLEMENTACIÓN DE LOS PROCESOS DE GESTIÓN DE LA PRESTACIÓN DE LOS SERVICIOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN (TI), BASADO EN EL ESTÁNDAR COBIT Y BUENAS PRÁCTICAS ITIL

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MÁSTER (MSc) EN GESTIÓN DE LAS COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

MARCO ANTONIO OCHOA MORENO

mochoa@eppetroecuador.ec

DIRECTOR: FRANCISCO HALLO

francisco.hallo@epn.edu.ec

Quito, Junio 2012

DECLARACIÓN

Yo, Marco Antonio Ochoa Moreno, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Marco Antonio Ochoa Moreno

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Marco Antonio Ochoa Moreno, bajo mi supervisión.

Ing. Francisco Hallo

DIRECTOR DE PROYECTO

CONTENIDO

FIGURAS

CUADROS

RESUMEN

Esta Tesis es producto de la necesidad de mejorar la Gestión de las Comunicaciones y Tecnologías de la Información (TI) en las Instituciones, en lo referente al Plan de Continuidad de Servicios Críticos de TI, porque las operaciones empresariales dependen cada vez más de la continuidad de dichos Servicios. Para comprobar si esta Tesis aportó o no a la satisfacción de dicha necesidad, se realizó un caso de estudio en la Unidad de Sistemas de PETROECUADOR, donde se definió, desarrolló y probó con éxito el Plan antes citado.

Para este fin se describió en forma didáctica y utilizó a COBIT estándar de facto para el Gobierno de TI alineado al Gobierno Corporativo, así como también, a ITIL conjunto de buenas prácticas de TI y al Cuadro de Mando Integral. Lo cual ha permitido desarrollar de inicio a fin dicho Plan, considerando para ello el impacto de las interrupciones sobre la Institución, los riesgos a los cuales están expuestos, el acuerdo de nivel de servicio que lo respalda, los escenarios anterior, durante y posterior a una situación de emergencia, las pruebas periódicas del Plan, y las conclusiones y recomendaciones fundamentadas en los resultados obtenidos.

El Plan fue probado y aplicado en la Unidad de Sistemas de PETROECUADOR, logrando recuperarse sin pérdida de datos a todos los Servicios Críticos de TI, en las diferentes fechas en que hubo la necesidad de recurrir a él, razón por la cual dicha Unidad lo tomará como punto de partida para definir y elaborar el Plan de Continuidad para todos sus Servicios de TI.

Por la utilidad que prestaría el Plan a las Instituciones que se encuentren interesadas en definir, desarrollar e implantar un Plan de Continuidad de Servicios Críticos de TI, se invita a leer esta Tesis para que encuentren en ella una guía clara y sencilla para lograrlo.

La descripción didáctica y la utilidad del Plan de Continuidad de Servicios Críticos de TI, han permitido y permitirán contribuir al fortalecimiento de la Gestión de TI.

PRESENTACIÓN

Esta Tesis se ha denominado "Procedimiento de Implementación de los Procesos de Gestión de la Prestación de los Servicios de las Tecnologías de la Información (TI), basado en el estándar COBIT y buenas prácticas ITIL"[1], cuyo Objetivo General es "*Describir en forma didáctica a COBIT e ITIL como estándar y buenas prácticas de TI respectivamente, integrarlos para la gestión de la entrega de servicios de TI, desarrollar un caso de estudio para demostrar que sí se obtienen beneficios de la integración y desarrollar un Procedimiento de Implementación del Proceso de Gestión de la Continuidad de los Servicios de Tecnologías de la Información (TI), resultante del correspondiente análisis costo-beneficio*" [1], y en su contenido se encontrará la siguiente temática:

Una breve descripción didáctica de COBIT e ITIL, considerando:

- Al Gobierno de TI fundamentado en COBIT e ITIL; y

- La Integración de COBIT e ITIL para la gestión de la Entrega de Servicios de IT

Un caso de estudio que permitió demostrar:

- Al "Procedimiento de Implementación del Proceso de Gestión de la Continuidad de los Servicios de Tecnologías de la Información", que conforme COBIT lo establece, pertenece al Proceso "DS4 Garantizar la Continuidad del Servicio" [2].

- Los beneficios de la integración y la correspondiente observación de los resultados obtenidos.

---

[1] OCHOA, Marco, Plan de Tesis elaborado en el Formulario para la presentación del plan de tesis de magister de la Escuela Politécnica Nacional, Coordinación de Postgrado: Maestría Gestión de las Comunicaciones y Tecnologías de la Información, Quito-Ecuador, 2006, p.1, 14 p.

[2] IT Governance Institute, COBIT 4.0, ITGI, U.S.A., 2005, ISBN 1-933284-37-4, p. 26, 201 p.

El caso de estudio se lo realizó en la Empresa Estatal Petróleos del Ecuador (PETROECUADOR), siendo la Unidad de Sistemas la dependencia que se benefició de la respectiva integración de COBIT e ITIL.

Esta temática desarrollada en lenguaje natural, permitirá conocer el marco de referencia de COBIT e ITIL, para comprender que sí podrían contribuir a Garantizar la Continuidad del Servicio de las TI, que es uno de los 34 procesos con los que COBIT pretende lograr el gobierno, control y auditoría de las TI, en las instituciones que apliquen dicho marco de referencia que se complementa con el de ITIL. Se han utilizado elementos que generalmente están al alcance de las dependencias responsables de la Administración de las TI en las Instituciones. La información más reciente sobre estos marcos de referencia para el gobierno de las TI se puede consultar en **www.isaca.org/cobit** y **www.itil-live-portal.com**.

CAPÍTULO 1. GOBIERNO DE TI FUNDAMENTADO EN COBIT E ITIL

El Gobierno Corporativo establece los objetivos de la Institución y los medios para alcanzarlos. El Gobierno de TI mantiene una adecuada alineación estratégica, crea valor, administra riesgos y recursos, evalúa el desempeño del personal, y provee información útil para dueños, autoridades, personal, clientes y proveedores. Ambos gobiernos trabajan para cumplir metas que aseguren que se están alcanzando los objetivos y la visión institucional.

La metodología utilizada en esta investigación, fue la Deductiva e Inductiva que permitió ir de lo general a lo particular y viceversa, apoyada en Técnicas y Procedimientos para de recolección, análisis, entrevistas y observación, mediante la cual se logró generar este aporte al Gobierno de TI y a la Gestión de la Continuidad de los Servicios de TI, sobre la base del conocimiento y entendimiento obtenido. A continuación se presentan conceptos, ideas, etc., que se desarrollan usando el caso de estudio como medio de facilitar la comprensión.

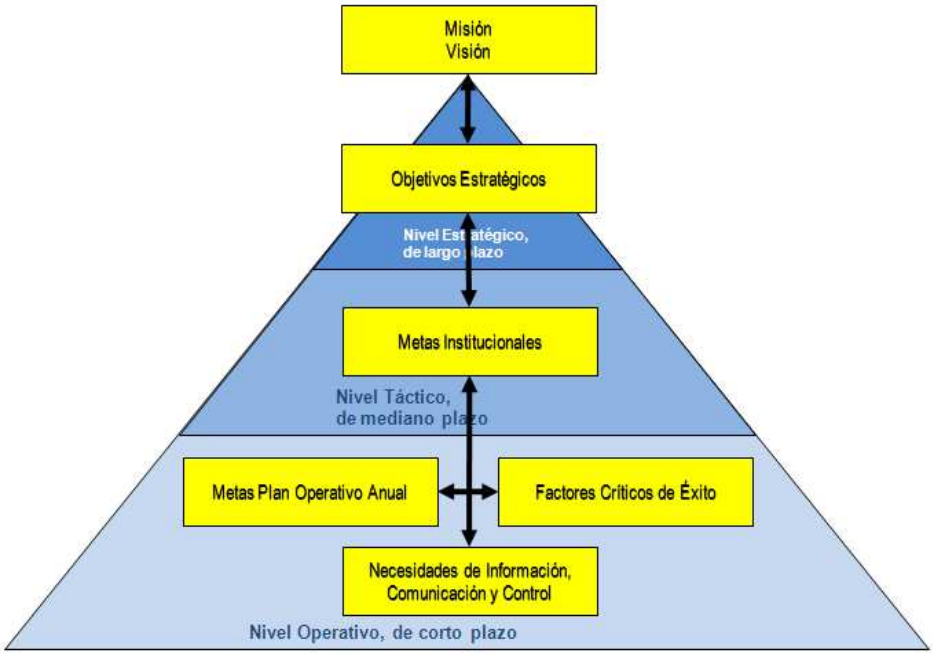


Figura 1. Método de “Factores Críticos de Éxito (FCE)”.

La Misión Institucional: "*Misión es el propósito o razón por la que la organización existe y lo que la organización debe hacer*"[3].

La Misión Institucional de PETROECUADOR se transcribe: "*Empresa estatal que genera riqueza para los ecuatorianos mediante la exploración, explotación, transporte, industrialización y comercialización de hidrocarburos, con recurso humano idóneo y comprometido con el desarrollo del país*" [4].

La Visión Institucional: "*Visión es un enunciado breve que expresa el estado futuro deseado de una manera realista y posible de alcanzar*" [3].

La Visión Institucional se cita: "*PETROECUADOR será líder regional en la industria, manteniendo óptimos niveles de rentabilidad en sus operaciones, aplicando tecnología adecuada, realizando buenos negocios, protegiendo siempre al ambiente, favoreciendo el desarrollo comunitario, siendo una empresa con recurso humano con alto nivel de motivación y compromiso, y gestionando con transparencia y pulcritud, con lo cual espera ser competitiva a nivel internacional , que satisface con su producción la demanda nacional de hidrocarburos; y está comprometida con la preservación ambiental*" [3].

El Objetivo Estratégico Institucional: "*Objetivo es un enunciado breve que definen los resultados esperados por la Institución, que establecen las bases para la medición de los logros obtenidos*" [3].

El Objetivo Estratégico de PETROECUADOR en materia de TI es "*Reestructurar Organizacional y Tecnológicamente la Gestión Empresarial de PETROECUADOR*" [5].

---

3 e-Strategia Consulting Group, Empresa por resultados, San Pedro Garza, México, 1999-2008, pp. 35, 38, 41, 76 p.

4 Presidente Ejecutivo, Plan Estratégico Corporativo 2008-12 de PETROECUADOR y sus Empresas Filiales, aprobado por el señor Presidente de la República el 2008-02-25, Quito-Ecuador, 158 p., p. 4. Noticia: Revista Petróleo Actualidad, año 8, No.7, marzo 2008.

5 Ibid., p. 88.

Las Metas Institucionales son la cuantificación del avance requerido para el cumplimiento de cada uno de los Objetivos dentro de cada período planificado a mediano y largo plazo.

La Meta de PETROECUADOR en materia de TI es "*Implementar el Sistema Integrado de Información*"[4], conforme a lo establecido en el Plan Operativo Anual.

Las Metas del Plan Operativo Anual son resultado de la evaluación del cumplimiento de los Objetivos Estratégicos Institucionales, cuyas desviaciones y gaps deben corregirse en el menor tiempo posible, a fin de evitar el retraso o incumplimiento de los mismos.

Las Meta de PETROECUADOR en su Plan Operativo Anual para el área de competencia de TI, se transcribe: "*13. Definición e incorporación al 30% la Plataforma Tecnológica que apalanque la integración, consolidación, ejecución, monitoreo y cumplimiento del Plan Estratégico y Operativo del Sistema PETROECUADOR, con el Presupuesto de US$600.000,0*, *bajo la responsabilidad de la Gerencia Administrativa (GAD)*" [6].

Las Necesidades de Información, Comunicación y Control Institucionales son responsabilidad del Gobierno de TI, porque con ellas las TI apalancan el cumplimiento de las Metas y Objetivos Institucionales.

Las Necesidades de Información, Comunicación y Control de PETROECUADOR son una adecuada Administración del Cambio que asegure la motivación y el empoderamiento del personal, una Estructura Matricial que asegure el cumplimiento de metas y objetivos, y un Sistema Integrado de Información que apalanque el mejoramiento continuo de la gestión Institucional. En consecuencia, la Unidad de Sistemas responsable del Gobierno de TI se alinea a dichas necesidades mediante un estándar como COBIT ("Objetivos de Control para la Información y Tecnologías Afines) y buenas prácticas como las de ITIL (Biblioteca

[6] Directorio de PETROECUADOR, Resolución No. 09-DIR-2008-01-16: aprobación del Presupuesto y plan Operativo 2008, Quito-Ecuador, 1 p.

de infraestructura de TI), para apalancarlas con herramientas idóneas de organización por procesos un Business Process Management Corporativo y de TI, de un sistema integrado y consolidado un Enterprise Resource Planning (ERP), de tablero de mando una metodología automatizada de Empresa Por Resultados (EPR), etc., que son productos y servicios de calidad que contribuyen al cumplimiento de plazos, costos y beneficios estimados. Tan solo el monitoreo permanente del cumplimiento de las metas puede asegurar su cabal cumplimiento.

Los Factores Críticos de Éxito:

Figura 2. Factores Críticos de Éxito

Los Factores Críticos de Éxito en PETROECUADOR entre otros, son las decisiones oportunas de los ejecutivos y su respaldo incondicional para el logro de las metas y objetivos Institucionales, lo cual asegura tanto la disponibilidad a tiempo de los recursos de TI, como el cumplimiento de plazos, costos y beneficios estimados planificados.

A continuación se describe a COBIT e ITIL porque son el estándar y las buenas prácticas de las TI, respectivamente, razón por la cual son importantes para lograr que el mensaje contenido en esta Tesis llegue a sus lectores. Los términos técnicos están acompañados de su significado y además se los define en el Glosario.

COBIT

El Instituto de Gobierno de IT (IT Govenance Institute ITGI) de Estados Unidos de Norte América investigó a nivel internacional en más de 40 documentos entre ellos estándares, marcos de referencia y mejores prácticas, tendientes a garantizar la probidad de COBIT para la resolución de todas las áreas de las TI en las Instituciones. Para la versión COBIT 4.0 contó con la valiosa contribución de las siguientes organizaciones:

1. El Comité de organizaciones patrocinadoras de la Comisión Treadway (COSO): Control Interno—Marco de trabajo integrado, 1994 Administración de riesgos empresariales—Marco de trabajo integrado, 2004.
2. La Oficina de Comercio Gubernamental (OGC®): Biblioteca de infraestructura de IT® (ITIL®), 1999-2004.
3. La Organización internacional para la estandarización: ISO/IEC 17799:2005, Código de prácticas para la administración de la seguridad de la información.
4. El Instituto de Ingeniería de Software (SEI®): SEI Modelo de madurez de la capacidad (CMM®), 1993 SEI Integración del modelo de madurez de la capacidad (CMMI®), 2000.
5. El Instituto de administración de proyectos (PMI®): Cuerpo de conocimiento de administración de proyectos (PMBOK®), 2000.
6. El Foro de seguridad de información (ISF): El estándar de buenas prácticas para la seguridad de la información, 2003.

COBIT considera cinco áreas de Gobierno de TI: Alineación estratégica, Creación de Valor, Administración de Riesgos, Administración de Recursos y Evaluación de Desempeño, que las cubre mediante los cuatro dominios de la siguiente cadena de valor:

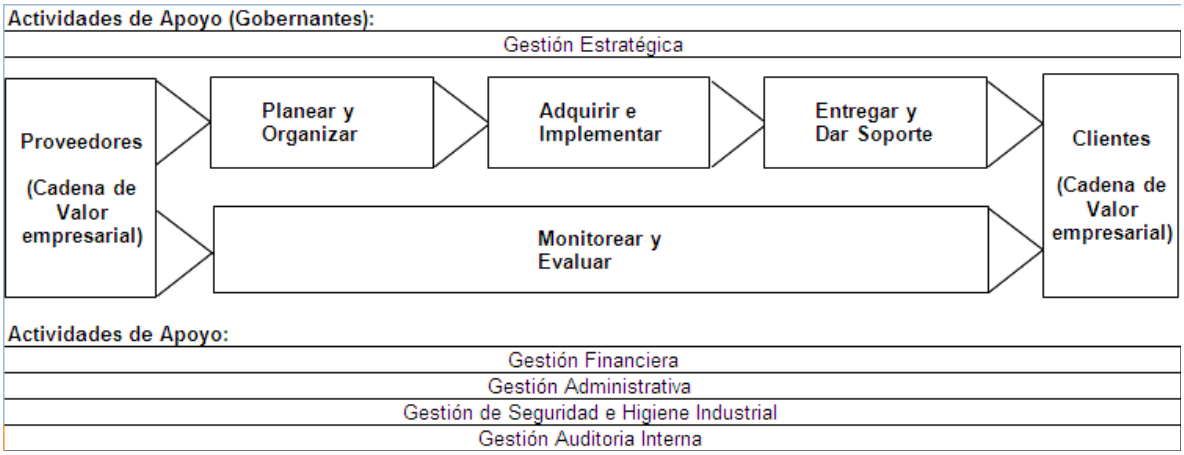


Figura 3. Cadena de Valor de TI

COBIT fundamenta la capacidad técnica de las TI en la disponibilidad de cuatro recursos internos y/o externos mediante los cuales se logra la satisfacción de las Necesidades de Información, Comunicación y Control Institucionales:

- ✓ Las habilidades de las personas;
- ✓ La información en todas sus formas;
- ✓ La infraestructura que incluye a toda la tecnología requerida para la prestación de los servicios de TI, tales como, redes, sistemas, bases de datos, instalaciones, equipos auxiliares, etc.; y,
- ✓ Las aplicaciones que automatizan procedimientos que apalancan a la prestación de tales servicios, así como, a las tareas cuotidianas del personal.

COBIT actúa como un integrador que permite la identificación y utilización de herramientas idóneas de TI para la satisfacción de las Necesidades de Información, Comunicación y Control Institucionales, porque tiene una visión global del Gobierno de TI que asegura el alineamiento al Gobierno Corporativo, mediante una estructura de 34 procesos, tareas, métricas y modelo de madurez, a cargo de sus respectivos dueños, sin embargo hay que considerar que:

- Los dueños de la Institución y autoridades demandan un mejor retorno de las inversiones de TI.

- Existe preocupación por el incremento de gastos en las TI y por la consiguiente necesidad de reducir o mantener los costos, adoptando herramientas idóneas que eviten el desplazamiento de personal y que se constituyan en soluciones estándares a mediano y largo plazo, posibilitando mediante la mejora continua el desarrollo personal e Institucional.

- Hay que cumplir y hacer cumplir la normativa vigente, y satisfacer los requerimientos Institucionales y de organismos de control; así como, las políticas que transparentan las operaciones.

- Es necesario medir, monitorear y mejorar las actividades críticas de TI para incrementar el valor que TI entrega a la Institución; así como para, asegurar la continuidad de los servicios de TI y de las operaciones de la Institución, además lo es para el oportuno cumplimiento de las metas y la evaluación de desempeño, que permite la comparación con sus pares y contra estándares generalmente aceptados.

- Es necesario un marco de referencia para el Gobierno y control de TI, porque tiene un impacto importante en el destino de la Institución, por su aporte significativo al logro de las metas.

- Los servicios que TI provea a la Institución deben contribuir a:

    - La eficacia en la entrega de la información que la Institución necesita para su gestión, crecimiento y desarrollo, así como para el cumplimiento de la normativa vigente y de exigencias de los organismos de control.

    - La eficiencia en la utilización de los recursos para la obtención de la información que la Institución necesita.

- La confidencialidad establecida en la clasificación de la información, que asegure la diseminación selectiva de la información, evitando así el acceso no autorizado a la misma.

- La integridad de la información garantizándose que provenga de una sola fuente, exacta, completa y válida.

- La disponibilidad de la información, para la realización de las tareas y procesos; así como, para el logro gradual de metas, objetivos y la misión de la Institución.

- La conformidad dada por el cabal cumplimiento de la normativa vigente.

- La confiabilidad en la información disponible, respaldada por marcos de referencia generalmente aceptados; así como, por el proceso de mejoramiento continuo.

- Al control para optimizar el uso de los recursos y asegurar que se alcancen gradualmente las metas de TI y de la Institución, este es el principal beneficio de implementar COBIT como marco de referencia para el Gobierno de IT.

- Los recursos de TI que COBIT considera en su marco de referencia son:

    - Las personas requeridas para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, o externas por outsourcing o contratadas, de acuerdo a como se requieran.

- La información que son los datos en todas sus formas de entrada, procesados y generados por las aplicaciones y sistemas de información que son utilizados por la Institución.

- Las aplicaciones que incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

- La infraestructura son las instalaciones y la tecnología que incluye redes, hardware, software, sistemas operativos, sistemas de administración de base de datos, multimedia, etc., así como el sitio donde éstas se encuentran y los ambientes en los que operan, que es la que sustenta y apalanca a los otros tres recursos.

Los beneficios de implementar COBIT como marco de referencia de Gobierno de TI son:

- ✓ La alineación de TI a las Necesidades de Información, Comunicaciones y Control Institucionales.
- ✓ La total transparencia de las operaciones de TI, implementada mediante procesos debidamente definidos, ejecutados y controlados por sus dueños y autoridades, que son generalmente aceptados dentro y fuera de la Institución.
- ✓ Una visión compartida entre todos los participantes, con base en un lenguaje común.
- ✓ El cumplimiento de los requerimientos COSO que asegura el cabal establecimiento y cumplimiento del Sistema de Control Interno de la Institución.

		Áreas Gobierno Corp.						Áreas Gobierno TI					Criterios de Información							Recursos			
Dominio	**Proceso**	Control Mediambiente	Administr. Riesgos	Control Actividades	Inform. y Comunición	Monitoreo	Importancia	Alineación Estratégica	Creación Valor	Administr. Recursos	Administr. Riesgos	Evalluac. Desempeño	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	RRHH	Información	Aplicaciones	Infraestructura e Inst.
Planeación y Organización de TI																							
PO1	Definir el Plan Estratégico en función del Plan Institucional		P		S	S	A	P		S	S		P	S						✓	✓	✓	✓
PO2	Definir la Arquitectura de Información			P	P		B	P	S	P	S		S	P	S	P					✓	✓	
PO3	Determinar la Dirección Tecnológica		S	P	S		M	S	S	P	S		P	P								✓	✓
PO4	Definir Procesos, Organización y Relaciones	P			S	S	B	S		P	P		P	P						✓			
PO5	Administrar la Inversión		S	P			M	S	P	S		S	P	P					S	✓		✓	✓
PO6	Comunicar el Gobierno de TI y la Administración de	P			P		M	P			P		P					S		✓	✓		
PO7	Administrar Recursos Humanos	P			S		B	P		P	S	S	P	P						✓			
PO8	Administrar Calidad	P		P	S	P	M	P	S		S		P	P		S			S	✓	✓	✓	✓
PO9	Evaluar y Administrar Riesgos		P				A	P			P		S	S	P	P	P	S	S	✓	✓	✓	✓
PO10	Administrar proyectos	S	S	P		S	A	P	S	S	S	S	P	P						✓		✓	✓
Adquisición e Implementación																							
AI1	Identificar Soluciones Automatizadas			P			M	P	P	S	S		P	S								✓	✓
AI2	Adquisición y Mantener Software de Aplicación			P			M	P	P		S		P	P		S			S			✓	
AI3	Adquirir y Mantener infraestructura de Tecnología			P			B			P			S	P		S	S						✓
AI4	Habilitar la operación y el uso			P	S		B	S	P	S	S		P	P		S	S	S	S	✓		✓	✓
AI5	Asignar los Recursos			P			M		S	P			S	P				S		✓	✓	✓	✓
AI6	Administrar Cambios		S	P		S	A		P	S			P	P		P	P		S	✓	✓	✓	✓
AI7	Instalar y Acreditar Soluciones y Cambios			P	S	S	M	S	P	S	S	S	P	S		S	S			✓	✓	✓	✓
Servicios y Soporte																							
DS1	Definir y Administrar Niveles de Servicio	S		P	S	S	M	P	P	P		P	P	P	S	S	S	S	S	✓	✓	✓	✓
DS2	Administrar Servicios de Terceros	P	S	P		S	B		P	S	P	S	P	P	S	S	S	S	S	✓	✓	✓	✓
DS3	Administrar Desempeño y Capacidad			P		S	B	S	S	P	S	S	P	P			S					✓	✓
DS4	Asegurar Servicio Continuo	S		P	S		M	S	P	S	P	S	P	S			P			✓	✓	✓	✓
DS5	Garantizar la Seguridad de Sistemas			P	S	S	A				P				P	P	S	S	S	✓	✓	✓	✓
DS6	Identificar y Asignar Costos			P			B		S	P		S		P					P	✓	✓	✓	✓
DS7	Educar y Capacitar Usuarios	P			S		B	S	P	S	S		P	S						✓			
DS8	Asistir a los Clientes de TI	S			P	P	B		P			S	P	P						✓		✓	
DS9	Administrar la Configuración			P			M		P	P	S		P	S			S		S		✓	✓	✓
DS10	Administrar Problemas			P	S	S	M		P		S	S	P	P			S			✓	✓	✓	✓
DS11	Administrar Datos			P			A		P	P	P					P			P		✓		
DS12	Administrar el Ambiente Físico		S	P			B			S	P					P	P						✓
DS13	Administrar Operaciones			P	S		B			P			P	P		S	S			✓	✓	✓	✓
Monitoreo																							
M1	Monitorear y Evaluar el Desempeño de TI				S	P	A	S	S	S	S	P	P	S	S	S	S	S	S	✓	✓	✓	✓
M2	Monitorear y Evaluar el Control Interno					P	M		P		P		P	P	S	S	S	S	S	✓	✓	✓	✓
M3	Asegurar el Cumplimiento de Requerimeintos Externos			P	S	S	A	P			P							P	S	✓	✓	✓	✓
M4	Gobernar TI	P	S		S	P	A	P	P	P	P	P	P	P	S	S	S	S	S	✓	✓	✓	✓

Cuadro1. Los 34 Procesos de COBIT

ITIL

La Librería de Infraestructura de IT (ITIL), que está disponible en su tercera versión fue creada por la Office of Government Commerce (OGC) a partir de 2005-08, preservando los fundamentos (core) de ITIL, la misma que finalizó en 2006-12 y se publicó en 2007-02, en cinco libros con sus respectivas guías complementarias: Estrategia de Servicios o Service Strategies, Diseño de servicios o Service Design, Transición de Servicios o Service Transition, Operación de Servicios o Service Operation & Mejora Continua de Servicios o Continual Service Improvement; y que además cuenta con los siguientes libros de valor agregado:

- ✓ Introducción, Vista General, Contexto;
- ✓ La Administración de Servicios como una Práctica
- ✓ Ciclo de Vida del Servicio
- ✓ Rol de los Procesos en el Ciclo de Vida
- ✓ Rol de las Funciones en el Ciclo de Vida
- ✓ Fundamentos de la Práctica
- ✓ Principios de la Práctica
- ✓ Procesos
- ✓ Diseño y Estructuras Organizacionales, Roles y Responsabilidades
- ✓ Retos, Factores Críticos de Éxito, Riesgos
- ✓ Guía Suplementaria
- ✓ Referencias

El libro Estrategia de Servicios es el primero del Ciclo de Vida del Servicio, cubre un conjunto de metas y expectativas que aseguran que la Estrategia de IT considere debidamente:

- ✓ La Práctica de Administración de Servicios
- ✓ Los Principios de Servicio:
  - o Los Activos de Servicio, Tipos de Proveedores, Estructuras, Fundamentos
- ✓ La Estrategia de Servicios
- ✓ La Economía “Economics” de Servicios:
  - o La Administración Financiera de IT
  - o El Retorno de Inversión
  - o La Administración de Portafolio de Servicios
  - o La Administración de la Demanda
- ✓ La Estrategia y Cultura Organizacional, Tecnología y Operaciones

El libro Diseño de Servicios es el segundo del Ciclo de Vida del Servicio, inicia con un conjunto de requerimientos nuevos o cambiados y termina con el desarrollo de una solución diseñada para alcanzar las necesidades documentadas del Negocio:

- ✓ Los Principios de Diseño de Servicios
- ✓ Los Procesos de Diseño de Servicios:
  - o La Administración del Catálogo de Servicios
  - o La Administración de Niveles de Servicios
  - o La Administración de la Capacidad
  - o La Administración de la Disponibilidad
  - o La Administración de la Continuidad de Servicios
  - o La Administración de la Seguridad de la Información
  - o La Administración de Proveedores
- ✓ La Actividades Relacionadas
  - o La Administración de Aplicaciones
  - o La Administración de Datos e Información
  - o La Ingeniería de Requerimientos
- ✓ Las Consideraciones para el Diseño de Servicios (Organización, Proceso y Herramientas)

El libro Transición de Servicios es el tercero del Ciclo de Vida del Servicio, se ocupa de la administración de cambios, riesgos y aseguramiento de la calidad y tiene como objetivo implementar diseños de servicios de manera que la Operación de Servicios pueda administrar los siguientes servicios e infraestructura de una manera controlada:

- ✓ Los Principios de Transición de Servicios
- ✓ Los Procesos de Transición de Servicios:
  - o La Planeación y Soporte a la Transición
  - o La Administración de Cambios
  - o La Administración de Activos y Configuración de Servicios
  - o La Administración de Liberaciones y Despliegues
  - o La Validación y Prueba de Servicios
  - o La Evaluación
  - o La Administración del Conocimiento
- ✓ El Sistema de Administración de la Configuración

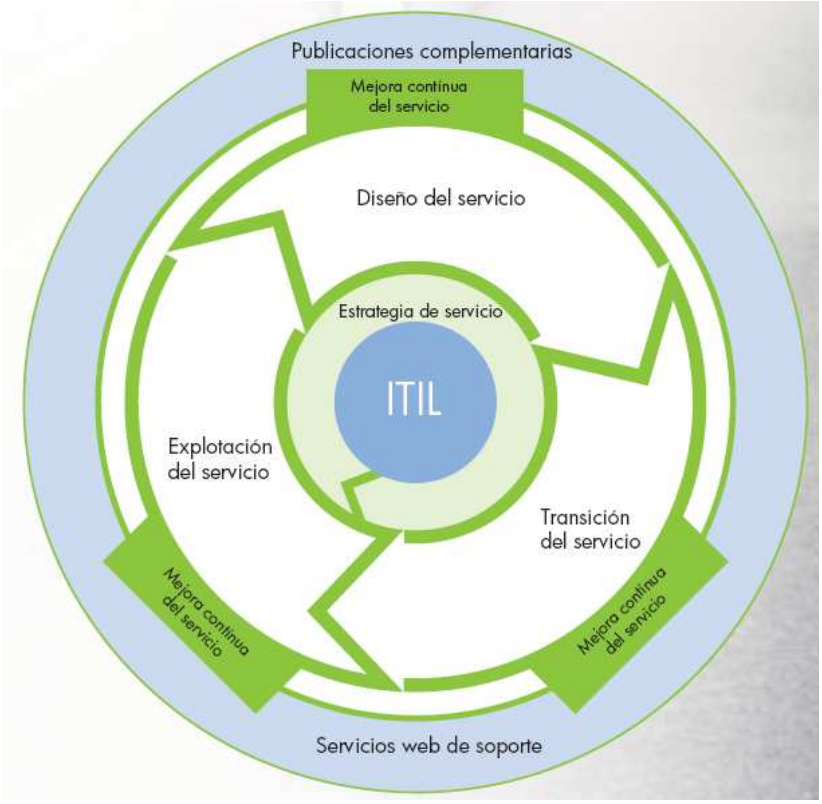
El libro Operación de Servicios es el cuarto del Ciclo de Vida del Servicio, se ocupa de las siguientes actividades cotidianas del Negocio:

- ✓ Principios de Operación de Servicios
- ✓ Procesos de Operación de Servicios:
  - o Administración de Eventos
  - o Administración de Incidentes
  - o Ejecución de Requerimientos
  - o Administración de Problemas
  - o Administración de Accesos
- ✓ Funciones:
  - o Mesa de Servicios
  - o Administración Técnica
  - o Administración de Operaciones IT
  - o Administración de Aplicaciones

El libro Mejora Continua de Servicios es el quinto del Ciclo de Vida del Servicio, contiene una visión integral de los siguientes elementos y busca maneras en las cuales el proceso general y la provisión de servicios pueden ser mejorados:

- ✓ Principios y Fundamentos de Mejora Continua
- ✓ Procesos de Mejora Continua:
  - o Los 7 Pasos del Proceso de Mejora
  - o Reporte de Servicios
  - o Medición de Servicios
  - o Retorno de Inversión (ROI) para MCS
  - o Preguntas de Negocio para MCS
  - o Administración de Niveles de Servicio y Mejora de Servicios
- ✓ Métodos y Técnicas de MCS: Evaluaciones, Benchmarking, Modelos de Medición (SWOT, Balanced Score Card)

ITIL ayuda a elegir cuidadosamente todos los recursos de TI, de modo que estén totalmente integrados y aporten capacidades que se ajusten a los mapas de procesos de alto nivel, para evitar la resistencia de la organización, de modo que el personal de IT pueda llevar a cabo una transición de los procesos sin interrupciones, aplicando el enfoque de la implementación: "cómo conseguirlo" y "cómo hacer que funcione"[7].



Fuente: © Pink Elephant, 2006. Todos los Derechos Reservados.
ITIL® es una marca registrada de la OGC (Office of Government Commerce).

Figura 4. ITIL

COBIT e ITIL

Ambos sustentan procesos, recursos, criterios de información, relaciones, etc., que atraviesan por empresas, unidades de negocio y dependencias; que son comunes en las Instituciones; pero inter dependientes entre la Institución, clientes

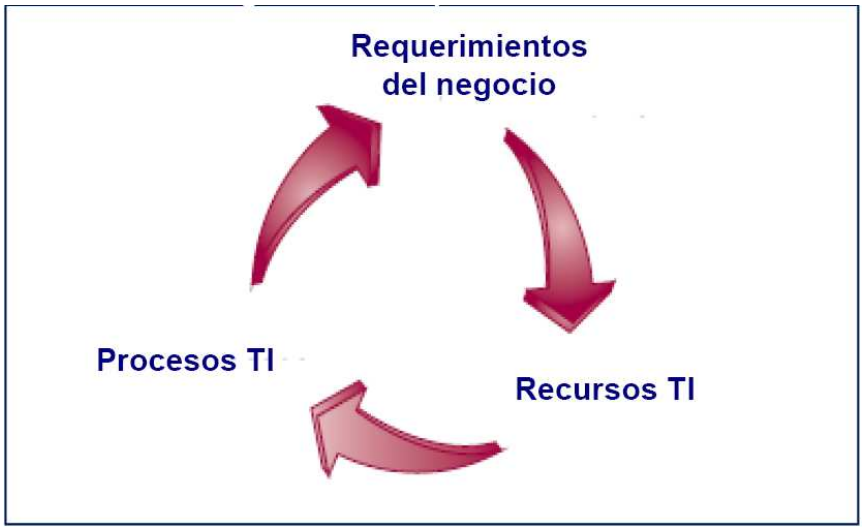
[7] FLORES José Manuel, Director de Servicios y Consultoría, Integrando TI al negocio a través de las Mejores Prácticas de ITIL, Pink Elephant LAM, 2007, p. 51, 68 p.

y usuarios, cuyas expectativas deben ser balanceadas, ya que los usuarios son quienes usan los servicios diariamente por lo que demandan alta disponibilidad y los clientes que son los que pagan por los servicios de IT necesitan confiabilidad.

La orientación a procesos y la aplicación de modelos de mejoramiento contínuo tales como el Círculo de Control de Ishikawa y el Ciclo de Deming:

- Planear - ¿Qué se debe hacer, cuándo, quién debe hacerlo, cómo y utilizando qué?
- Hacer - se llevan a cabo las actividades programadas
- Verificar - determinar si las actividades dan los resultados esperados
- Actuar - ajustar los planes basándose en la información recogida al verificar (Check).

El Principio básico de Cobit e ITIL demuestran su total alineación a los objetivos de la Institución:



Fuente: Cobit 4.0 Objetivos de Control, Directrices Gerenciales, Modelos de Madurez, p.13.

Figura 5. Mejoramiento Continuo

La prestación de Servicios de IT se fundamenta en la integración de COBIT e ITIL, porque en conjunto aseguran la satisfacción de las “Necesidades de Información, Comunicación y Control Institucionales.

Por lo expuesto COBIT es considerado en el ámbito mundial como estándar e ITIL como buenas prácticas de TI, y en tal virtud, se complementan para facilitar tanto el Gobierno de TI, como la posible obtención de certificación en normas ISO.

CUADRO DE MANDO INTEGRAL (CMI) APLICADO AL CASO DE ESTUDIO

Los autores Nils-Göran Olve manifiestan que "*El concepto del cuadro de mando integral, (CMI) apareció a principios de los años 90. En el año 2000, algunos estudios indicaban que una mayoría d empresas de EE.UU., el Reino Unido y Escandinavia usaba el cuadro de mando*" [8]. Otros estudios, como el de herramientas de gestión de Bain, [9] indicaban una disminución en el uso que bajaba hasta el 36%, aunque con un alto porcentaje de satisfacción con la herramienta apoyada en programas informáticos.

"*Si tenemos el personal adecuado (perspectiva del desarrollo) haciendo lo correcto (perspectiva del proceso), los clientes estarán encantados (perspectiva del cliente) y nosotros mantendremos y conseguiremos más negocios (perspectiva financiera)*" [10].

El éxito de la utilización del Cuadro de Mando Integral (CMI) está en la delegación y asignación de responsabilidades a todo nivel, esto es, un responsable para cada objetivo estratégico, cada Factor Crítico de Éxito (FCE), cada indicador de resultados asociado a cada FCE. Cada persona es responsable de controlar el adecuado desarrollo y cabal cumplimiento de lo encomendado. La TI tiene en este campo la oportunidad de contribuir al éxito corporativo, con la prestación de servicios de calidad, que satisfagan las Necesidades de Información, Comunicaciones y Control Institucionales, con los consiguientes beneficios potenciales inherentes.

---

[8] OLVE, Nils-Göran, El Cuadro de Mando en Acción: Equilibrando la Estrategia y Control, Ediciones Deusto, 2004, Barcelona-España, p. 19, 334 p.
[9] Para el año 2000: http://www.bain.com/bainweb/expertise/tools/mtt/balance_scorecard.asp
[10] Dirigidas a Kaplan y Norton (1996, 2001); Olve et al. (1999); u Olve y Sjöstrand (2002).

¿Cómo introducir el cuadro de mando en las empresas?

Metas de los proyectos de cuadros de mando.

El aporte que el CMI proporciona a los empleados es valioso porque gracias a él comprenden la situación de la empresa, y para los ejecutivos ya que obtienen información confiable, a medida que la Institución implementa, desarrolla y documenta de forma continua las medidas de control que aceleran la alineación y consecución de metas, objetivos y visión Institucionales. Su aplicación asegura que las operaciones diarias se fundamenten en la visión compartida de hacia dónde se dirige la Institución en el corto, mediano y largo plazo. Por lo expuesto es recomendable segmentar al CMI por áreas operativas para que sus Indicadores, FCE, metas y objetivos tengan y mantengan su real importancia y adecuado grado de urgencia, con lo cual empleados y ejecutivos estarán mejor motivados para ser más comprensivos, abiertos al cambio y firmes en la implementación de las acciones proactivas y reactivas que se requieran para alcanzar objetivos Institucionales, desarrollar sus capacidades y usar el CMI para transparentar las ganancias socio-económicas.

Algunos autores manifiestan que unas empresas comienzan sus proyectos de CMI en el máximo nivel jerárquico Institucional, otras en los niveles superiores o con un proyecto piloto en un nivel inferior, algunas nunca salen de sus niveles superiores, mientras que otras tienen hasta cuadros de mando para equipos e individuales para personas concretas. Todo esto responde a una decisión sobre qué objetivos y/o funciones de apoyo interno deberían incluirse en los CMI.

La comunicación es importante para lograr una visión sistémica de la Institución, con objetivos compartidos e interdependientes y el CMI facilita diálogos para:

- Acordar e informar sobre resultados a obtener a los niveles superiores.

- Decidir respecto a los servicios que se necesitan sobre la base de los beneficios esperados y su impacto socio-económico.
- Asignar prioridades a los requerimientos de clientes.
- Demostrar que los esfuerzos de los empleados de funciones de apoyo sí contribuyeron al cumplimiento de los Objetivos estratégicos Institucionales, lo cual es útil para motivar al personal.

Las siguientes cuatro perspectivas del CMI en el caso de entidades gubernamentales y otras organizaciones sin fines de lucro tienen que ser orientadas a un propósito y fin socio-económico:

- *Perspectiva socio-económica*. La principal perspectiva por su contribución definitiva a satisfacer las necesidades Institucionales, departamentales, de equipos y/o personales.
- *Perspectiva del cliente*. Es una perspectiva "externa" que está sujeta a la capacidad que se tenga para identificar, determinar, atender y satisfacer las Necesidades de los Clientes, incluye a todos los contactos de la sociedad que interactúan con ellos.
- *Perspectiva del proceso*. Con o sin grandes cambios, dado que los procesos internos de todas las Instituciones deben ser eficaces y estar bien dirigidos, para producir las obras, bienes y/o servicios que los Clientes internos y externos requieren para satisfacer sus necesidades.
- *Perspectiva de desarrollo*. La fuente de la innovación, motivación, compromiso, desarrollo, etc., es el aprendizaje y crecimiento tanto individual como Institucional, sean éstas con o sin fines de lucro.

Desarrollo de los primeros cuadros de mando.

El primer paso fue reunir material sobre las características y requisitos de la Institución, considerando sus clientes, sector, posición y papel actual de la Institución y Unidad. Para contar con una plataforma sólida para elaborar nuestra visión, estrategias y objetivos, se utilizaron entrevistas personales con la alta

dirección, líderes de opinión, clientes destacados, proveedores, etc., mediante las cuales se confirmó la visión Institucional y de la Unidad de Sistemas.

El siguiente paso es elegir y establecer las perspectivas sobre las cuales construir el CMI, y para cada una de ellas desglosar la visión en objetivos o metas estratégicas generales e identificar los factores críticos para el éxito de cada una de ellas.

Luego se definieron las medidas importantes para comprobar que la estructura del CMI mantenga consistencia lógica y equilibrio entre las relaciones causa-efecto y las medidas de las diferentes perspectivas.

Si se ha cumplido con este paso, las mejoras a corto plazo deberían contribuir al cumplimiento de objetivos a largo plazo y las medidas de las diferentes perspectivas deberían estimular la optimización y el alineamiento a la visión para apoyar la estrategia general.

Aplicación del CMI al caso de estudio: A continuación se presenta:

- El Cuadro de Mando Integral (CMI) de Gestión de Continuidad de los Servicios de TI.
- El Mapa Estratégico del CMI de Gestión de Continuidad de los Servicios de TI.
- La Matriz del CMI de Gestión de Continuidad de los Servicios de TI.
- Los cuadros de los Indicadores Clave de Resultados de las perspectivas Socio-Económica, del Proceso, de Desarrollo y el Cliente.

CUADRO DE MANDO INTEGRAL (CMI) DE GESTIÓN DE CONTINUIDAD DE LOS SERVICIOS DE TI

Parte I: Lógica Institucional del apoyo de TI

Objetivo estratégico: Lograr la Continuidad de los Servicios críticos de TI.

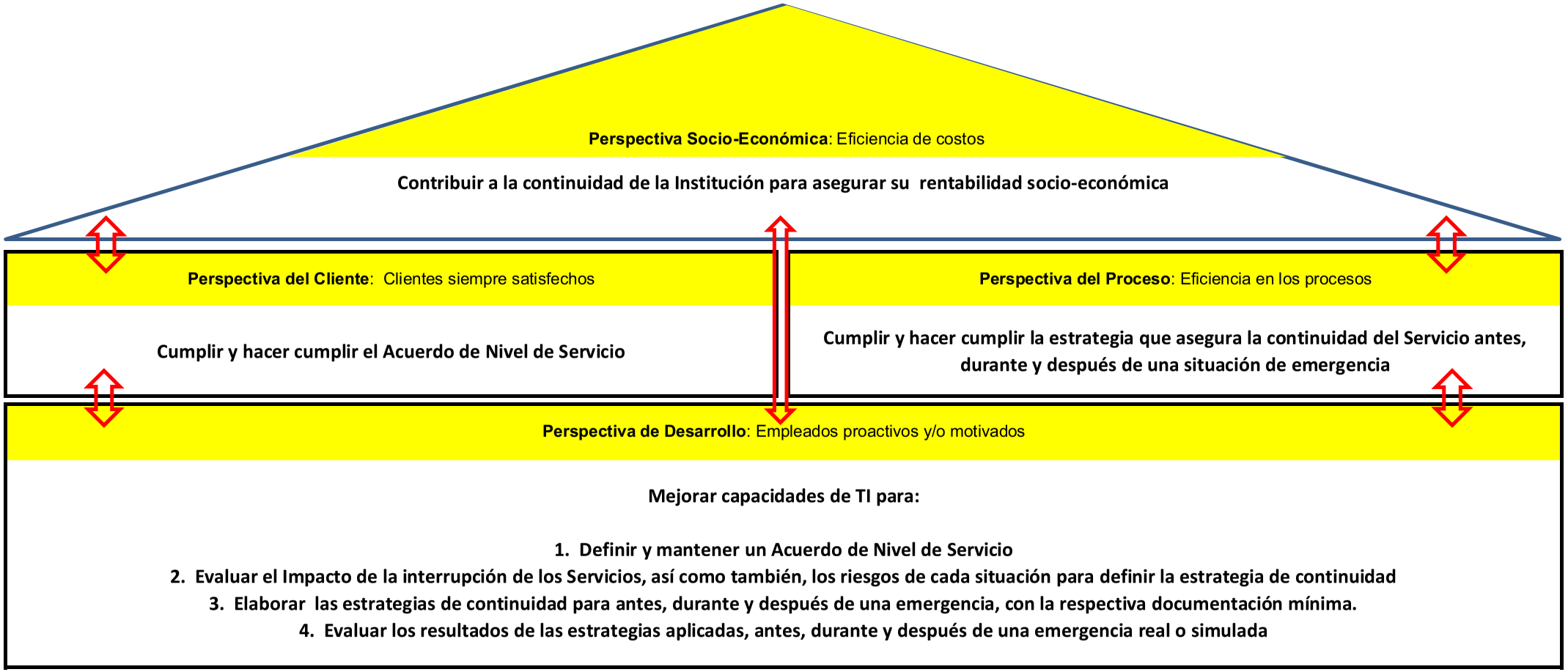


Figura 6. CMI de Gestión de Continuidad de los Servicios de TI

CMI DE GESTIÓN DE CONTINUIDAD DE LOS SERVICIOS CRÍTICOS DE TI

Mapa estratégico.- Conjunto de acciones que se deben llevar a cabo para alcanzar el Objetivo Estratégico: Lograr la Continuidad de los Servicios Críticos de TI.

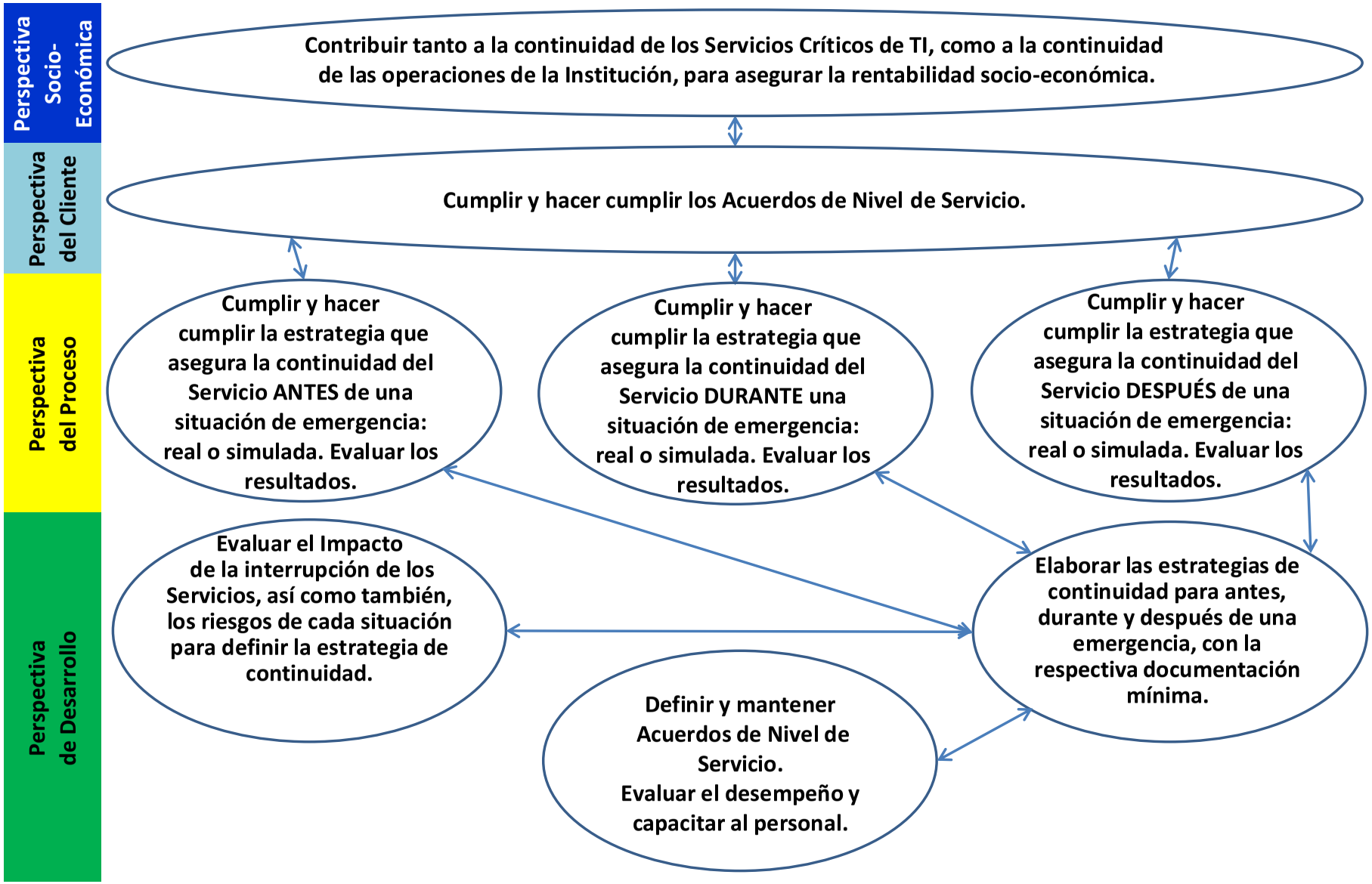


Figura 7 de la Tesis. CMI de Gestión de Continuidad de los Servicios de TI

PARTE III: MATRIZ DEL CMI DE GESTIÓN DE CONTINUIDAD DE SERVICIOS DE TI

Empresa:	PETROECUADOR, Unidad de Sistemas
Misión:	PETROECUADOR es una empresa estatal, con enfoque internacional, cuya finalidad es explorar, explotar, transportar, almacenar, industrializar y comercializar eficaz y eficientemente los recursos hidrocarburíferos, con calidad, respeto y protección al ambiente; todo esto de acuerdo con las políticas de hidrocarburos establecidas por el gobierno nacional y acorde al marco jurídico vigente.
Visión:	PETROECUADOR será una Empresa 100% Estatal, con autonomía operativa, administrativa y financiera, capaz de manejar los negocios petroleros del Estado con excelencia, capacidad estratégica, flexibilidad organizacional y una cultura empresarial competitiva a nivel internacional; y que opere con estándares de eficacia, eficiencia y calidad.
Objetivo estratégico:	Lograr la Continuidad de los Servicios Críticos de TI

Perspectivas:	**Socio-Económica**	**Del Proceso**	**De Desarrollo**	**Del Cliente**
Objetivos estratégicos / Posición deseada:	Contribuir a la continuidad de la Institución para asegurar su rentabilidad socio-económica	Cumplir y hacer cumplir las estrategias que aseguran la continuidad del Servicio antes, durante y después de una situación de emergencia	1. Definir y mantener un Acuerdo de Nivel de Servicio 2. Evaluar el Impacto de la interrupción de los Servicios, así como también, los riesgos de cada situación para definir la estrategia de continuidad 3. Elaborar las estrategias de continuidad para antes, durante y después de una emergencia, con la respectiva documentación mínima. 4. Evaluar los resultados de las estrategias aplicadas, antes, durante y después de una emergencia real o simulada	Cumplir y hacer cumplir el Acuerdo de Nivel de Servicio
FCE:	Ejecutar el presupuesto	Probar las estrategias formuladas para antes, durante y después de una situación de emergencia	Asumir las responsabilidades asignadas de inicio a fin.	Satisfacer sus necesidades de continuidad de Servicios
Indicador clave de resultado (ICR):	% de ejecución presupuestaria de este año con relación a la del año anterior	Hay de disponibilidad de procedimientos de Respaldo, Restauración y Recuperación; y, listas de chequeo y actas de enrega recepción	Evaluación del desempeño en el cumplimiento de las responsabilidades asignadas. Escala de 1 a 5: Deficiente, Regular, Bueno, Muy bueno y Excelente.	Calificación del cliente de su nivel de satisfacción. Escala de 1 a 5.
Metas:	Año 2008: 90% Año 2009: 95% Ano 2010: 100%	Año 2008: Si	Año 2008: Muy bueno Año 2009: Excelente	Año 2008: Muy bueno Año 2009: Excelente
Acciones estratégicas / proactivas:	Elaborar y ejecutar el presupuesto de Continuidad de Servicios.	Trabajar en equipo con el Cliente para mejorar las estrategias que aseguran la continuidad del Servicio antes, durante y después de una situación de emergencia	Elaborar y mantener actualizadas las estrategias para antes, durante y después de una situación de emergencia Coordinar la renovación de contratos a tiempo, y Cumplir el Acuerdo de Nivel de Servicios.	Acordar el Nivel de Servicios

Cuadro 2. Matriz de CMI de Gestión de Continuidad de Servicios de TI

INDICADORES CLAVE DE RESULTADO (ICR) DE GESTIÓN DE CONTINUIDAD DE SERVICIOS DE TI

Perspectiva Socio-Económica

Indicador clave de resultado (ICR): % de ejecución presupuestaria de este año con relación al año anterior

Ítem del gasto	2007 Ene-Ago	2008 Ene-Ago	Cumplimiento
22. Energía eléctrica comprada	3.023,29	3.255,69	108%
24. Seguros	6.699,54	5.616,86	84%
28. Servicios contratados de operación	27.407,15	22.686,72	83%
29. Servicios contratados de mantenimiento	47.515,63	47.790,65	101%
41. Materiales y suministros de mantenimiento	376,99	369,49	98%
42. Combustibles y lubricantes	465,75	492,45	106%
Totales	85.488,36	80.211,86	94%

Cuadro 3. Indicador de la perspectiva Socio-Económica

Perspectiva de Desarrollo

Indicador clave de resultado (ICR): Evaluación del desempeño en el cumplimiento de las responsabilidades asignadas. Escala de 1 a 5: Deficiente, Regular, Bueno, Muy bueno y Excelente.

Id. Servicios críticos de TI	Cumplimiento
1. Reactivación Contraseña y 4. Creación / Accesos Usuarios	4
2. Provisión de telecomunicaciones	4
3. Provisión / Renovación Telefonía móvil	4
5. Correo Electrónico	4
6. Instalación / reparación de Energía regulada y Red de Datos	4
7. Gestión de Respaldos	4
8. Interbase (Datos del RCP)	4
9. Internet/Intranet	4

Cuadro 4. Indicador de la perspectiva de Desarrollo

Perspectiva del Proceso

Indicador clave de resultado (ICR): Hay de disponibilidad de procedimientos de Respaldo, Restauración y Recuperación; y, listas de chequeo y actas de entrega recepción

Id. Servicios críticos de TI	Cumplimiento
1. Reactivación Contraseña y 4. Creación / Accesos Usuarios	
2. Provisión de telecomunicaciones	Si
3. Provisión / Renovación Telefonía móvil	Si
5. Correo Electrónico	Si
6. Instalación / reparación de Energía regulada y Red de Datos	Si
7. Gestión de Respaldos	Si
8. Interbase (Datos del RCP)	Si
9. Internet/Intranet	Si

Cuadro 5. Indicador del Proceso

Perspectiva del Cliente

Indicador clave de resultado (ICR): Calificación del cliente de su nivel de satisfacción. Escala de 1 a 5.

Id. Servicios críticos de TI	Cumplimiento
1. Reactivación Contraseña y 4. Creación / Accesos Usuarios	4
2. Provisión de telecomunicaciones	4
3. Provisión / Renovación Telefonía móvil	4
5. Correo Electrónico	4
6. Instalación / reparación de Energía regulada y Red de Datos	4
7. Gestión de Respaldos	4
8. Interbase (Datos del RCP)	4
9. Internet/Intranet	4

Cuadro 6. Indicador de la perspectiva del Cliente

CAPÍTULO 2. INTEGRACIÓN DE COBIT E ITIL PARA LA GESTIÓN DE LA ENTREGA DE SERVICIOS DE TI

El Proceso de Entrega de Servicios de TI se fundamenta en la satisfacción de las Necesidades de Información, Comunicaciones y Control Institucional, así como, en COBIT e ITIL, cuyos subprocesos se describen a continuación.

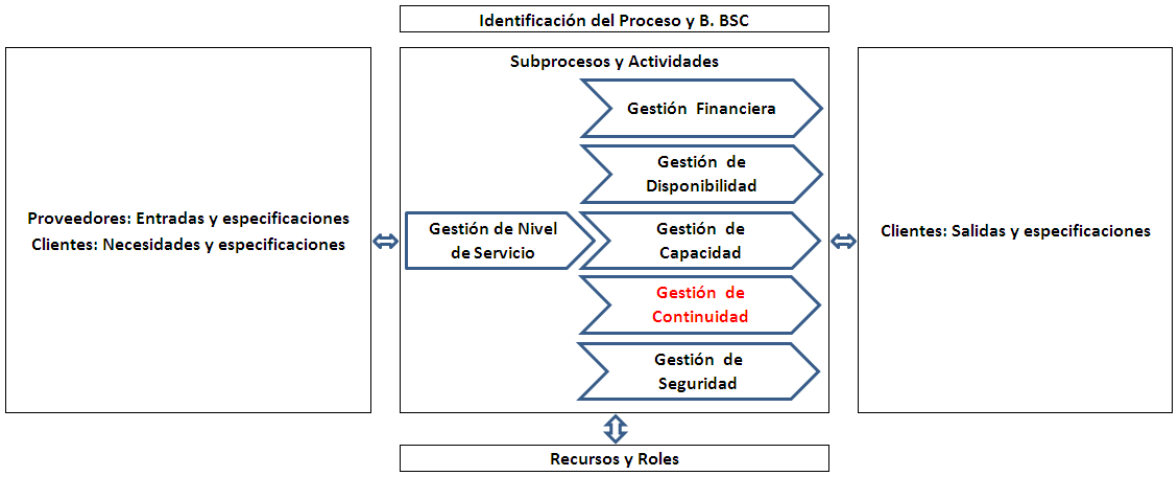


Figura 8. Proceso de Entrega de Servicios de TI.

A continuación de describe cada uno de ellos:

2.1 Gestión de Nivel de Servicio
2.2 Gestión Financiera
2.3 Gestión de la Disponibilidad
2.4 Gestión de la Capacidad
2.5 Gestión de la Seguridad
2.6 Gestión de Continuidad de los Servicios

2.1 Gestión de Nivel de Servicio

La Gestión de Nivel de Servicios (SLM) incluye la planificación, coordinación, ejecución, seguimiento y control de acuerdos de niveles de servicio (SLA), cuya finalidad es asegurar el cumplimiento de las características y condiciones en las que se acuerda prestar cada uno de los Servicios de TI. Esto permite contar con una herramienta para el seguimiento y control de la calidad del servicio, mediante la cual se logre mantener y mejorar la calidad de los servicios de TI, así como, la relación entre el personal de TI, clientes y proveedores de servicios.

Los beneficios esperados son:

- ✓ El establecimiento de acuerdos de nivel de servicio fundamentados en la calidad del servicio sobre parámetros medibles, que permitan el respectivo seguimiento y control, considerando la concentración de esfuerzo y recursos en la satisfacción de las Necesidades de Información, Comunicación y Control Institucional. En ciertas instituciones pueden ser utilizados los acuerdos como base para la facturación de los servicios.
- ✓ La clara definición de roles y responsabilidades para las partes, considerando su inter dependencia.
- ✓ El mejoramiento de la calidad de servicio y reducción en la interrupción de servicio.
- ✓ Los acuerdos de nivel de servicio deben sustentar la elaboración de presupuestos, así como, del valor agregado que reciben los clientes (por su dinero).
- ✓ Facilitar la rápida y objetiva resolución de conflictos.

El Gobierno de TI debe asegurarse que su catálogo de servicios cuente con acuerdos de nivel de servicios debidamente respaldados por similares acuerdos con sus proveedores.

Para tal efecto, el dueño de este subproceso será responsable de:

- ✓ Elaborar y mantener actualizado el Catálogo de Servicios.
- ✓ Negociar y elaborar acuerdos de nivel de servicio, de beneficio mutuo, en forma conjunta con clientes y proveedores internos y externos.
- ✓ Elaborar una lista de chequeo que permita registrar el cumplimiento de cada acuerdo, la misma que será inmediatamente evaluada para tomar oportunamente las medidas preventivas y/o correctivas que aseguren el cabal cumplimiento de lo acordado.
- ✓ Cumplir y hacer cumplir los roles y responsabilidades de las partes.
- ✓ Coordinar las actividades tendentes al cabal cumplimiento de lo acordado.
- ✓ Utilizar herramientas de seguimiento y control que sustenten las decisiones.

El Catálogo de Servicios es una lista de todos los servicios provistos, con un resumen de sus características. A continuación se muestra el Cuadro 7. Catálogo de Servicios de TI.

Un servicio puede ser provisto por una o más aplicaciones de TI que contribuyen en forma parcial o total a la satisfacción de las Necesidades de Información, Comunicaciones y Control Institucional.

La negociación debe propender a lograr un acuerdo de beneficio mutuo, lo cual va a requerir de varias iteraciones hasta alcanzar un balance entre las expectativas de clientes y proveedores del servicio, sustentado en la normativa vigente y real capacidad de la Institución. El acuerdo se firmará entre los jefes de las áreas involucradas.

El Acuerdo de Nivel de Servicio (SLA) contendrá los datos que se consideren necesarios, como por ejemplo:

- ✓ Introducción
- ✓ Horas de servicio

CATÁLOGO DE SERVICIOS DE COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

ID	DENOMINACION	MEDIO DE COMUNICACIÓN	CLASE DE USUARIOS	CARACTERISTICA DEL SERVICIO	INDICADOR MENSUAL	Valor Esperado (Optm+4*Prob+Pesm)/6
1	Internet	llamada	TODOS	Confiable, con velocidad adecuada de navegación y disponible 24/7 con las seguridades que garanticen este servicio.	# horas reales de servicio / # Horas mes	0,969
2	Correo Electrónico	llamada, memo	TODOS	Confiable, disponible 24/7 con las seguridades que garanticen este servicio.	# horas reales de servicio / # Horas mes espacio utilizado / espacio asignado	0,905
3	Creación / Accesos Usuarios	memo, correo electrónico	TODOS	Asignación oportuna de los servicios de TIC	# requerimientos Atendidos / # requerimientos Solicitados	0,000
4	Reactivación Contraseña	llamada	TODOS	Disponibilidad inmediata de la nueva contraseña, basado en sugerencias para recordarla.	# de contraseñas reactivadas / # de usuarios activos	0,000
5	Soporte herramientas de Ofimática: procesador de palabras, hoja electrónica, presentaciones	llamada, memo	TODOS	Oportunidad y efectividad en el soporte para la utilización de las herramientas de ofimática	# de atenciones / # de usuarios registrados	0,000
6	Instalación / renovación de Software especializado	memo	ESPECIFICO	Oportunidad y agilidad en la gestión de adquisición y renovación de software especializado requerido por las dependencias de PEC	# de requerimientos / # de usuarios activos	0,000
7	Soporte básico en Software especializado	llamada, memo	ESPECIFICO	Oportunidad y efectividad en el soporte básico para la utilización de Software especializado	# de atenciones / # de usuarios de software especializado	0,000
8	Desarrollo Sistemas de Información	memo	ESPECIFICO	Oportunidad y agilidad en la implementación de sistemas de información requeridos por las dependencias de PEC	tiempo real / tiempo estimado	0,000
9	Soporte / Mantenimiento Sistemas de Información	llamada, memo, correo electrónico	ESPECIFICO	Oportunidad y efectividad en el soporte y mantenimiento de los sistemas de información		0,000
10	Instalación / reparación de Energía regulada y Red de Datos	llamada, memo	TODOS	Oportuna, confiable y que cumpla con las normas técnicas que garanticen este servicio.	# de instalaciones realizadas / # de requerimientos # de reparaciones realizadas / # de requerimientos	0,000
11	Instalación / reparación Telefonía fija	llamada, memo	TODOS	Oportuna, confiable y ágil.	# de instalaciones realizadas / # de requerimientos # de reparaciones realizadas / # de requerimientos	0,000
12	Provisión / Renovación Telefonía móvil	llamada, memo	ESPECIFICO	Oportunidad y agilidad en la gestión externa para la entrega de telefonía celular	# de requerimientos atendidos / # de requerimientos solicitados	0,000
13	Provisión de energía regulada	llamada, memo	TODOS	Confiable, continua y que cumpla con las normas técnicas	# de horas de servicio no entregadas / 720 (horas al mes)	0,000
14	Provisión de telecomunicaciones	llamada, memo		Confiable, continua y que cumpla con las normas técnicas		0,000
15	Provisión de telefonía fija	llamada, memo		Confiable, continua y que cumpla con las normas técnicas		0,000
16	Provisión de infraestructura (Hw, Sw, Aplicaciones, Telecomunicaciones y equipos auxiliares)	memo, Plan operativo TIC	TODOS	Oportunidad y agilidad en la gestión de provisión de Hw, Sw, aplicaciones, Telecomunicaciones y equipos auxiliares indispensable para el cumplimiento de objetivos de las dependencias de PEC	# de requerimientos atendidos / # de requerimientos % obsolescencia de PC's % obsolescencia de servidores % obsolescencia de equipos de comunicación % obsolescencia de almacenamiento % obsolescencia de software % obsolescencia de aplicaciones % obsolescencia de equipos auxiliares	0,000
17	Reparación de equipos TI	llamada, memo	TODOS	Oportunidad y agilidad para efectuar el diagnóstico primario para remitirlo a la empresa proveedora del mantenimiento y recibir el equipo reparado	# de equipos reparados / # de equipos enviados a reparación	0,000
18	Interbase (Datos del RCP)	llamada, memo	ESPECIFICO	Eficiencia en el acceso a la base de datos de Interbase que soporta al Sistema de Registro de Calificación de Proveedores.	# de requerimientos atendidos / # de requerimientos solicitados	0,000
19	Diseño Grafico (logos, web, presentaciones)	llamada, memo, personal, correo electrónico	ESPECIFICO	Oportunidad y calidad en la entrega del diseño solicitado	# de requerimientos de diseño grafico / # de requerimientos solicitados en diseño, digitalización, impresiones, copias digitales	0,000
20	Digitalización de documentos	llamada, memo, personal, correo electrónico	ESPECIFICO	Oportunidad en la entrega del documento digitalizado	# de requerimientos de digitalización de documentos / # de requerimientos solicitados en diseño, digitalización, impresiones, copias digitales	0,000
21	Copias en medios digitales e Impresiones	llamada, memo, personal, correo electrónico	TODOS	Oportunidad en la entrega de las copias digitales y de las impresiones	# de requerimientos copias e impresiones / # de requerimientos solicitados en diseño, digitalización, impresiones, copias digitales	0,000
22	Escaneo de mapas y planos	llamada, memo, personal	ESPECIFICO	Oportunidad, Claridad y máxima resolución	# requerimientos atendidos / # requerimientos GIS	0,000
23	Georeferenciación de mapas y planos	llamada, memo, personal	ESPECIFICO	Oportunidad, Exactitud y precisión		0,000
24	Digitalización de mapas y planos	llamada, memo, personal	ESPECIFICO	Oportunidad, Exactitud y precisión		0,000
25	Diseño y Construcción de mapas	llamada, memo, personal	ESPECIFICO	Oportunidad, Calidad y precisión		0,000
26	Impresión de mapas y planos a diferentes escalas	llamada, memo, personal	ESPECIFICO	Oportunidad, Calidad y precisión		0,000
27	Gestión de Respaldos	memo, correo electrónico	ESPECIFICO			

Nomenclatura, ID: Identificación del Servicio de TI.

Cuadro 7. Catálogo de Servicios de TI

- ✓ Disponibilidad
- ✓ Fiabilidad
- ✓ Soporte
- ✓ Carga de trabajo
- ✓ Tiempos de respuesta
- ✓ Tiempo de proceso por lotes
- ✓ Cambio
- ✓ Continuidad y seguridad
- ✓ Cobranza
- ✓ Reportes y revisiones
- ✓ Incentivos y penalidades

El seguimiento y control de los acuerdos firmados, debe ser reportado periódicamente, a fin de conocer las novedades encontradas, así como, las medidas preventivas y/o correctivas requeridas para el cabal cumplimiento de los mismos. Los reportes serán de dos tipos, de situaciones de excepción y las actas de reuniones entre las partes, en ambos casos, contendrán la evaluación del desempeño del personal involucrado, la satisfacción o insatisfacción del cliente, señalarán que medidas preventivas y/o correctivas se han aplicado y se adjuntará el respectivo cronograma con el cual se aplicarán las medidas que se encuentran pendientes a la fecha del reporte.

Para evitar posibles problemas se debe considerar la supervisión para asegurarse que los resultados sean alcanzables, que se cuente con los recursos necesarios para su cabal cumplimiento, que no haya conflictos de autoridad, que esté establecido por escrito y suscrito, que las responsabilidades de las partes estén claramente definidas, que sean comunicados apropiadamente, que se valore el servicio aunque no se lo cobre realmente, etc.

2.2 Gestión Financiera

La Gestión Financiera incluye la contabilidad total de los costos y gastos de los servicios de IT y en algunas Instituciones la recuperación de los mismos al facturar los servicios prestados; así como también el asesoramiento en inversiones de TI y la elaboración de presupuestos en coordinación con las dependencias de planificación y finanzas.

Los beneficios esperados son:

- ✓ El saber los costos actuales de la prestación de servicios, para analizarlos en función de la calidad de los mismos, para plantear opciones de mejoramiento y/o reducción de costos a corto, mediano y largo plazo.

- ✓ Al contar con información financiera precisa se puede calcular el costo total de propiedad o TCO (Total Cost of Ownership) y la tasa de retorno de la inversión o ROI (Return on Investment), así como también el valor agregado con el cual las TI aportan a la Institución.

- ✓ La toma de decisiones cotidianas con una comprensión completa de las implicaciones de costos con menor riesgo, referentes a ejecución presupuestaria, priorización en el uso de recursos para renovación tecnológica y/o provisión de servicios de TI.

- ✓ La posibilidad de distribuir y recuperar los costos de los servicios de TI considera: Los Centros de costos, que implican desarrollar el comportamiento de los usuarios y que el Gobierno de TI tenga la habilidad de elegir como financiarse por sí mismo; Centro de recuperación, que requiere del reconocimiento de los costos verdaderos de los clientes; y, Centro rentable, en el cual el producto o servicio es claramente identificado y vendido a precio de mercado.

- ✓ El conocimiento y reconocimiento de los costos directos que son aquellos que pueden atribuirse claramente a un cliente único; así como también los costos indirectos que son aquellos incurridos por todos o por un grupo de clientes, que tienen que ser prorrateados a todos los clientes de la manera más justa posible. Los costos fijos no están en función de la cantidad de servicios que se prestan, los variables sí.

El Gobierno de TI debe asegurarse que existan políticas que determinen claramente: el nivel de recuperación de costos requerido; el comportamiento de proveedores y Clientes (usuarios), la utilización eficiente de recursos; la capacidad instalada requerida; la priorización de los trabajos; la adecuada relación costo, precio, calidad y cobro.

Para tal efecto el dueño del subproceso será responsable de:

- ✓ Cumplir y hacer cumplir las políticas, así como también proponer cambios.
- ✓ Asesorar en materia financiera, al Gobierno de TI, clientes y proveedores.
- ✓ Lograr confianza en la gestión financiera de TI.
- ✓ Comunicar o concienciar a los clientes de los costos asociados de los servicios de TI que utilizan.

El seguimiento y control de las finanzas, debe ser reportado periódicamente, a fin de conocer las novedades encontradas, así como, las medidas preventivas y/o correctivas requeridas para el cabal cumplimiento de las mismas. Los reportes serán de dos tipos, de situaciones de excepción y las actas de reuniones entre las partes, en ambos casos, contendrán la evaluación del desempeño del personal involucrado, la satisfacción o insatisfacción del cliente, señalarán que medidas preventivas y/o correctivas se han aplicado y se adjuntará el respectivo cronograma con el cual se aplicarán las medidas que se encuentran pendientes a la fecha del reporte.

Para evitar posibles problemas se debe considerar la supervisión para asegurarse cuando sea pertinente, que la presupuestación, contabilidad, prestación de servicios, precio y cobranza estén bien formuladas y documentadas, así como también que se utilicen las herramientas idóneas para tal fin.

2.3 Gestión de la Disponibilidad

La Gestión de la Disponibilidad incluye diseño, implementación y medición de la disponibilidad de los recursos de TI, y es un proceso continuo que inicia con la determinación de requerimientos de disponibilidad de cada recurso crítico y termina cuando los servicios de TI dejan de utilizar dicho recurso, consecuentemente se fundamenta en el conocimiento y atención oportuna de los requerimientos de disponibilidad de los recursos de TI: personal, información, infraestructura y aplicaciones, los mismos que deben ser debidamente administrados, para asegurar que las Necesidades de Información, Comunicaciones y Control Institucionales de los clientes sean satisfechas.

Los beneficios esperados son:

- ✓ El fortalecimiento de la imagen y confianza en el Gobierno de TI, porque se dispone de los recursos que satisfacen la demanda de los servicios de TI de la Institución y clientes, con una adecuada relación costo-beneficio.
- ✓ El disponer del conocimiento, recursos y presupuesto necesarios para mantener la disponibilidad de los servicios de TI.
- ✓ El enfoque proactivo para el mejoramiento de la disponibilidad de los recursos y servicios de IT, mediante un costo justificado para lograr que los servicios de IT sean diseñados conforme los requerimientos de disponibilidad de cada categoría de Institución a la cual se provea, así como también para disminuir la frecuencia y duración de las interrupciones en la disponibilidad de recursos y servicios de TI.

- ✓ El Gobierno de TI es sistémico y está debidamente alineado al Gobierno Corporativo, y en tal virtud es visto como un valor agregado a la Institución.
- ✓ Mejores prestaciones de recursos y servicios de TI, reducción de costos, alineación entre el Gobierno de TI y el Gobierno Corporativo.
- ✓ Un marco de referencia uniforme para la comunicación mutua y la contratación de acuerdos de niveles de servicio y disponibilidad, decisiones de outsourcing, con el consiguiente cambio cultural hacia la entrega de servicios de calidad, alto desempeño y rendimiento.
- ✓ Servicios de TI detallados, bien documentados, estables, confiables y de calidad garantizada, que cuenta además con adecuados canales de comunicación.
- ✓ Preparación para la certificación ISO-9000.

El Gobierno de TI debe asegurarse que la Gestión de la Disponibilidad realice análisis de riesgos de los incidentes que pueden impactar sobre la disponibilidad de los servicios, así como también de la forma en que se manejan y resuelven. El análisis de riesgos de desastres e interrupciones de los servicios importantes son de responsabilidad de la Gestión de la Continuidad.

Es importante entender como cada recurso aporta a funciones importantes de la Institución a través de los servicios de TI, para lograr que su disponibilidad y fiabilidad influyan positivamente en la satisfacción de las necesidades de sus clientes.

La disponibilidad es la habilidad del Gobierno de TI para contar con los componentes de calidad, que sean necesarios, resistentes a fallas, debidamente mantenidos, seguros, integrados y con datos actualizados, a fin de que un recurso pueda entregar la funcionalidad requerida mientras esté activo.

La Fiabilidad del servicio de IT es la confianza de que está libre de falla operacional. Se logra mediante el mantenimiento preventivo que asegura el retorno a su estado de funcionalidad nuevamente. La seguridad se refiere a la

confidencialidad, integridad y disponibilidad de los datos asociados con dicho servicio.

El mantenimiento se refiere a la capacidad de servicio interno y/o contratado con conocimiento, información, repuestos, infraestructura y aplicaciones que aseguren la disponibilidad, fiabilidad y capacidad de mantenimiento de los recursos y servicios de TI. Todo esto determina la disponibilidad del Servicio de TI.

Para tal efecto el dueño del subproceso será responsable de:

- ✓ La determinación de los requerimientos de disponibilidad de cada recurso crítico, calificación dada porque de él depende la disponibilidad de uno o más servicios de TI, que deben incorporarse en los acuerdos de niveles de servicio.
- ✓ La evaluación del impacto que tendría la pérdida temporal o definitiva de cada recurso crítico en el servicio del cual depende.
- ✓ La provisión de datos útiles sobre acuerdos de niveles de servicio, configuraciones, monitoreo, incidentes y problemas de los recursos críticos.
- ✓ La utilización de métodos y técnicas idóneas para la Gestión de la Disponibilidad, tales como:
    - El Análisis de Impacto de falla de componente (CFIA): Este método utiliza una matriz de disponibilidad con componentes estratégicos y sus roles en cada servicio.
    - Análisis de árbol de fallas (FTA): Es una técnica que se usa para identificar la cadena de eventos que producen la falla de un servicio. Se diseña un árbol de fallas separado para cada servicio.
    - Análisis de interrupción del servicio, es una técnica que puede emplearse para identificar las causas de la fallas para investigar la eficacia de la organización de IT y sus procesos, y para presentar e implementar las propuestas de mejoras.
    - Observación de Técnicas Post (TOP): Cuando se usa este método, un equipo de especialistas de IT dedicados pone toda su atención en un solo aspecto de la disponibilidad.

- Análisis de riesgo CCTA y Método de Gestión (CRAMM).

- ✓ Lograr la satisfacción del usuario, incluso en la recuperación de un incidente cuya duración debe ser mínima para retornar a la operación normal.
- ✓ La coordinación y comunicación necesarias con la gestión de incidentes y problemas para conocer y aportar en el análisis del ciclo de vida del incidente, para identificar cuándo se pierde más tiempo, cuáles son las posibles áreas de ineficiencia, qué datos de disponibilidad se tienen de la caída y/o interrupción de un servicio, tales como disminución de la calidad, improductividad de los recursos, pérdida de ventas y cobranzas, insatisfacción, incumplimiento, demandas de tipo legal, etc.
- ✓ El cálculo total de la disponibilidad de cada recurso y/o servicio, mediante el producto de todos los porcentajes de disponibilidad de cada componente individual o de elementos paralelos.

  Disponibilidad Infraestructura= Disp. Server x Disp. Red x Disp. PC.

  Ejemplo: Disponibilidad = 0,9996 x 0,98 x 0,96 =0,9404 (94,04%).
- ✓ Asegurar que los recursos y Servicios de TI sean capaces de entregar los niveles de disponibilidad acordados.
- ✓ Justificar la optimización de los recursos y servicios de TI para asegurar la disponibilidad requerida para cumplir los acuerdos de niveles de servicio.
- ✓ Reducir la frecuencia y duración de los incidentes porque impactan directamente a la disponibilidad.
- ✓ Definir la disponibilidad en los términos utilizados al establecer los acuerdos de nivel de servicio.

El seguimiento y control de la disponibilidad, debe ser reportado periódicamente, a fin de conocer las novedades encontradas, así como, las medidas preventivas y/o correctivas requeridas para el cabal cumplimiento de la misma. Los reportes serán de dos tipos, de situaciones de excepción y las actas de reuniones entre las partes, en ambos casos, contendrán la evaluación del desempeño del personal involucrado, la satisfacción o insatisfacción del cliente, señalarán que medidas preventivas y/o correctivas se han aplicado y se adjuntará el respectivo

cronograma con el cual se aplicarán las medidas que se encuentran pendientes a la fecha del reporte.

Para evitar posibles problemas se debe considerar la supervisión para asegurarse que el costo de la gestión de disponibilidad esté justificado, por los requerimientos de disponibilidad de los clientes, por la posible dificultad para encontrar profesionales experimentados, por la posible dependencia de proveedores, por el desconocimiento de los recursos y servicios de TI, y/o por la escasez de recursos de TI.

2.4 Gestión de la Capacidad

La Gestión de la Capacidad de Recursos y Servicios de TI es identificar y comprender la capacidad y la utilización de cada una de sus partes componentes, para determinar y asegurar el rendimiento presente y futuro de los recursos y Servicios de TI para satisfacer las Necesidades de Información, Comunicación y Control Institucionales, por medio del mantenimiento de los mismos y/o del reemplazo oportuno a un costo justificado, con lo cual se logra la disminución de interrupciones por la gestión de cambios, así como también se asegura que se atiendan eficientemente las demandas cambiantes de la Institución, para lo cual se debe balancear:

- ✓ El Costo con relación tanto con la Capacidad de procesamiento comprada de acuerdo a las necesidades de la Institución, como con el uso más eficiente de esos recursos.
- ✓ La Oferta con relación a la Demanda presente y futura de la Institución.
- ✓ La utilización actual y la planeada de los componentes individuales que permiten saber qué y cuándo actualizar; y, cuánto costará la actualización.
- ✓ El proceso con relación a todo lo que TI requiere para operar eficientemente, es decir el personal, información, infraestructura y

aplicación, la ausencia y/o falta de uno de ellos degrada el tiempo de respuesta, tanto en el ambiente de producción como en el de desarrollo.

Los beneficios esperados son:

- ✓ La respuesta oportuna a los requerimientos cambiantes de la capacidad de procesamiento, fundamentada en el conocimiento de los acuerdos de nivel de servicio, plan de capacidad y modelos de análisis, simulaciones, tendencias, líneas base y dimensionamiento de aplicaciones.
- ✓ El incremento de la disponibilidad de los recursos y servicios, gracias a la administración adecuada de la capacidad, lo cual contribuye a mantener y/o incrementar el desempeño y rendimiento de los recursos y Servicios de TI, lo cual incide directamente en la eficiencia y disminución de costos, porque reduce riesgos de incidentes y problemas por falta de capacidad.
- ✓ La confiabilidad en la capacidad de los recursos y Servicios de TI, para realizar pronósticos, el ciclo de vida de las aplicaciones, establecer e incrementar el nivel de servicio, la renovación tecnológica, etc., todo esto contribuye a incrementar la satisfacción del usuario.
- ✓ Mejora la posición de negociación de los acuerdos de nivel de servicio.

El Gobierno de TI debe asegurarse que el proceso de Gestión de la Capacidad de Servicios sea responsable de asegurar que se cumplan los objetivos de los acuerdos de niveles de servicio, así como también, de mantener el rendimiento, desempeño y monitoreo permanente de los recursos de TI, y proveer de información útil para realizar mediciones, análisis y ajustes en función de la demanda.

La Gestión de la Capacidad de recursos y Servicios de TI se fundamenta en la recolección iterativa de información sobre la utilización de recursos y sus componentes tales como procesadores, memoria, discos, ancho de banda de la red, conexiones de red, etc., para anticiparse al surgimiento de dificultades, mediante un proceso proactivo, y reactivo ante problemas específicos por la

ausencia y/o falta de un recurso, así con también por el uso ineficiente de los mismos.

Para tal efecto el dueño del subproceso será responsable de:

- ✓ La evaluación de nuevas tecnologías y de cómo pueden éstas ser aprovechadas para satisfacer las Necesidades de Información, Comunicaciones y Control Institucionales.
- ✓ Identificar la resistencia inherente en los recursos y Servicios de TI, así como también el impacto de fallas particulares en los recursos disponibles, y el potencial de ejecutar los servicios más importantes con los recursos restantes.
- ✓ El monitoreo de la utilización de cada recurso y servicio para asegurar su óptima utilización, así como también, el cumplimiento de los acuerdos de nivel de servicio y que los Servicios de TI son los esperados.
- ✓ El análisis de los datos recolectados para identificar tendencias y su proyección para considerarlas en los acuerdos de niveles de servicio.
- ✓ El mejoramiento y/o cambio parcial o total de los recursos para optimizar el desempeño o rendimiento de los mismos.
- ✓ La gestión de la demanda de recursos y Servicios de TI está en función de las Necesidades de Información, Comunicaciones y Control Institucionales, lo cual permite el correspondiente alineamiento, en la provisión y uso de recursos en el corto, mediano y largo plazo. Todo esto contribuye al desarrollo de la imagen Institucional.
- ✓ La recolección y almacenamiento de los datos de capacidad en una base de datos común para todos los procesos, considerando los respectivos datos de la Institución, Servicios, acuerdos de nivel de servicio, financieros, de disponibilidad, de capacidad, de seguridad, de continuidad, etc. Estos se usan como base para la producción de reportes sobre la capacidad actual y futura.
- ✓ El tratamiento adecuado de restricciones existentes y impuestas para el óptimo uso de los recursos, en cuanto a horarios, cantidad, costo, duración,

acuerdos de nivel de servicio, financieras, de disponibilidad, de capacidad, de seguridad, de continuidad, etc.

- ✓ La utilización o no de modelos para predecir la demanda de capacidad de los recursos por el comportamiento de los servicios de IT, tales como:
  - El Análisis de tendencias que provee una estimación de la utilización futura de los recursos.
  - El Modelo analítico que utiliza técnicas matemáticas para representar el comportamiento de los sistemas de computación.
  - El Modelo de simulación que utiliza al modelo de eventos discretos para dimensionar una nueva aplicación o para predecir los efectos de los Cambios en las aplicaciones existentes.
  - Modelo de Líneas Base que crea un modelo de referencia que refleja con precisión el desempeño y/o rendimiento actual, sobre el cual se puede obtener un modelo predictivo que responsa a ¿qué pasa sí?, se realizan cambios planeados, hasta encontrar la mejor opción para hacerlo.
  - El ciclo de vida definido de las aplicaciones, para estimar los recursos requeridos por una nueva aplicación o un cambio de la misma, considerando que:
    - Se debe mantener el nivel de servicio acordado.
    - Los aspectos de resistencia o redundancia incluidos en el diseño de la aplicación, conforme ésta se desarrolla, se cambia y/o mejora.
- ✓ La creación y mantenimiento del plan de capacidad de recursos y Servicios de TI, que incluye datos de la demanda actual y futura, costos, beneficios, impactos, etc., de:
  - El nivel de utilización de recursos y Servicios de TI, así como también de su desempeño y/o rendimiento.
  - El alineamiento a las Necesidades de Información, Comunicaciones y Control Institucionales.
- ✓ La disponibilidad adecuada de capacidad de TI para cumplir con todos los acuerdos de niveles de servicio.

- ✓ El asesoramiento en materia de capacidad de TI al quienes elaborarán y/o suscribirán los acuerdos de nivel de servicio.
- ✓ El registro y actualización de la información de supervisión del desempeño y/o rendimiento de recursos y Servicios de TI, así como también del incremento o reducción de los mismos, y su disponibilidad para quienes tengan acceso a ella.

El seguimiento y control de los acuerdos firmados, debe ser reportado periódicamente, a fin de conocer las novedades encontradas, así como, las medidas preventivas y/o correctivas requeridas para el cabal cumplimiento de los mismos. Los reportes serán de dos tipos, de situaciones de excepción y las actas de reuniones entre las partes, en ambos casos, contendrán la evaluación del desempeño del personal involucrado, la satisfacción o insatisfacción del cliente, señalarán que medidas preventivas y/o correctivas se han aplicado y se adjuntará el respectivo cronograma con el cual se aplicarán las medidas que se encuentran pendientes a la fecha del reporte.

Para evitar posibles problemas se debe evitar expectativas irreales de los clientes, la Influencia de los vendedores y la falta de seguimiento y control a la Gestión de Capacidad que impidan conocer la posibilidad de que ocurran fallas y/o problemas por falta de capacidad, por otra parte, se deben considerar los ambientes centralizado, distribuido, de desarrollo y de producción, así como la capacitación necesaria para que el personal responsable cuente con el conocimiento necesario para realizar la gestión de capacidad.

2.5 Gestión de la Seguridad

La Gestión de Seguridad es mantener seguros a todos los recursos y Servicios de TI, así como también a sus componentes, lo cual incluye la salvaguarda, confidencialidad, integridad y disponibilidad de información que tiene que ser protegida, para tal efecto se debe contar con elementos de control que permitan

determinar los requisitos de seguridad, garantizar el acceso controlado a los recursos y Servicios de TI, y la provisión controlada de los mismos.

Los beneficios esperados son:

- ✓ El disponer de una forma segura de utilizar los recursos y Servicios de TI, fundamentada en estándar y mejores prácticas.
- ✓ El manejar un nivel de seguridad definido e implementado, con el correspondiente tratamiento en casos de que se produzcan incidentes de seguridad.
- ✓ El control en el acceso a la información que incluye documentación, procedimientos, etc., para prevenir el acceso y uso no autorizado de los mismos, así como también, el control en la provisión de los recursos y Servicios de TI.
- ✓ Los requisitos de seguridad están determinados en los acuerdos de nivel de servicio, de conformidad con la naturaleza del recurso y/o servicio.
- ✓ La confidencialidad que protege la información sensible de revelación no autorizada.
- ✓ La integridad que salvaguarda la exactitud y totalidad de los recursos y Servicios de TI.
- ✓ La disponibilidad que asegura que recursos y Servicios estén disponibles cuando sean requeridos.

El Gobierno de TI debe garantizar la seguridad de los recursos y Servicios de TI, lo cual incluye la administración de la seguridad, plan de seguridad, administración de identidad, administración de cuentas del usuario, pruebas, vigilancia y monitoreo de la seguridad, definición de incidente de seguridad, protección de la tecnología de seguridad, administración de llaves criptográficas, prevención, detección y corrección de software malicioso, seguridad de la red e intercambio de datos sensitivos.

Para tal efecto el dueño del subproceso será responsable de:

- ✓ La administración de la seguridad de forma tal que sus acciones estén alineadas con las Necesidades de Información, Comunicación y Control Institucionales.
- ✓ La elaboración y el mantenimiento del Plan de seguridad de TI, para lo cual tiene que considerar los requerimientos de seguridad de los recursos y Servicios de TI de la Institución, la administración de los riesgos, la cultura, las políticas y procedimientos de seguridad, las inversiones, etc.
- ✓ La asignación, utilización y retiro de la identificación única y las respectivas cuentas de usuario, otorgadas a todos los usuarios internos, externos, sean éstos temporales o definitivos, para que utilicen recursos y Servicios de TI acordes a su ámbito de acción y competencia, las mismas que tienen que estar debidamente solicitadas, definidas, documentadas y autorizadas.
- ✓ La administración de cuentas del usuario mediante el respectivo procedimiento otorga privilegios de acceso a los usuarios de acuerdo al rol autorizado, los mismos que tienen que ser revisados periódicamente.
- ✓ Las pruebas, vigilancia y monitoreo de la seguridad para garantizar que se mantiene el nivel seguridad aprobado, con lo cual se detectarían oportunamente actividades inusuales o anormales.
- ✓ La definición y comunicación de las características de posibles incidentes y problemas de seguridad para que sean debidamente tipificados y oportunamente tratados, a fin de que su impacto en la Institución sea el mínimo, para el efecto se pre definen tanto las acciones específicas requeridas, como las personas que necesitan ser notificadas.
- ✓ La diseminación selectiva de la información para evitar el acceso no autorizado.
- ✓ La administración de llaves criptográficas tendientes a protegerlas de modificación y/o divulgación no autorizadas, lo cual incluye el establecimiento de políticas y procedimientos para generar, certificar,

almacenar, capturar, distribuir, usar, cambiar, revocar, destruir, etc., las llaves criptográficas implantadas en la Institución.

- ✓ La prevención, detección y eliminación de software malicioso: virus, gusanos, spyware, correo basura, software fraudulento desarrollado internamente, etc., mediante bases de datos actualizadas, parches de seguridad y más mecanismos de detección y tratamiento de dicho software.

- ✓ Las técnicas de seguridad y procedimientos asociados a firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos, etc., utilizadas para autorizar acceso y controlar flujos de información desde y hacia las redes.

- ✓ Garantizar que las transacciones de datos sensibles sean intercambiadas únicamente a través de rutas y/o medios confiables con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen.

El seguimiento y control de la seguridad, debe ser reportado periódicamente, a fin de conocer las novedades encontradas, así como, las medidas preventivas y/o correctivas requeridas para el cabal cumplimiento de la misma. Los reportes serán de dos tipos, de situaciones de excepción y las actas de reuniones entre las partes, en ambos casos, contendrán la evaluación del desempeño del personal involucrado, la satisfacción o insatisfacción del cliente, señalarán que medidas preventivas y/o correctivas se han aplicado y se adjuntará el respectivo cronograma con el cual se aplicarán las medidas que se encuentran pendientes a la fecha del reporte.

Para evitar posibles problemas de seguridad se debe considerar estándares, mejores prácticas, regulaciones, estado, privacidad, acuerdos y planes de accesibilidad, costos, riesgos, violaciones, ataques de virus y nuevos requerimientos de seguridad, así como también las correspondiente evaluación, mantenimiento y mejora de la misma.

2.6 Gestión de Continuidad de los Servicios

La Gestión de Continuidad de los Servicios incluye la respectiva planificación; análisis de activos, riesgos y amenazas; administración de contra medidas internas o externas; administrar los planes de acción preventivos, correctivos y de retorno a la normalidad, así como también la ejecución de pruebas y actualización de planes, todo ello asegura la continuidad de las operaciones de la Institución. El Plan de Continuidad de Servicios de TI es también conocido como Plan de Contingencias o Plan de Recuperación de Desastres, sin embargo en esta Tesis mantendrá la primera denominación.

Los beneficios esperados son:

- ✓ La seguridad que los recursos y Servicios críticos de TI sí pueden ser recuperados dentro del los tiempos acordados.
- ✓ La habilidad para continuar operando y proveer un servicio en todo momento, incluso en situaciones de interrupción de la disponibilidad de recursos y/o Servicios de TI, asegurando la supervivencia de la Institución, reduciendo el impacto de un desastre o interrupción considerable.
- ✓ La confianza del cliente en el Plan de Continuidad de los Servicios de TI.
- ✓ El establecimiento del Plan de Continuidad de los Servicios de TI con políticas debidamente comunicadas a todo el personal relacionado con los recursos y Servicios Críticos de TI de la Institución, así como también con las responsabilidades dentro de su área de competencia.
- ✓ La reducción potencial de primas de seguro porque se demuestra a aseguradoras que se están gestionando proactivamente los riesgos de TI.
- ✓ El cumplimiento de regulaciones y la recuperación obligatoria y regulada de los recursos y/o Servicios de TI, otorga credibilidad Institucional frente a Clientes, Estado, Socios de Negocio, Accionistas y la Industria.
- ✓ Las ventajas competitivas traducidas en su oportunidad para demostrar que la Institución sí está en capacidad de Gestionar sus contingencias eficientemente.

El Gobierno de TI debe asegurarse que se realicen las siguientes actividades:

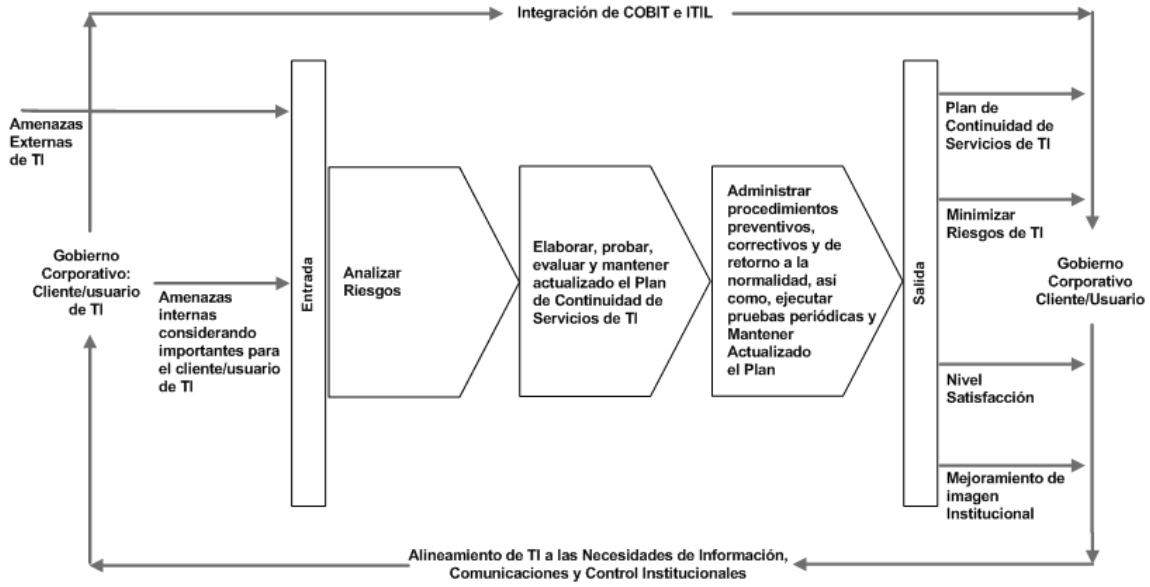


Figura 9. Gestión de Continuidad de los Servicios de TI.

La evaluación de riesgos de los recursos y Servicios críticos de TI se la realiza en base a la experiencia y/o con métodos tales como el Computer Risk Analysis & Management Methodology (CRAMM) de OGC, que permiten identificar las amenazas y vulnerabilidades, a fin de reducir los riesgos a un nivel aceptable. Las amenazas son posibles desastres naturales, accidentes y daños, errores humanos, etc., que atentan contra la continuidad de la prestación de Servicios críticos de TI. Las vulnerabilidades son debilidades ante amenazas a los recursos y Servicios de TI.

Las acciones proactivas que evitan o minimizan los riesgos son:

- ✓ La estrategia de respaldo y recuperación con los procedimientos debidamente elaborados, probados y aprobados, con su correspondiente lista de chequeo, para reducir la probabilidad de interrupciones en la prestación de Servicios críticos de TI. El almacenamiento local, remoto y externo. Probar la recuperación de los recursos y Servicios de TI, de

acuerdo a las prioridades de las Necesidades de Información, Comunicaciones y Control Institucionales.

- ✓ Los sistemas tolerantes a fallas para aplicaciones críticas. La utilización de arreglos de discos protegidos con RAID 5 y discos de spare. La redundancia con componentes de repuesto.
- ✓ La tercerización de servicios si es posible en más de un proveedor. La restauración de software y datos a un punto de referencia común que es consistente.
- ✓ Los controles de seguridad como control de acceso físico a través de tarjetas, huella dactilar, códigos, etc. La utilización de zonas de tiempo y/o puntos de control. La instalación de UPS, UPS de back-up y generador energía.
- ✓ El mantenimiento preventivo para detectar en forma anticipada posibles daños, fallos, desgastes, etc., que eviten interrupciones en la operación de recursos y Servicios de TI. La instalación y prueba del recurso reemplazado.

Para tal efecto el dueño del subproceso será responsable de:

- ✓ Desarrollar, ejecutar, mantener actualizado y en circulación sólo la última versión del Plan de Continuidad de los Servicios críticos de TI, para que en caso de una interrupción de la prestación de los mismos, en un tiempo aceptable para la Institución un recurso o Servicio crítico de TI sea debidamente recuperado, con sus respectivas seguridades, así como también con la disponibilidad de personal y presupuesto, tanto durante la interrupción de la prestación, como para volver a la normalidad.

  Las opciones de recuperación que son:

  - La recuperación en el mismo sitio habitual de trabajo.
  - La recuperación utilizando Acuerdos Recíprocos que se fundamentan en configuraciones similares o idénticas,

procedimientos de administración de cambios integrados y tiempos de procesamiento compartidos.

- La recuperación gradual o "Cold stand by": "cold start fixed" que implica la existencia de una sala de computación en un sitio fijo con todo lo necesario para su cabal funcionamiento; y "Cold start portable" que es un ambiente portable con energía, control de equipos y telecomunicaciones.
- La recuperación intermedia referida como "Warm standby", por las organizaciones que recuperan sus funciones en un plazo de 24 a 72 horas.
- La recuperación inmediata o "Hot stand by" que proporciona la inmediata recuperación de los recursos y Servicios de TI, y usualmente es una extensión de la recuperación intermedia. Tiene 2 enfoques: "Hot start" = cold start + equipos de computación y software; y "Hot start mobile" = una computadora en la parte de atrás de un furgón para una rápida respuesta.
- La recuperación utilizando Acuerdos de reserva ("stand by") que incluye negociar asistencia de terceras partes para utilizar sus planes de contingencia para preparar, equipar el sitio de reserva, comprar e instalar sistemas de computación de reserva, todo esto para recuperar la prestación de Servicios críticos de TI.

✓ Cumplir y hacer cumplir el cronograma de pruebas. La prueba inicial y las periódicas, son la única forma de asegurar que la estrategia seleccionada, los Acuerdos de Nivel de Servicio, la logística, los planes y procedimientos de recuperación de los Servicios críticos de TI, funcionarán realmente en la práctica. Tanto en la prueba inicial como en las periódicas, se evaluarán los resultados obtenidos con la finalidad de aceptar o mejorar la calidad de los procedimientos de dicho Plan. Asegurar que se cuente con los componentes necesarios cuando sean invocados por el Plan de Continuidad de los Servicios de TI. Administrar y distribuir oportuna y eficazmente los componentes, recursos y Servicios de TI, antes, durante y después de una interrupción parcial o total de uno o más de ellos. Revisar

regularmente la calidad de todos los entregables del proceso para asegurar que se mantienen actualizados y sean aceptables para el personal y los ejecutivos inmersos en este proceso de recuperación.

- ✓ Comunicar y mantener el alineamiento al Plan de Continuidad de los Servicios críticos de TI a las Necesidades de Información, Comunicaciones y Control Institucionales.
- ✓ El seguimiento y control de los Acuerdos de Nivel de Servicio firmados, a fin de conocer las novedades encontradas, así como, las medidas preventivas y/o correctivas requeridas para el cabal cumplimiento de los mismos. Negociar y mantener vigentes los contratos de servicios de Mantenimiento y/o recuperación.
- ✓ La debida Coordinación General para lograr reducir riesgos, atender oportunamente a emergencias, evaluar daños, ejecutar el plan de salvamento de los recursos de TI, manejo de crisis y relaciones públicas. Capacitar el equipo de recuperación del negocio para asegurar que tengan los niveles de competencia necesarios.

Los reportes serán de dos tipos, de situaciones de excepción y las actas de reuniones entre las partes, en ambos casos, contendrán la evaluación del desempeño del personal involucrado, la satisfacción o insatisfacción del cliente, señalarán que medidas preventivas y/o correctivas se han aplicado y se adjuntará el respectivo cronograma con el cual se aplicarán las medidas que se encuentran pendientes a la fecha del reporte.

Para evitar posibles problemas se debe obtener el compromiso del personal involucrado en la Gestión de Continuidad de los recursos y Servicios de TI, encontrar la forma para probar cada una de las opciones del Plan de Continuidad de los Servicios de TI, elaborar y ejecutar eficientemente el presupuesto de dicho Plan.

CAPÍTULO 3. CASO DE ESTUDIO DE IMPLEMENTACIÓN DE LA GESTIÓN DE CONTINUIDAD DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN

El Objetivo específico de este capítulo es describir en forma didáctica el Procedimiento elaborado para la implementación de la "Gestión de la Continuidad de Servicios de TI" y aplicado en la Unidad de Sistemas de PETROECUADOR Matriz, para demostrar cómo COBIT e ITIL trabajan conjuntamente para contribuir eficazmente a la continuidad de los Servicios de TI de PETROECUADOR.

3.1 PROCEDIMIENTO DE IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD DE SERVICIOS CRÍTICOS DE TI

Este documento describe paso a paso el procedimiento de Implementación del Plan de Continuidad de Servicios Críticos de TI, considerando lo mínimo indispensable para este fin:

1. Definir dos dueños del Plan, una Política, un Objetivo y un Alcance.
2. Evaluar el impacto en la Institución de la interrupción de los Servicios de TI, para definir cuáles son críticos.
3. Evaluar los riesgos de interrupción de los Servicios Críticos de TI.
4. Evaluar cada situación y definir la Estrategia de Continuidad de Servicios de TI: Recuperación en el mismo sitio cuando la situación lo permita o en un sitio alterno bajo Acuerdos recíprocos entre clientes, con el respectivo Acuerdo de Nivel de Servicio.
5. Asignar dos responsables para cada uno de los Servicios críticos de TI, quienes responderán por la calidad y sistematización de los procedimientos

de obtención de los respectivos Registros Vitales y Respaldos Diarios requeridos para la Restauración, Recuperación y Retorno a la Normalidad, Evaluación y Mejora del Plan. Si no existen tales procedimientos ellos mismos los elaborarán.

6. Conformar el equipo de Emergencia con los dos dueños del Plan y todos los responsables de cada uno de los Servicios Críticos de TI que se necesiten recuperar en cada caso, quienes realizarán la prueba inicial y las pruebas periódicas de sus respectivos procedimientos y evaluarán los resultados obtenidos en cada una de ellas, para realizar ajustes y mejoras a dicho Plan. El mínimo número de integrantes será un Dueño del Plan y un Responsable de un Servicio crítico de TI.
7. Los dueños del Plan y los responsables de cada Servicio Crítico de TI analizarán cada interrupción para decidir cuándo declarar la Emergencia y en forma urgente utilizar tanto el Plan, como el Presupuesto y Autorización de horas extras y extraordinarias, para contrarrestar la situación de emergencia y retornar a la normalidad, a la brevedad posible. Tienen que registrar en una lista de chequeo los pasos ejecutados del Plan y la evidencia del cumplimiento del respectivo Acuerdo de Nivel de Servicio. Deben mantener permanentemente informados a los Ejecutivos inmediatos superiores, mediante Reportes y Comunicaciones en los que consten las novedades, avance y logros alcanzados.

Nota: Si no existe el Presupuesto y/o autorización para horas extras y extraordinarias, el Jefe de la Unidad de Sistemas en forma conjunta con los dueños del Plan y los responsables de los Servicios, elaborarán el correspondiente Presupuesto y obtendrán la respectiva autorización y/o aprobación de la Autoridad pertinente y competente, de acuerdo a la normativa vigente. Para el efecto tienen que considerar tres escenarios antes, durante y después de la Emergencia, y en cada uno de ellos el Personal, Procedimientos, Capacitación, Sitio de Operaciones, Software, Hardware, etc.

Este Procedimiento de implementación fue aplicado con éxito en el caso de estudio realizado en la Unidad de Sistemas de PETROECUADOR.

La estructura utilizada está fundamentada en la integración de COBIT e ITIL, así como también en el Gobierno de TI que a través de sus Servicios se mantiene alineado a las Necesidades de Información, Comunicaciones y Control Institucionales del Gobierno Corporativo, y en los Acuerdos de Nivel de Servicio.

PLAN DE CONTINUIDAD PARA TODOS LOS SERVICIOS CRÍTICOS DE TI

3.1.1 Introducción

Dueños: El Jefe de la Unidad de Sistemas y su delegado.

Política: Todo Servicio crítico de TI cuenta con su correspondiente Acuerdo de Nivel de Servicio, en el que se incluye el tiempo de recuperación requerido, debidamente justificado con el correspondiente análisis costo – beneficio acorde a los riesgos a los que está expuesto.

Objetivo: Contar con un Plan de Continuidad de Servicios de TI, que asegure la rápida recuperación de un Servicio Crítico de TI que se encuentre interrumpido, para aplicarlo cuando el resultado del análisis costo – beneficio sea conveniente a los intereses de la Institución.

Alcance:

- La recuperación inmediata sin considerar las causas de que provocaron tal interrupción, para la cual, se tiene que contar con todos los recursos necesarios para su inmediata recuperación, considerando los escenarios anterior, concurrente y posterior a la interrupción.

- La recuperación gradual de cada uno de los Servicios de TI interrumpidos, para la cual, se tiene que contar con todos los recursos necesarios para su recuperación secuencial considerando los escenarios anterior, concurrente y posterior a la interrupción.

3.1.2 Evaluar el impacto en la Institución de la interrupción de los Servicios de TI, para definir cuáles de todos, son críticos

Evaluar el impacto en la Institución de la interrupción de los Servicios de TI, para definir cuáles son críticos, para el efecto se utilizan métodos tales como análisis de FCE, revisión de Indicadores Clave de Desempeño (KPI), Flujos de procesos, Categorización de la actividad, revisión de la documentación, cuestionarios, entrevistas, talleres, etc., con lo cuales se determina la magnitud, intensificación, recursos y tiempo de recuperación, que se detallan en el cuadro de la siguiente página. Esta evaluación es indispensable para el análisis costo-beneficio del tratamiento de los riesgos de corto, mediano y largo plazo.

- La Magnitud estima sobre la base del volumen, costo, cantidad, etc., el impacto en la Institución, de las consecuencias derivadas de una interrupción de un Servicio de TI, tales como, contratación a proveedores de dichos servicios y dependencia de los mismos, incumplimientos de contrato y/o estándares preestablecidos, gastos asociados, violación a la Ley, inseguridad, pérdida de clientes, pérdida de cuota de mercado, deterioro de la imagen Institucional, etc. Asignar a cada consecuencia el valor de magnitud que le corresponda dentro de la escala de 1 a 10, siendo 1 insignificante y 10 severo:

La Magnitud
1. Retraso en la ejecución de las operaciones
2. Gastos asociados adicionales
3. Contratación adicional y dependencia del mismo
4. Incumplim. de contrato y/o Acuerdo de Nivel de Servicio
5. Incumplimientos de estándares preestablecidos
6. Inseguridad
7. Pérdida de clientes

8. Pérdida de cuota de mercado
9. Violación a la Ley
10. Deterioro de la imagen Institucional

- La Intensificación se estima sobre la base de la velocidad con la cual es probable que la situación causada por la interrupción en la prestación de un Servicio degradará cada vez más, el rendimiento total de los demás Servicios de TI con el consiguiente impacto en la Institución. Asignar a cada consecuencia el valor de intensificación que le corresponda dentro de la escala de 1 a 10, siendo 1 bajo y 10 el más alto:

La Intensificación
1. 2 meses o más.
2. 1 mes
3. 2 semanas
4. 1 semana
5. 2 días
6. 1 día
7. 12 horas
8. 3 horas
9. 1 hora
10. Menos de 15'

- El factor de los recursos se estima sobre la base de las habilidades requeridas para la prestación del Servicio y la complejidad de la infraestructura que lo soporta, y el restablecimiento del mismo luego de una interrupción en la prestación de un Servicio de TI con el consiguiente impacto en la Institución. Asignar a cada factor el valor que le corresponda dentro de la escala de 1 a 10, siendo 1 bajo requerimiento de habilidades y recursos necesarios para mantener el servicio, y 10 requiere un Experto y muchos y valiosos recursos para mantener el servicio:

Los recursos: Habilidades e Infraestructura
1. Soporte Técnico bajo pedido
2. Nuevos procedimientos de respaldo
3. Revisiones de funcionalidades del Portal de respaldo
4. Nuevas adquisiciones de equipo
5. Nuevas versiones, parches del sistema. Infraestructura
6. Nuevas aplicaciones y usuarios o cambios en ellos
7. Cambios de política organizativa o sitio de operación

8. Mantenimiento de registros vitales: BK, BD, umbrales, etc.
9. Cambios de personal crítico
10. Aplicaciones críticas operativas y/o cambios en ellas

- Al tiempo de interrupción en la prestación de un Servicio se lo evalúa por el nivel de importancia derivado del costo que el impacto de tal interrupción tendría sobre la Institución, así como también por la urgencia con la cual tiene que ser recuperado y por la táctica utilizada para recuperación: una recuperación emergente rápida y puntual, o la recuperación lenta y total del Servicio con todas las aplicaciones asociadas, para que esté el Servicio nuevamente esté disponible y sea confiable para su utilización. Asignar a cada Servicio evaluado el valor del cuadro siguiente según corresponda, dentro de la escala de 1 a 10:

Tiempo: Prioridad y tipo de recuperación
1. No importante, no urgente y parcial
2. No importante, no urgente y total
3. No importante, urgente y parcial
4. No importante, urgente y total
5. Importante, no urgente y parcial
6. Importante, no urgente y total
7. Importante, urgente y parcial
8. Importante, urgente y total
9. Crítico para la Institución y parcial
10. Crítico para la Institución y total

En la Evaluación realizada a todos los Servicios de TI, se consideraron la magnitud, intensificación, recursos y tiempo de recuperación, cuyo resultado fue un valor de impacto para cada uno de ellos, y si determinó que si ese valor es igual o superior a 5, entonces se lo considera como un Servicio de TI Crítico:

Id. Servicios críticos de TI	**Impacto**
1. Reactivación Contraseña	5
2. Provisión de telecomunicaciones	5
3. Provisión / Renovación Telefonía móvil	6
4. Creación / Accesos Usuarios	6
5. Correo Electrónico	7
6. Instalación / reparación de Energía regulada y Red de Datos	7
7. Gestión de Respaldos	8
8. Interbase (Datos del RCP)	9
9. Internet/Intranet	9

Evaluar el impacto en la Institución, de las consecuencias derivadas de una interrupción de un Servicio de T, para definir cuáles son críticos. Factores y escala de menor a mayor importancia (1-10)

La Magnitud
1. Retraso en la ejecución de las operaciones
2. Gastos asociados adicionales
3. Contratación adicional y dependencia del mismo
4. Incumplim. de contrato y/o Acuerdo de Nivel de Servicio
5. Incumplimientos de estándares preestablecidos
6. Inseguridad
7. Pérdida de clientes
8. Pérdida de cuota de mercado
9. Violación a la Ley
10. Deterioro de la imagen Institucional

La Intensificación
1. 2 meses o más.
2. 1 mes
3. 2 semanas
4. 1 semana
5. 2 días
6. 1 día
7. 12 horas
8. 3 horas
9. 1 hora
10. Menos de 15'

Los recursos: Habilidades e Infraestructura
1. Soporte Técnico bajo pedido
2. Nuevos procedimientos de respaldo
3. Revisiones de funcionalidades del Portal de respaldo
4. Nuevas adquisiciones de equipo
5. Nuevas versiones, parches del sistema. Infraestructura
6. Nuevas aplicaciones y usuarios o cambios en ellos
7. Cambios de política organizativa o sitio de operación
8. Mantenimiento de registros vitales: BK, BD, umbrales, ...
9. Cambios de personal crítico
10. Aplicaciones críticas operativas y/o cambios en ellas

Tiempo: Prioridad y tipo de recuperación
1. No importante, no urgente y parcial
2. No importante, no urgente y total
3. No importante, urgente y parcial
4. No importante, urgente y total
5. Importante, no urgente y parcial
6. Importante, no urgente y total
7. Importante, urgente y parcial
8. Importante, urgente y total
9. Crítico para la Institución y parcial
10. Crítico para la Institución y total

Servicios de TI	Magnitud		Intensificación		Recursos		Tiempo		Impacto	
Copias en medios digitales e Impresiones	1		3		1		1		1,5	
Correo Electrónico	1		5		10		10		6,5	
Creación / Accesos Usuarios	6		5		6		7		6	
Desarrollo Sistemas de Información	4		1		6		5		4	
Digitalización de documentos	1		4		1		5		2,75	
Digitalización de mapas y planos	1		4		1		5		2,75	
Diseño Grafico (logos, web, presentaciones)	1		4		1		5		2,75	
Diseño y Construcción de mapas	1		4		1		5		2,75	
Escaneo de mapas y planos	1		4		1		5		2,75	
Georeferenciación de mapas y planos	1		4		1		5		2,75	
Gestión de Respaldos	9		6		8		10		8,25	
Impresión de mapas y planos a diferentes escalas	1		4		1		5		2,75	
Instalación / renovación de Software especializado	5		2		1		5		3,25	
Instalación / reparación de Energía regulada y Red de Datos	7		5		10		7		7,25	
Instalación / reparación Telefonía fija	1		5		1		5		3	
Interbase (Datos del RCP)	10		6		10		10		9	
Internet/Intranet	10		6		10		10		9	
Provisión / Renovación Telefonía móvil	7		7		1		7		5,5	
Provisión de energía regulada	4		2		1		5		3	
Provisión de infraestructura (Hw, Sw, Aplicaciones, Telecomunicaciones y equipos auxiliares)	5		1		4		5		3,75	
Provisión de telecomunicaciones	5		4		5		6		5	
Provisión de telefonía fija	4		4		1		5		3,5	
Reactivación Contraseña	6		5		1		7		4,75	
Reparación de equipos TI	4		2		1		7		3,5	
Soporte / Mantenimiento Sistemas de Información	4		2		6		5		4,25	
Soporte básico en Software especializado	4		5		1		7		4,25	
Soporte herramientas de Ofimática: procesador de palabras, hoja electrónica, presentaciones	4		1		1		7		3,25	

Cuadro 8. Evaluar el Impacto

Id. Servicios críticos de TI, porque su impacto es 5 o más dentro de la escala de 1 a 10.	Magnitud		**Intensificación**		**Recursos**		**Tiempo**		**Impacto**	
1. Reactivación Contraseña	6		5		1		7		5	
2. Provisión de telecomunicaciones	5		4		5		6		5	
3. Provisión / Renovación Telefonía móvil	7		7		1		7		6	
4. Creación / Accesos Usuarios	6		5		6		7		6	
5. Correo Electrónico	1		5		10		10		7	
6. Instalación / reparación de Energía regulada y Red de Datos	7		5		10		7		7	
7. Gestión de Respaldos	9		6		8		10		8	
8. Interbase (Datos del RCP)	10		6		10		10		9	
9. Internet/Intranet	10		6		10		10		9	

Cuadro 9. Servicios Críticos de TI

3.1.3 Evaluar los riesgos de interrupción de los Servicios Críticos de TI

El análisis de riesgo se lo realiza considerando únicamente los Servicios Críticos de TI del Catálogo de Servicios, los Acuerdos de Nivel de Servicio y Activos relacionados con las respectivas amenazas a las que están expuestos y la su vulnerabilidad ante dichas amenazas, lo cual implica que se debe contar con el respectivo procedimiento de respaldo, restauración y recuperación desde cero. Esto es indispensable para el adecuado tratamiento de los riesgos aceptando su responsabilidad o transfiriéndola a terceros como un contrato y/o seguro.

Una amenaza**,** es un hecho probable que afecte a la continuidad de Servicios de TI, y que al materializarse probablemente un determinado Servicio será interrumpido:

No.	Amenazas
1	Daño voluntario por personal externo
2	Daño voluntario por personal interno
3	Desastres naturales (Catástrofe)
4	Error accidental de enrutamiento
5	Error de mantenimiento de hardware
6	Error de mantenimiento de software
7	Error de operaciones
8	Error de usuario
9	Escasez de personal
10	Falla de aire acondicionado
11	Falla de software de aplicación
12	Falla de administración de red o servidor
13	Falla técnica de almacenamiento
14	Falla de componente de red
15	Falla técnica de Gateway o Router de red
16	Falla técnica de impresora
17	Falla técnica de interfaz de red
18	Falla técnica de servicio de red
19	Falla técnica de Servidor
20	Falla de comunicaciones
21	Falla de software de red o sistema
22	Falla de UPS, fuente de poder o suministro de energía
23	Fuego o incendio
24	Infiltración de comunicaciones
25	Interceptación de comunicaciones
26	Introducción de virus o software perjudicial
27	Inundación o daño de agua
28	Mal uso de recursos de sistema

29	Manipulación de comunicaciones
30	Rechazo (repudio)
31	Robo por personal de fuera de la Institución
32	Robo por personal de la Institución
33	Suplantac.Identid.Usuario por Proveedores/Contratistas
34	Suplantac.Identid.Usuario por personal externo
35	Suplantac.Identid.Usuario por personal interno
36	Terrorismo
37	Uso no autorizado de una aplicación

Probabilidad de Amenaza: se representa mediante el porcentaje que indica la probabilidad de que la amenaza se materialice en forma deliberada o por casualidad.

La vulnerabilidad, es inversamente proporcional a la capacidad para anticipar, resistir y recuperarse del impacto de una amenaza, por lo tanto está o no en riesgo. La vulnerabilidad es una medida de que tan susceptible a ser afectado está un Servicio de TI (activos que lo apalancan) por la materialización de un riesgo asociado con él. Por ejemplo, ante el riesgo de que un documento crítico no esté disponible al ser consultado en la aplicación que lo grabó, la aplicación no será vulnerable sí comprobó la validez de dicho documento antes de almacenarlo, caso contrario, si es vulnerable a dicho riesgo. Consecuentemente, una vulnerabilidad es una debilidad en los procedimientos de seguridad, diseño, implementación o control interno que podría ser explotada accidental o intencionalmente.

Probabilidad de Vulnerabilidad: se representa mediante el porcentaje que indica la proporción de amenaza que subsiste a pesar de todas las medidas preventivas y correctivas aplicadas oportunamente sobre el componente amenazado en forma deliberada o por casualidad. Por ejemplo si necesitamos alta disponibilidad de las computadoras que disponemos, los posibles cortes de energía se constituyen en una amenaza, en consecuencia, para contrarrestar esta amenaza se dispone de un generador de energía que proveerá de energía cuando se produzca el corte de la red pública, sin embargo al producirse el corte hay un tiempo de cambio de fuente de energía, que apaga y/o daña a las computadoras, esa amenaza que aún subsiste podría ser eliminada con la disponibilidad de un UPS, con lo cual la

Institución no es vulnerable a dicha amenaza, en este caso la confiabilidad será del 100% y el riesgo de falla del 0%. Por tal razón, el riesgo está en función del Impacto (medido por su importancia y/o costo de afectación), la probabilidad de que se materialice la amenaza y la probabilidad de la vulnerabilidad de la Institución ante esa amenaza.

Disponibilidad es el Criterio de Información que con la debida seguridad otorga accesibilidad oportuna a los recursos y capacidades de los procesos. Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

Confiabilidad es el Criterio de Información que mide si es o no apropiada y útil para la gestión y toma de decisiones de IT y la Institución.

El riesgo, disponibilidad y confiabilidad estimados para cada Servicio Crítico de TI son:

Id. Servicios críticos de TI	Riesgo acumulado de falla del	Disponibilidad y Confiabilidad del
1. Reactivación Contraseña	0,021%	99,980%
2. Provisión de telecomunicaciones	0,019%	99,981%
3. Provisión / Renovación Telefonía móvil	0,009%	99,991%
4. Creación / Accesos Usuarios	0,098%	99,902%
5. Correo Electrónico	0,039%	99,962%
6. Instalación / reparación de Energía regulada y Red de Datos	0,025%	99,975%
7. Gestión de Respaldos	0,050%	99,950%
8. Interbase (Datos del RCP)	0,065%	99,935%
9. Internet/Intranet	0,113%	99,887%

A continuación se muestra la Matriz de Riesgos y el Acuerdo de Nivel de Servicio asociado, en el que consta el riesgo, disponibilidad y confiabilidad estimados para cada Servicio Crítico de TI, que tienen que ser debidamente considerados para mantener la Continuidad de los Servicios Críticos de TI.

Evaluar los riesgos de interrupción de los Servicios críticos de TI, utilizando porcentajes y la escala de 1 (bajo) a 10 (alto), según corresponda

Servicio críticos de TI

No.	Amenazas	React.Contraseña					Provis.Telecom.					Prov/Renov.Cel				
		Prioridad	Impacto	n.	Prob.Vuln.	Riesgo	Prioridad	Impacto	n.	Prob.Vuln.	Riesgo	Prioridad	Impacto	n.	Prob.Vuln.	Riesgo
1	Daño voluntario por personal externo	1	5	5	5	0,01	2	5	1	1	0	3	6	1	1	0
2	Daño voluntario por personal interno	1	5	1	1	0,00	2	5	1	1	0	3	6	1	1	0
3	Desastres naturales (Catástrofe)	1	5	1	1	0,00	2	5	1	1	0	3	6			0
4	Error accidental de enrutamiento	1	5			0,00	2	5			0	3	6			0
5	Error de mantenimiento de hardware	1	5			0,00	2	5	1	1	0	3	6			0
6	Error de mantenimiento de software	1	5	1	1	0,00	2	5	1	1	0	3	6			0
7	Error de operaciones	1	5	1	1	0,00	2	5			0	3	6			0
8	Error de usuario	1	5	1	1	0,00	2	5			0	3	6			0
9	Escasez de personal	1	5	1	1	0,00	2	5			0	3	6			0
10	Falla de aire acondicionado	1	5			0,00	2	5			0	3	6			0
11	Falla de software de aplicación	1	5			0,00	2	5			0	3	6			0
12	Falla de administración de red o servidor	1	5			0,00	2	5	1	1	0	3	6			0
13	Falla técnica de almacenamiento	1	5			0,00	2	5			0	3	6			0
14	Falla de componente de red	1	5	1	1	0,00	2	5	1	1	0	3	6			0
15	Falla técnica de Gateway o Router de red	1	5			0,00	2	5	1	1	0	3	6			0
16	Falla técnica de impresora	1	5			0,00	2	5			0	3	6			0
17	Falla técnica de interfaz de red	1	5			0,00	2	5	1	1	0	3	6			0
18	Falla técnica de servicio de red	1	5			0,00	2	5	1	1	0	3	6			0
19	Falla técnica de Servidor	1	5	1	1	0,00	2	5	1	1	0	3	6			0
20	Falla de comunicaciones	1	5			0,00	2	5	1	1	0	3	6			0
21	Falla de software de red o sistema	1	5	1	1	0,00	2	5	1	1	0	3	6			0
22	Falla de UPS, fuente de poder o suministro de energía	1	5			0,00	2	5			0	3	6			0
23	Fuego o incendio	1	5	1	1	0,00	2	5	1	1	0	3	6			0
24	Infiltración de comunicaciones	1	5			0,00	2	5	1	1	0	3	6			0
25	Interceptación de comunicaciones	1	5			0,00	2	5			0	3	6			0
26	Introducción de virus o software perjudicial	1	5	1	1	0,00	2	5			0	3	6			0
27	Inundación o daño de agua	1	5			0,00	2	5			0	3	6	1	1	0
28	Mal uso de recursos de sistema	1	5			0,00	2	5			0	3	6			0
29	Manipulación de comunicaciones	1	5			0,00	2	5	1	1	0	3	6			0
30	Rechazo (repudio)	1	5			0,00	2	5			0	3	6			0
31	Robo por personal de fuera de la Institución	1	5			0,00	2	5	1	1	0	3	6	1	1	0
32	Robo por personal de la Institución	1	5			0,00	2	5	1	1	0	3	6	1	1	0
33	Suplantac.Identid.Usuario por Proveedores/Contratistas	1	5	1	1	0,00	2	5			0	3	6			0
34	Suplantac.Identid.Usuario por personal externo	1	5	1	1	0,00	2	5			0	3	6			0
35	Suplantac.Identid.Usuario por personal interno	1	5	1	1	0,00	2	5			0	3	6			0
36	Terrorismo	1	5	1	1	0,00	2	5	1	1	0	3	6			0
37	Uso no autorizado de una aplicación	1	5	1	1	0,00	2	5			0	3	6			0
	Riesgo acumulado de falla o interrupción=	0,021%					0,019%					0,009%				
	Confiabilidad del	99,980%					99,981%					99,991%				

No.	Amenazas	Creac.Acc.Usuari					Correo Electrónic					Inst.Rep.Red E/D				
		Prioridad	Impacto	n.	Prob.Vuln.	Riesgo	Prioridad	Impacto	n.	Prob.Vuln.	Riesgo	Prioridad	Impacto	n.	Prob.Vuln.	Riesgo
1	Daño voluntario por personal externo	4	6	1	1	0	5	7			0	6	7	1	1	0
2	Daño voluntario por personal interno	4	6	5	5	0	5	7			0	6	7	1	1	0
3	Desastres naturales (Catástrofe)	4	6	1	1	0	5	7	1	1	0	6	7	1	1	0
4	Error accidental de enrutamiento	4	6			0	5	7	1	1	0	6	7	1	1	0
5	Error de mantenimiento de hardware	4	6			0	5	7			0	6	7			0
6	Error de mantenimiento de software	4	6	1	1	0	5	7			0	6	7			0
7	Error de operaciones	4	6	1	1	0	5	7			0	6	7			0
8	Error de usuario	4	6	1	1	0	5	7			0	6	7			0
9	Escasez de personal	4	6	1	1	0	5	7			0	6	7			0
10	Falla de aire acondicionado	4	6			0	5	7			0	6	7			0
11	Falla de software de aplicación	4	6			0	5	7			0	6	7			0
12	Falla de administración de red o servidor	4	6			0	5	7	1	1	0	6	7			0
13	Falla técnica de almacenamiento	4	6			0	5	7			0	6	7			0
14	Falla de componente de red	4	6	1	1	0	5	7			0	6	7			0
15	Falla técnica de Gateway o Router de red	4	6			0	5	7			0	6	7			0
16	Falla técnica de impresora	4	6			0	5	7			0	6	7			0
17	Falla técnica de interfaz de red	4	6			0	5	7			0	6	7			0
18	Falla técnica de servicio de red	4	6			0	5	7			0	6	7			0
19	Falla técnica de Servidor	4	6	1	1	0	5	7			0	6	7			0
20	Falla de comunicaciones	4	6			0	5	7			0	6	7			0
21	Falla de software de red o sistema	4	6	1	1	0	5	7	1	1	0	6	7			0
22	Falla de UPS, fuente de poder o suministro de energía	4	6			0	5	7			0	6	7			0
23	Fuego o incendio	4	6	1	1	0	5	7			0	6	7	1	1	0
24	Infiltración de comunicaciones	4	6			0	5	7	1	1	0	6	7			0
25	Interceptación de comunicaciones	4	6			0	5	7	1	1	0	6	7			0
26	Introducción de virus o software perjudicial	4	6	1	1	0	5	7	1	1	0	6	7			0
27	Inundación o daño de agua	4	6			0	5	7			0	6	7			0
28	Mal uso de recursos de sistema	4	6			0	5	7			0	6	7			0
29	Manipulación de comunicaciones	4	6			0	5	7			0	6	7			0
30	Rechazo (repudio)	4	6			0	5	7			0	6	7			0
31	Robo por personal de fuera de la Institución	4	6			0	5	7			0	6	7			0
32	Robo por personal de la Institución	4	6			0	5	7			0	6	7			0
33	Suplantac.Identid.Usuario por Proveedores/Contratistas	4	6	1	1	0	5	7	1	1	0	6	7			0
34	Suplantac.Identid.Usuario por personal externo	4	6	1	1	0	5	7	1	1	0	6	7			0
35	Suplantac.Identid.Usuario por personal interno	4	6	1	1	0	5	7	1	1	0	6	7			0
36	Terrorismo	4	6	1	1	0	5	7			0	6	7	1	1	0
37	Uso no autorizado de una aplicación	4	6	1	1	0	5	7	1	1	0	6	7			0
	Riesgo acumulado de falla o interrupción=	0,098%					0,039%					0,025%				
	Confiabilidad del	99,902%					99,962%					99,975%				

No.	Amenazas	Gestión Respaldo					Interbase RCP					Internet/Intranet				
		Prioridad	Impacto	n.	Prob.Vuln.	Riesgo	Prioridad	Impacto	n.	Prob.Vuln.	Riesgo	Prioridad	Impacto	n.	Prob.Vuln.	Riesgo
1	Daño voluntario por personal externo	7	8	1	1	0	8	9			0	9	9	1	1	0
2	Daño voluntario por personal interno	7	8	1	1	0	8	9			0	9	9	1	1	0
3	Desastres naturales (Catástrofe)	7	8	1	1	0	8	9	1	1	0	9	9	1	1	0
4	Error accidental de enrutamiento	7	8			0	8	9			0	9	9	1	1	0
5	Error de mantenimiento de hardware	7	8			0	8	9			0	9	9			0
6	Error de mantenimiento de software	7	8			0	8	9			0	9	9			0
7	Error de operaciones	7	8	1	1	0	8	9	1	1	0	9	9			0
8	Error de usuario	7	8	1	1	0	8	9			0	9	9			0
9	Escasez de personal	7	8			0	8	9			0	9	9			0
10	Falla de aire acondicionado	7	8			0	8	9			0	9	9			0
11	Falla de software de aplicación	7	8			0	8	9			0	9	9			0
12	Falla de administración de red o servidor	7	8			0	8	9			0	9	9	1	1	0
13	Falla técnica de almacenamiento	7	8			0	8	9	1	1	0	9	9			0
14	Falla de componente de red	7	8			0	8	9			0	9	9			0
15	Falla técnica de Gateway o Router de red	7	8			0	8	9			0	9	9			0
16	Falla técnica de impresora	7	8			0	8	9			0	9	9			0
17	Falla técnica de interfaz de red	7	8			0	8	9			0	9	9			0
18	Falla técnica de servicio de red	7	8			0	8	9			0	9	9			0
19	Falla técnica de Servidor	7	8			0	8	9			0	9	9			0
20	Falla de comunicaciones	7	8			0	8	9			0	9	9			0
21	Falla de software de red o sistema	7	8			0	8	9			0	9	9	1	1	0
22	Falla de UPS, fuente de poder o suministro de energía	7	8			0	8	9			0	9	9			0
23	Fuego o incendio	7	8	1	1	0	8	9	1	1	0	9	9	1	1	0
24	Infiltración de comunicaciones	7	8			0	8	9			0	9	9	1	1	0
25	Interceptación de comunicaciones	7	8			0	8	9			0	9	9	1	1	0
26	Introducción de virus o software perjudicial	7	8			0	8	9			0	9	9	1	1	0
27	Inundación o daño de agua	7	8	1	1	0	8	9			0	9	9			0
28	Mal uso de recursos de sistema	7	8			0	8	9			0	9	9			0
29	Manipulación de comunicaciones	7	8			0	8	9			0	9	9			0
30	Rechazo (repudio)	7	8			0	8	9			0	9	9			0
31	Robo por personal de fuera de la Institución	7	8			0	8	9			0	9	9			0
32	Robo por personal de la Institución	7	8			0	8	9			0	9	9			0
33	Suplantac.Identid.Usuario por Proveedores/Contratistas	7	8			0	8	9	1	1	0	9	9	1	1	0
34	Suplantac.Identid.Usuario por personal externo	7	8			0	8	9	1	1	0	9	9	1	1	0
35	Suplantac.Identid.Usuario por personal interno	7	8			0	8	9	1	1	0	9	9	1	1	0
36	Terrorismo	7	8	1	1	0	8	9	1	1	0	9	9			0
37	Uso no autorizado de una aplicación	7	8	1	1	0	8	9	1	1	0	9	9	1	1	0
	Riesgo acumulado de falla o interrupción=	0,050%					0,065%					0,113%				
	Confiabilidad del	99,950%					99,935%					99,887%				

Cuadro 10. Evaluar el Riesgo

ACUERDO DE NIVEL DE SERVICIOS (ANS o SLA) PARA MANTENER LA CONTINUIDAD DE LOS SERVICIOS CRÍTICOS DE TI

Fecha: 2008-01-02 Vigencia un año 2008, si no se lo termina con un mes de anticipación, se renovará automáticamente No. 2008-01

El presente acuerdo tiene como finalidad definir las condiciones y características del servicio acordado entre el Proveedor y el Cliente.

Alcance: Acordar las condiciones y características del Nivel de Servicio requerido para asegurar la oportuna rehabilitación de dichos servicios.

Descripción del Servicio: La Unidad de Sistemas a través del personal de Soporte Técnico, cumplirá con todo lo establecido en este Acuerdo y todo lo que haga falta para rehabilitar cada Servicio Crítico de TI, que se encuentre interrumpido. Soporte que será requerido en forma directa por los responsables de dichos Servicios.

Excepciones: Cuando se requiera de los recursos contratados, la Unidad de Sistemas a través del personal de Soporte Técnico, cumplirá y hará cumplir el objeto contractual.

Funcionarios autorizados por el Proveedor: Todo el Personal de Soporte Técnico que dispone.

Funcionarios autorizados por el Cliente: Todos los responsables de los Servicios Críticos de TI.

Observaciones: Los equipos y medios de respaldo determinados por los Responsables de los Servicios se constituyen en elementos vitales para rehabilitar dichos servicios.

CONDICIONES Y CARACTERÍSTICAS, que complementan a los procedimientos de recuperación preestablecidos

Horas de Servicio/Soporte Técnico en sitio, para mantener la Continuidad de los Servicios Críticos de TI, autorizada por el Jefe de la Unidad de Sistemas

Calendario de servicios, días laborables 8 horas: Si Bajo Pedido: Si Todos los días las 24 horas: Obs: Durante la emergencia se trabajará 18 horas al día

Horas anuales acordadas inicialmente: 200 Total de horas utilizadas por trimestre y el saldo:

1er.T.	-26	174	2do.T.	-19	155	3er.T.	-45	110	4to.T.		

Tiempo de respuesta requerido, en horas, para mantener la Continuidad de los Servicios Críticos de TI, una vez formulado el requerimiento ante el Proveedor

IMPORTANCIA	Respuesta a consulta, en:	Plazos máximos para rehabilitar el Servicio y el respectivo seguimiento									
Alta	1 hora	Diagnóstico:	1 hora	Corrección:	1 hora	Cambio:	1 hora	Reparación:	4 horas	Capacitación:	1 hora
Media	2 horas	Diagnóstico:	2 horas	Corrección:	2 hora	Cambio:	2 horas	Reparación:	4 horas	Capacitación:	2 horas
Baja	4 horas	Diagnóstico:	4 horas	Corrección:	4 hora	Cambio:	4 horas	Reparación:	8 horas	Capacitación:	4 horas

Id. Servicios Críticos considerados y datos de recuperaciones:	%disp.	Lug.	Recur.	Fecha	Hora	Responsables	Horas	Lug.	Recur.	Fecha	Hora	Responsables	Horas
1. Reactivación Contraseña: Recuperar y rehabilitar el Servicio	99,980	SIS	LDAP	24/03/2008	8h0	BS, GP	25						
2. Provisión de telecomunicaciones: Recuperar y rehabilitar el Servicio	99,981	PCH	Radio	21/04/2008	10h0	WA	4						
3. Provisión / Renovación Telefonía móvil: Recuperar y rehabilitar el Servicio	99,991	SIS	Celular	13/05/2008	11H0	EA	1						
4. Creación / Accesos Usuarios: Recuperar y rehabilitar el Servicio	99,902	SIS	SAC	12/08/2008	15H0	BS	5						
5. Correo Electrónico: Recuperar y rehabilitar el Servicio	99,962	SIS	Buzón	02/01/2008	8H0	GP	1						
6. Instalación/reparación de Energía regulada y Red de Datos: Recuperar y rehabilitarlo	99,975	SIS	LAN	24/06/2008	17H0	GP	10						
7. Gestión de Respaldos: Recuperar y rehabilitar el Servicio	99,950	SIS	BD	24/06/2008	17H0	MC	2						
8. Interbase (Datos del RCP): Recuperar y rehabilitar el Servicio	99,935	SIS	BD	03/06/2008	18H0	MO	2						
9. Internet/Intranet: Recuperar y rehabilitar el Servicio	99,887	SIS	UCM	12/08/2008	8H0	BS, GP, Proveedor	40						
						Total de horas utilizadas =	90						0

Observaciones:

Por el personal de Soporte Técnico de la Unidad de Sistemas Por los responsables de los Servicios Críticos de TI de la Unidad de Sistemas **Autorizado Jefe SIS**

Nomenclatura: SIS= Unidad de Sistemas. LDAP=Lightweight Directory Access Protocol. PCH= Estación del Pichincha. UCM= Universal Content Management. SAN= Storage Area Network. BD= Base de Datos

Cuadro 11. Acuerdo de Nivel de Servicio

Costos

En este caso de estudio, se ha observado que PETROECUADOR ya dispone de todas las comunicaciones, hardware, software, aplicaciones y recursos necesarios para mantener la Continuidad de los Servicios Críticos de TI, y que además cuenta con el presupuesto necesario para que en casos excepcionales se pueda adquirir lo que haga falta para mantener la Continuidad de los Servicios Críticos de TI. En razón de que el concepto de tiempo de interrupción en la prestación de un Servicio, ya se evaluó en el nivel de importancia el costo que el impacto de tal interrupción tendría sobre la Institución.

PETROECUADOR es la principal fuente de financiamiento del Presupuesto del Estado, en el 2007 aportó con US$3.086'813.393,00 que representa el 19,51% del Presupuesto Inicial del Estado de 2007 US$15.817'954.065,00.

Sin embargo PETROECUADOR no dispone de un Plan de Continuidad de Servicios de TI. Por estas razones esta Tesis se enfocó en la necesidad del caso de estudio, esto es únicamente en la elaboración de los procedimientos que aseguren la Continuidad de cada uno de los Servicios Críticos de TI, que incluyen la obtención de respaldos, restauración y recuperación de cada uno de los Servicios Críticos de TI, con las correspondientes listas de chequeo y actas de entrega recepción de retorno a la normalidad.

Los procedimientos, listas y actas del Plan de Continuidad de cada uno de dichos Servicios constan en el Anexo 1.

3.1.4 Evaluar cada situación y definir la Estrategia de Continuidad de Servicios Críticos de TI

Evaluar cada situación y definir la Estrategia de Continuidad de Servicios de TI: Recuperación en el mismo sitio cuando la situación lo permita o en un sitio alterno

bajo Acuerdos recíprocos entre clientes, con el respectivo Acuerdo de Nivel de Servicio.

La recuperación inmediata sin considerar las causas de que provocaron tal interrupción, para la cual, se tiene que contar con todos los recursos necesarios para su inmediata recuperación, considerando los escenarios anterior, concurrente y posterior a la interrupción.

La recuperación gradual de cada uno de los Servicios de TI interrumpidos, para la cual, se tiene que contar con todos los recursos necesarios para su recuperación secuencial considerando los escenarios anterior, concurrente y posterior a la interrupción.

Requisitos:

- Acuerdos de Nivel de Servicio para ejecutar la correspondiente recuperación, incluye Sitio de operaciones y plan de Recuperación.

- Tecnología para la respectiva recuperación, incluye Infraestructura, aplicación y registros vitales. Lista de todo el personal responsable por la recuperación de los activos que apalancan al Servicio de TI que se requiere recuperar.

- Seguridad en una emergencia es indispensable, incluye seguridades de TI y de todas dependencias afectadas. Seguridades que deben ser supervisadas permanentemente.

- Finanzas para las opciones requeridas de recuperación, que sebe ser debidamente consideradas en los presupuestos.

- Acuerdos recíprocos entre clientes:

    1. Requisitos previos

- Una copia completa de datos y aplicaciones, así como de configuraciones de la infraestructura debería ser almacenada en un sitio externo.
- Cualquier documentación necesaria y Servicios de TI operativos.
- El espacio libre suficiente para manipular los datos y aplicaciones requeridas.
- Las aseguradoras deben conocer este acuerdo recíproco.
- Las instalaciones adecuadas.
- Una lista de contactos de personal de ambas partes será distribuida.
- Un acuerdo firmado y vigente.

2. Proveer espacio suficiente para oficinas, áreas y reuniones de trabajo, bodega, caja fuerte, etc.

3. Proveer de equipo de oficina, teléfono, fax, e-mail, Correo, mensajero, y servicios de mensajero, papel de escribir, fotocopia, y otras instalaciones.

4. Proveer de equipo de computación: Pcs, impresora, copias de seguridad (carga de datos inicial), copias de seguridad (dentro de provisión de servicio), especifique la plataforma de la cual los datos deberían ser hechos una copia de seguridad, soporte de especialistas, etc.

5. La lista de restricciones y posibles salvedades.

6. Procedimiento de terminación parcial o total del acuerdo.

7. Derechos y obligaciones de las partes.

8. Pruebas del plan

Estrategia de Continuidad de Servicios de TI										
Servicio Crítico de TI	Dueño	Opción Recuperac.		Necesidades Institucionales	Riesgo acumulado de falla del	Cliente	Acuerdos de Nivel de Servicio			Procedi-mientos
		Inmediato	Gradual				SLA	Tiempo de respues.	Tiempo de recuper.	
1. Reactivación Contraseña	BS y MC	Si	Si	LDAP y AS/400	0,021%	Personal	2008-01	1 hora	30 min.	Anexo 1.1
2. Provisión de telecomunicaciones	WA	No	Si	Inalámbricas y puntos de red	0,019%	Dependencias	2008-01	1 hora	4 a 28 horas	Anexo 1.2
3. Provisión / Renovación Telefonía móvil	EA	Si	Si	Planes e Internet	0,009%	Ejecutivos	2008-01	1 hora	4 a 28 horas	Anexo 1.3
4. Creación / Accesos Usuarios	BS y MC	Si	Si	LDAP y AS/400	0,098%	Personal	2008-01	1 hora	30 min.	Anexo 1.1
5. Correo Electrónico	GP	Si	Si	Toda la Institución	0,039%	Personal	2008-01	1 hora	4 a 28 horas	Anexo 1.4
6. Instalación / reparación de Energía regulada y Red de Datos	WA	Si	Si	UPS	0,025%	Dependencias	2008-01	1 hora	4 a 28 horas	Anexo 1.5
7. Gestión de Respaldos	MC	Local y sitio de almace-namiento	Si	CCP	0,050%	Personal	2008-01	1 hora	4 a 28 horas	Anexo 1.6
8. Interbase (Datos del RCP)	MO	Si	Si	GEF, REI	0,065%	Jefes	2008-01	1 hora	4 a 28 horas	Anexo 1.7
9. Internet/Intranet	GP	Si	Respaldos	Toda la Institución	0,113%	Personal	2008-01	1 hora	4 a 28 horas	Anexo 1.8

Cuadro 12. Estrategia de Continuidad de Servicios Críticos de TI

3.1.5 Asignar dos responsables para cada uno de los Servicios Críticos de TI, quienes responderán por la calidad y sistematización de los procedimientos.

Asignar dos responsables para cada uno de los Servicios críticos de TI, quienes responderán por la calidad y sistematización de los procedimientos de obtención de los respectivos Registros Vitales y Respaldos Diarios requeridos para la Restauración, Recuperación y Retorno a la Normalidad, Evaluación y Mejora del Plan. Si no existen tales procedimientos ellos mismos los elaborarán. PETROECUADOR no dispone de un Plan de Continuidad de Servicios de TI, por esta razón esta Tesis se enfocó en la necesidad del caso de estudio, esto es, en la elaboración de los procedimientos que aseguren la Continuidad de cada uno de los Servicios Críticos de TI, que incluyen la obtención de respaldos, restauración y recuperación de cada uno de los Servicios Críticos de TI, con las correspondientes listas de chequeo y actas de entrega recepción de retorno a la normalidad. Los procedimientos, listas y actas del Plan de Continuidad de cada uno de dichos Servicios constan en el Anexo 1. La documentación mínima de cada Servicio Crítico de TI consta de:

1. Un diagrama de bloque.
2. Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0.
3. Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles.
4. Lista de chequeo que incluye a los procedimientos anteriores.
5. Acta de entrega – recepción del retorno a la normalidad.

Id. Servicio crítico de TI	Cargo	Teléfono	Unidad
1. Reactivación Contraseña	Especialista Informática II	5932-2524072	Sistemas
2. Provisión de telecomunicaciones	Especialista Telecomunicaciones IV	5932-2524072	Sistemas
3. Provisión / Renovación Telefonía móvil	Especialista Comunicaciones II	5932-2524072	Sistemas
4. Creación / Accesos Usuarios	Especialista Informática II	5932-2524072	Sistemas
5. Correo Electrónico	Especialista Informática III	5932-2524072	Sistemas
6. Instalación / reparación de Energía regulada y Red de Datos	Especialista Telecomunicaciones IV	5932-2524072	Sistemas
7. Gestión de Respaldos	Especialista Informática II	5932-2524072	Sistemas
8. Interbase (Datos del RCP)	Especialista Informática III	5932-2524072	Sistemas
9. Internet/Intranet	Especialista Informática III	5932-2524072	Sistemas

Cuadro 13. Responsables de cada Servicio Crítico de TI

Registros vitales:

1. Identificar el inventario archivos vitales:

- Consulte con el funcionario responsable de la coordinación de la emergencia sobre los archivos vitales de cada Servicio Crítico de TI.
- Las responsabilidades estatutarias y reguladoras de la organización, así como las de revisión y emergencia existente, deben ser incluidas en el inventario de archivos vitales indicando el Servicio Crítico de TI al que pertenecen.
- La documentación correspondiente a la revisión creada para la planificación de respuesta a emergencias y a la fase de asesoramiento de riesgo y estado de preparación de emergencia. Las oficinas responsables de estos trabajos deben entregar dichos documentos.

- Los archivos corrientes de oficinas que son responsables de realizar proyectos, funciones críticas y conservar derechos, y
- Todas las series de registro calificadas como vitales para asegurar la confiabilidad e integridad de los datos de los Servicios Críticos de TI.

2. El inventario de archivos vitales debería incluir:
   - El nombre de la oficina responsable de la serie de registro o sistema de información electrónico que contiene información vital.
   - El título de cada serie de registro o sistema de información que contiene información vital.
   - La identificación de cada serie o sistema que contiene archivos vitales que operan la emergencia o archivos vitales que se relacionan con derechos.
   - El medio en el cual los archivos son registrados.
   - La posición física para almacenamiento externo de copias de la serie de registro o sistema.
   - La frecuencia con la cual los archivos deben ser actualizados.

Inventario de Registros Vitales

No.	Nombre	Ubicación física	Período de Retención	Archivo físico	Formato	Copia Ubic.Física	Id. Servicio crítico de TI 1	2	3	4	5	6	7	8	9	Comentario
1	Respaldos D, S, M, A y E.	CCP	S, M	Cartucho LTO4	LTO4	Casillero				1	1		1	1	1	
2	Usuario y contraseña, y doc. pedidos	CCP	3 meses	Plan	Libro	Casillero	1			1						
3	Red de Telecomunicaciones	CCP	Indefinida	Red y Configuraciones	Mapa	Casillero		1								
4	Lista Equipos Telefonía móvil	CCP	Indefinida	Equipos Telefonía móvil	Lista	Casillero			1							
5	Cuentas de Correo	CCP	3 meses	Cuentas de correo	Lista	Casillero					1					Renova o cancela
6	Red de datos y eléctrica	CCP	Indefinida	Red	Mapa	Casillero						1				
7	Metadata y caracterísctcias BD y BK	CCP	Indefinida	Metadata	Carpeta	Casillero								1		Más uno por mes
8	Distribución ancho de banda y pórticos	CCP	Indefinida	Servicios	Lista	Casillero									1	
							1	1	1	2	2	1	1	2	2	

Nomenclatura:		
Respaldos Diarios con retención Semanal, Semanales con retención Mensual, Mensuales con retención Anual, Anuales y Especiales con retención Indefinida.		
Casillero de la bóveda del Banco de Pichincha.		
Plan de Continuidad de Servicios Críticos de TI.		
BD Bases de datos y sus características de multi archivo. BK archivos de respaldo y sus características de multi archivo.		
CCP: Centro de Cómputo.		
Id. Servicio crítico de TI		
1. Reactivación Contraseña	4. Creación / Accesos Usuarios	7. Gestión de Respaldos
2. Provisión de telecomunicaciones	5. Correo Electrónico	8. Interbase (Datos del RCP)
3. Provisión / Renovación Telefonía móvil	6. Instalación / reparación de Energía regulada y Red de Datos	9. Internet/Intranet

Cuadro 14. Inventario de Registros Vitales

3.1.6 Conformar el equipo de Emergencia con los dos dueños del Plan y todos los responsables de cada uno de los Servicios Críticos de TI que se necesiten recuperar.

Conformar el equipo de Emergencia con los dos dueños del Plan y todos los responsables de cada uno de los Servicios Críticos de TI que se necesiten recuperar en cada caso, quienes realizarán la prueba inicial y las pruebas periódicas de sus respectivos procedimientos y evaluarán los resultados obtenidos en cada una de ellas, para realizar ajustes y mejoras a dicho Plan. El mínimo número de integrantes será un Dueño del Plan y un Responsable de un Servicio crítico de TI.

- Responsabilidades y autoridad del Equipo de Emergencia:

    1. Desarrollar, promover y mantener el Proceso de Gestión de Continuidad de Servicios de TI.
    2. Coordinar revisiones del Proceso para lograr mayor objetividad y simplicidad, así como de poner en práctica las mejoras identificadas.
    3. Presidir las reuniones y trabajos de recuperación para verificar que todos los pasos fueron completados y el objetivo del proceso fue conseguido.
    4. Controlar y examinar los trabajos pendientes, la disponibilidad y el cumplimiento de los Acuerdos de Nivel de Servicio.
    5. Elaborar las comunicaciones para mantener informados del avance de los trabajos de recuperación a ejecutivos, clientes y equipos de recuperación.

3.1.7 Los dueños del Plan y los responsables de cada Servicio crítico de TI deben realizar las siguientes actividades antes, durante y después de una interrupción de cada uno de dichos Servicios.

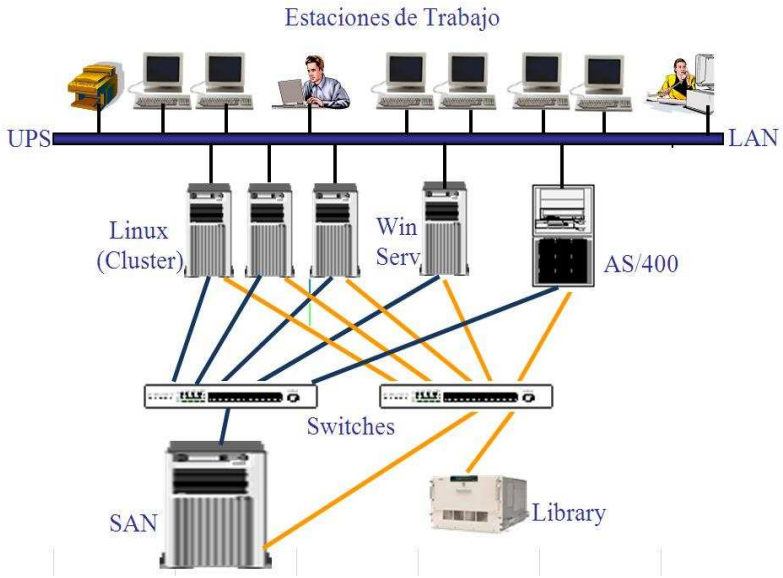


Figura 10. Recursos de TI

1 ANTES DE QUE OCURRA UNA EMERGENCIA:

Comprobar que la documentación mínima esté completa y descrita en detalle y acompañadas con todos los procedimientos, guías y más documentos que se necesiten para que se tenga éxito en el procesamiento de las transacciones en cada escenario y se las pueda justificar debidamente ante auditoria, lo cual incluye que esté:

1. Determinado, desarrollado y probado el Procedimiento a seguir para realizar el procesamiento alterno durante la emergencia (incluye la capacitación, entrenamiento, seguimiento, evaluación y acciones correctivas), en forma detallada y paso a paso.
2. Definida la lista del Personal principal y alterno, detallando para cada uno de ellos el rol a desempeñar durante la emergencia, con sus responsabilidades e indicando a quien

tienen que reportarse y bajo la coordinación de quién van a trabajar. El personal designado debe estar disponible cuando sea convocado, por el tiempo necesario y bajo el horario requerido.

3. Asignados y reservados los recursos mínimos indispensables para garantizar la continuidad de las operaciones.
4. Aplicado el Plan de Respaldos de Software, Aplicación y Datos guardando los medios magnéticos del respaldo en el mismo sitio de operación y fuera del sitio habitual de operaciones.
5. Registrada la información diaria necesaria para establecer y controlar el corte del procesamiento de los datos hasta la última transacción válida realizada antes de que se produzca una suspensión temporal o definitiva. El corte debe ser realizado en forma diaria.
6. Realizada la capacitación y entrenamiento a todos los integrantes del Plan de Continuidad en los roles y actividades que deben asumir y realizar, respectivamente, a fin de que estén en capacidad de cumplir con las responsabilidades asignadas, que son indispensables para garantizar la correcta aplicación y cumplimiento de lo dispuesto para este escenario, lo cual es vital para el éxito los dos escenarios siguientes.
7. Implantado, probado y ajustado este escenario del Plan de Continuidad, hasta que responda a las diferentes situaciones en las que podría operar PETROECUADOR.

2 DURANTE UNA EMERGENCIA (REAL O SIMULACRO):

Comprobar que la documentación mínima esté con todos los procedimientos, guías y más documentos que se necesiten para que se tenga éxito en el procesamiento de las transacciones en este

escenario y se pueda justificar debidamente dicho procesamiento ante auditoria, lo cual incluye que esté:

1. Calificada la Emergencia y comunicada a los respectivos Responsables de cada uno de los elementos críticos involucrados en ella.
2. Convocado el personal necesario, los dueños del Plan y los responsables de los Servicios Críticos de TI afectados, conforme a lo establecido en la documentación.
3. Disponibles los recursos, procesos, sistemas, aplicaciones o procedimientos de la Empresa (elementos críticos) necesarios para la recuperación en el mismo sitio de operación o Sitio alterno.
4. Realizada la capacitación y entrenamiento a todos los integrantes del Plan de Continuidad en los roles y actividades que deben asumir y realizar, respectivamente, a fin de que estén en capacidad de cumplir con las responsabilidades asignadas, que son indispensables para garantizar la correcta aplicación y cumplimiento de lo dispuesto para este escenario, lo cual es vital para el éxito del escenario “DESPUÉS DE LA EMERGENCIA”.
5. Implantado, probado y ajustado este escenario del Plan de Continuidad, hasta que responda a la situación en la que tiene que operar PETROECUADOR.
6. Confirmado que se hayan procesado la totalidad de las transacciones ejecutadas antes del período de emergencia y en caso de existir transacciones pendientes, determinar el mecanismo para su correcto y oportuno procesamiento.
7. Duplicados y disponibles los respaldos para realizar la recuperación de Software, Aplicación y/o Datos que se requieran para lograr la continuidad de las operaciones durante la emergencia.

8. Aplicado el “Procedimiento que se tiene que seguir para realizar el procesamiento alterno durante la emergencia”, definido en forma detallada y paso a paso.
9. Mantenida diariamente la información necesaria para establecer y controlar el corte del procesamiento de los datos desde la última transacción válida realizada antes de declarar la emergencia y hasta la última transacción válida realizada durante la emergencia. Sobre esa base diariamente, determinar los valores de corte, registrarlos y dejar las respectivas autorizaciones, aprobaciones y pistas de auditoría con la documentación suficiente y pertinente, para garantizar la confiabilidad de los mismos y poder volver a la normalidad en dicho procesamiento.
10. Ejecutado las pruebas de seguridad, mantenimiento, soporte, recuperación, disponibilidad, funcionalidad, desempeño, necesarias para el mantenimiento del plan, cumplir con lo programado, ajustarlo con las correcciones necesarias para que sea idóneo el Plan.

3 DESPUÉS DE LA EMERGENCIA (REAL O SIMULACRO):

Comprobar que se hayan realizado las siguientes acciones únicamente después de una emergencia y se las haya documentado con todos los procedimientos, guías y mas documentos que se necesiten para que tengan éxito y se puedan justificar debidamente ante auditoria, lo cual incluye que esté:

1. Realizada la capacitación y entrenamiento a todos los integrantes del Plan de Continuidad en los roles y actividades que deben asumir y realizar, respectivamente, a fin de que estén en capacidad de cumplir con las responsabilidades

asignadas, que son indispensables para garantizar la correcta aplicación y cumplimiento de lo dispuesto para este escenario.

2. Implantado, probado y ajustado este escenario del Plan de Continuidad, hasta que responda a la situación en la que tiene que operar PETROECUADOR.
3. Incorporada en las bases de datos Institucionales todas las transacciones procesadas durante el período de la emergencia, que dieron como resultado los valores de los dos cortes antes citados.
4. Confirmada:
   - La exactitud de los valores determinados en el corte del procesamiento de los datos correspondientes a la última transacción válida realizada antes de declarar la emergencia.
   - La validez de la documentación de soporte.
   - Que se haya registrado dicho valor en forma exacta y previa al procesamiento de las transacciones pendientes a la fecha de la declaratoria de emergencia, así como las ejecutadas durante el período de emergencia.
5. Confirmado que se hayan procesado la totalidad de las transacciones ejecutadas durante el período de emergencia y en caso de existir transacciones pendientes, determinar el mecanismo para su correcto y oportuno procesamiento.
6. Confirmado sobre la base de los dos numerales anteriores:
   - La exactitud de los valores determinados en el corte del procesamiento de los datos correspondiente a la última transacción válida realizada durante el período de emergencia.
   - La validez de la documentación de soporte.
7. Entendido que en forma previa al procesamiento de las transacciones que se encontraban pendientes y las que fueron ejecutadas luego del período de emergencia, se debe

registrar el valor de corte obtenido y confirmado en el literal anterior.

8. Verificado que el valor de corte fue registrado oportuna y adecuadamente para iniciar el procesamiento de las transacciones que se encontraban pendientes y las que fueron ejecutadas luego del período de emergencia.
9. Entendido que una vez que se ha superado la emergencia y se cuentan con las facilidades necesarias para su normal funcionamiento, se deben realizar las pruebas de aceptación hasta lograr su aprobación.
10. Disponer de toda la documentación necesaria para respaldar todo el proceso realizado antes, durante y después de la emergencia, la cual será útil para el mejoramiento del Plan de Continuidad de Servicios Críticos de TI, así como para justificar las inquietudes de Auditoria.
11. Declarada la finalización de la emergencia, por parte del respectivo Responsable del Servicio Crítico de TI.
12. Vuelto a la normalidad para realizar el procesamiento de las transacciones, bajo las condiciones de operación normal.

4. Decidir cuándo declarar la Emergencia.

5. En forma urgente utilizar tanto el Plan, como el Presupuesto y Autorización de horas extras y extraordinarias, para contrarrestar la situación de emergencia y retornar a la normalidad, a la brevedad posible.

6. Tienen que registrar en una lista de chequeo los pasos ejecutados del Plan y la evidencia del cumplimiento del respectivo Acuerdo de Nivel de Servicio.

7. Deben mantener permanentemente informados a los Ejecutivos inmediatos superiores, mediante Reportes y Comunicaciones en los que consten las novedades, avance y logros alcanzados.

- La difusión del Plan de Continuidad de Servicios de TI entre todos los ejecutivos de la Institución, Jefes y miembros de los equipos de recuperación; Plan que entra en vigencia desde la fecha de su comunicación.

- El nombramiento del Coordinador General del Plan de Continuidad de Servicios de TI y de los Equipos de Recuperación. La obligatoriedad de concurrir al Sitio de Recuperación tan pronto como sean convocados, para realizar la correspondiente evaluación de la situación y fundamentado por el respectivo análisis costo – beneficio aplicar el correspondiente Acuerdo de Nivel de Servicio.

- La elaboración de tres informes por Servicio de TI interrumpido, en los que se deja constancia de:

- El Informe del diagnóstico de la situación que incluye el análisis detallado del costo – beneficio de la recuperación, dirigido al Jefe del Área Usuario, quien lo debe aprobar, y suministrar los registros vitales antes de iniciar la recuperación acordada.

- El Informe detallado de la recuperación realizada, que incluye los registros vitales con los que se recuperó y los datos iniciales de la transacción con la continúan las operaciones hasta que se retorne a la situación de normalidad nuevamente.

- El Informe detallado del retorno a la normalidad, que incluye los registros vitales con los que se retornó a la normalidad, así como también los datos iniciales de la transacción con la continúan las operaciones.

- El informe de evaluación de la recuperación realizada, que incluye las novedades detectadas, conclusiones y recomendaciones, que permitan confirmar la validez del Plan y/o realizar los ajustes urgentes antes de su siguiente utilización.

3.2 RESULTADOS OBTENIDOS

3.2.1 Desde las Perspectivas del CMI

Una vez que se han probado y aplicado con éxito las estrategias de la "Perspectiva de Desarrollo", esto es haber:

- Definido y mantenido el Acuerdo de Nivel de Servicio que ha permitido realizar las recuperaciones de cada uno de los Servicios, cuando éstos lo requirieron, cuyo detalle consta en las correspondientes Listas de Chequeo y las respectivas Actas de Entrega Recepción.

- Se ha realizado la Evaluación del Impacto de la interrupción de los Servicios, cuyo resultado consta en el cuadro 8, lo cual permitió determinar los Servicios Críticos de TI que se muestran en el cuadro 9 y que correspondieron al puntaje de 5 o más, sobre 10.

- Luego se evaluaron los riesgos de cada uno de los Servicios Críticos de TI, obteniéndose así los valores que se muestran en el cuadro 10.

- Estos resultados fueron considerados para elaborar el Acuerdo de Nivel de Servicio requerido para asegurar la continuidad de los Servicios Críticos de TI, el cual se presenta en el cuadro 11.

- Considerando la realidad actual de PETROECUADOR y la Unidad de Sistemas, se definieron las estrategias de continuidad, para los escenarios anterior, concurrente y posterior a una situación de emergencia.

- Se procedió a elaborar las estrategias de continuidad para antes, durante y después de una emergencia, con la respectiva documentación mínima.

- Las estrategias fueron probadas con éxito y aplicadas satisfactoriamente en los casos de emergencia documentados en las correspondientes Listas de Chequeo de los Anexos del 1.1 al 1.8.

A continuación se han probado y aplicado con éxito las estrategias de la "Perspectiva del Proceso ", en cada uno de los Servicios críticos de TI:

1. Reactivación Contraseña y 4. Creación / Accesos Usuarios

Los beneficios obtenidos mediante las estrategias de seguimiento, control, respaldo y recuperación de contraseñas son:

- Los usuarios pueden trabajar con los recursos de TI para la ejecución de sus labores cuotidianas.
- Los usuarios pueden cambiar la contraseña y proteger sus recursos, la misma que en caso de olvido o bloqueo puede se reactivada en el horario de 7h00 a 22h00.
- Se alerta a los usuarios a no divulgar sus contraseñas ni a dejar su sitios de trabajo con sesiones de trabajo abiertas.
- Las contraseñas caducan cada mes, lo cual reduce el riesgo de suplantación de identidad.

Los beneficios obtenidos mediante las estrategias de seguimiento, control, respaldo y recuperación de la de creación / accesos de usuarios son:

- Permite el uso controlado de los recursos de TI.
- La asignación de roles y sus responsabilidades.

- La incorporación de seguridades para evitar accesos no autorizados.
- Posibilita la administrar los recursos de TI.

2. Provisión de telecomunicaciones

Los beneficios obtenidos mediante las estrategias de seguimiento, control, respaldo y recuperación de las telecomunicaciones son:

- El manejo de la información a través de redes WAN y MAN que unen a las dependencias descentralizadas.
- El compartir información y recursos entre los usuarios.
- Facilitar el trabajo distribuido del Sistema de Registro de Proveedores y acceso remoto al Portal e Intranet.
- Se detectó un daño intermitente en el enlace Pichincha-Alpallana, gracias a lo cual se aplicó el procedimiento de recuperación, lográndose solucionar dicho daño.

3. Provisión / Renovación Telefonía móvil

Los beneficios obtenidos mediante las estrategias de seguimiento, control, respaldo y recuperación de la telefonía móvil son:

- Poder comunicarse desde cualquier lugar a la empresa y entre ejecutivos.
- Tener información en tiempo real con Internet móvil.

5. Correo Electrónico

Los beneficios obtenidos mediante las estrategias de seguimiento, control, respaldo y recuperación del correo electrónico son:

- Envío y recepción de información en forma inmediata en los ámbitos nacional e internacional.
- Facilidad de difusión de comunicaciones personales e Institucionales.
- Permite la realización del comercio electrónico, como es el caso de la subasta en línea.
- Realizar las invitaciones a ofertar a proveedores en forma transparente, rápida y eficiente.
- El disponer de un medio de comunicación entre Ejecutivos y el personal para impartir órdenes y disposiciones, así como también el seguimiento respectivo a la ejecución de trabajos hasta la correspondiente entrega – recepción de los mismos.
- Reduce el uso de papel.
- Minimiza los tiempos de trámites, al facilitar la administración de contenido empresarial, como el de correspondencia, para cuyos flujos de trabajo y seguimiento utilizan correo electrónico.

6. Instalación / reparación de Energía regulada y Red de Datos

Los beneficios obtenidos mediante las estrategias de seguimiento, control, respaldo y recuperación de energía regulada y red de datos son:

Red eléctrica controlada:

- Tener energía regulada.
- Evitar que los equipos se dañen por variaciones de voltaje y por suspensión del servicio de la red eléctrica pública.
- Evitar en los cortes de energía ya que causan pérdida de datos e información de los usuarios.
- Evitar proactivamente daños de UPS y/o Sistema de baterías, por suspensión la prestación del servicio de energía eléctrica de la red Pública.

Red de datos controlada:

- Tener acceso a la Información en tiempo real.
- Utilizar los sistemas de información y demás servicios de TI.
- Evitar el reproceso de las transacciones.

7. Gestión de Respaldos

Los beneficios obtenidos mediante las estrategias de seguimiento, control, respaldo y recuperación de respaldos son:

- Disponer de todos los datos, información, aplicaciones y más elementos indispensables para poder recuperar la información a un determinado punto de sincronismo y consistencia, para lo cual se utiliza la librería SL500 de Storage Tek, cartuchos reutilizables y no reutilizables, así como también agentes para Windows, Linux y AS/400, archivos abiertos bajo Windows y Linux de 32 y 64 bits, agentes para respaldar bases de datos Oracle, y finalmente Llaptops & Desktops.

- Aplicar la política de respaldos, que consiste en tener:
  - Un conjunto de cartuchos para el respaldo diario para los días Lunes, Martes, Miércoles y Jueves, para cinco semanas, los mimos que se reutilizan cada mes.
  - Un conjunto de cartuchos para el respaldo semanal para los días viernes de las cinco semanas del mes, los mimos que se reutilizan cada mes.
  - Un conjunto de cartuchos para el respaldo mensual para los meses de enero a noviembre, los mimos que se reutilizan cada año.
  - Un conjunto de cartuchos para el respaldo anual y especiales, los mimos que no se reutilizan.

- Los Controles que se aplican a la Biblioteca Storage Tek SL500 incluyen:

    - La seguridad de acceso físico al contenido de la biblioteca, restringido sólo al personal autorizado que tenga acceso a la biblioteca y a los medios fuera de línea.
    - La seguridad de que la construcción física sí puede resistir el fuego externo / calor (por lo menos dos horas).
    - La disponibilidad de una copia de cartuchos en un casillero de seguridad del Banco del Pichincha, Agencia El Ejido.
    - El inventario permanente de todos los medios de almacenamiento y de los archivos almacenados en la biblioteca, con información del contenido, versiones y ubicación.
    - El registro de entregas y recepciones de todos los medios de almacenamiento, archivos y documentación trasladados a y desde la biblioteca. La documentación incluye: Procedimientos de operación; Documentación de Sistemas y de Programas; Procedimientos Especiales; Documentos Fuente de Entrada; Documentos de Salida; Plan de Continuidad.

- Estar en capacidad de realizar las restauraciones y/o recuperaciones de datos, bases de datos y archivos.
- El mantener las copias de los cartuchos de respaldo, en los casilleros del banco para poderlos utilizar en caso de emergencias.

8. Interbase (Datos del RCP)

Los beneficios obtenidos mediante las estrategias de seguimiento, control, respaldo y recuperación de Interbase son:

- Optimizar la estructura de la base de datos y el tiempo de respuesta de las transacciones de Registro de Proveedores.
- Recuperar la base de datos cuando se han producido daños en la fragmentación de los registros y/o daño o pérdida de los archivos de la base de datos.
- Mantener operativa a la base de datos y sus réplicas.

9. Internet/Intranet

Los beneficios obtenidos mediante las estrategias de seguimiento, control, respaldo y recuperación de Internet / Intranet son:

- Mantener la alta disponibilidad del Servicio de Internet e Intranet.
- Proteger la imagen institucional tanto de ataques externos, así como también de errores de operación.
- Apalancar la gestión diaria interna y externa, que se apoya en sistemas web enable, Internet e Intranet.

En las pruebas realizadas:

- Se verificó que el Plan de Continuidad de Servicios Críticos de TI si está completo y es preciso.
- Se evaluó el desempeño del personal que participó en el ejercicio.
- Se evaluó el entrenamiento y la conciencia de continuidad de los responsables de los Servicios.
- Se evaluó la coordinación entre responsables de Servicios y clientes, así como también con proveedores externos.
- Se midió la capacidad del personal de Soporte Técnico para realizar la recuperación y emitir los informes correspondientes.
    - Se realizó la prueba de la estrategia que se aplica antes de una situación de emergencia, que consistió en disponer de un escenario para la prueba real, lo cual incluye mesas o

escritorios en el área apropiada de recuperación de operaciones hasta transportar e instalar equipos de respaldo, teléfonos, etc.

- Se realizó la prueba de la estrategia que se aplica durante una situación de emergencia, que consistió en realizar las tareas operativas para probar la continuidad de los Servicios, con entrada de datos, llamadas telefónicas, el procesamiento de los sistemas de información, el manejo de las órdenes y el movimiento del personal, los equipos y los proveedores.
- Se realizó la prueba de la estrategia que se aplica después de una situación de emergencia, que consistió en devolver todos los recursos al lugar que les corresponde, desconectar los equipos y devolver al personal, eliminar todos los datos de la compañía de los sistemas de terceros, así como también evaluar formalmente el plan e implementar las mejoras requeridas.

Luego se han probado y aplicado con éxito las estrategias de la "Perspectiva del Cliente", de cumplir y hacer cumplir el Acuerdo de Nivel de Servicio en cada uno de los Servicios críticos de TI, cuyos beneficios son:

- El cumplimiento de todo lo establecido en el Acuerdo de Nivel de Servicio y todo lo que haga falta para rehabilitar cada Servicio Crítico de TI, que se encuentre interrumpido. Soporte que será requerido en forma directa por los responsables de dichos Servicios.
- Que los equipos y medios de respaldo determinados por los Responsables de los Servicios se constituyeron en elementos vitales para rehabilitar dichos servicios, con los procedimientos de recuperación preestablecidos.
- Que se establecieron las horas de Servicio/Soporte Técnico en sitio, para mantener la Continuidad de los Servicios Críticos de TI, autorizada por el Jefe de la Unidad de Sistemas.

- Que se acordó el horario de soporte en sitio durante los días laborables en 8 horas, con el respaldo de que se dispondrá de este servicio especializado, bajo pedido, de las horas que se requieran para asegurar la continuidad y/o recuperación en los tiempos acordados.
- Que se disponen de 200 horas anuales inicialmente, cuya utilización se la realiza a través de los supervisores de los contratos respectivos, cada vez que estén por terminar, se hará una reposición de las mismas, a fin de que siempre se cuente con el Soporte idóneo en forma oportuna.
- Que se acordaron los siguientes plazos para la atención especializada:

Tiempo de respuesta requerido, en horas, para mantener la Continuidad de los Servicios Críticos de TI, una vez formulado el requerimiento ante el Proveedor											
IMPORTANCIA	Respuesta a consulta, en:	Plazos máximos para rehabilitar el Servicio y el respectivo seguimiento									
Alta	1 hora	Diagnóstico:	1 hora	Corrección:	1 hora	Cambio:	1 hora	Reparación:	4 horas	Capacitación:	1 hora
Media	2 horas	Diagnóstico:	2 horas	Corrección:	2 horas	Cambio:	2 horas	Reparación:	4 horas	Capacitación:	2 horas
Baja	4 horas	Diagnóstico:	4 horas	Corrección:	4 horas	Cambio:	4 horas	Reparación:	8 horas	Capacitación:	4 horas

Finalmente se han probado y aplicado con éxito las estrategias de la "Perspectiva Socio-Económica", para Contribuir a la continuidad de la Institución para asegurar su rentabilidad socio-económica, como sigue:

Id. Servicios Críticos considerados y datos de recuperaciones:	%disp.	Lug.	Recur.	Fecha	Hora	Responsables	Horas
1. Reactivación Contraseña: Recuperar y rehabilitar el Servicio	99,980	SIS	LDAP	24/03/2008	8h0	BS, GP	25
2. Provisión de telecomunicaciones: Recuperar y rehabilitar el Servicio	99,981	PCH	Radio	21/04/2008	10h0	WA	4
3. Provisión / Renovación Telefonía móvil: Recuperar y rehabilitar el Servicio	99,991	SIS	Celular	13/05/2008	11H0	EA	1
4. Creación / Accesos Usuarios: Recuperar y rehabilitar el Servicio	99,902	SIS	SAC	12/08/2008	15H0	BS	5
5. Correo Electrónico: Recuperar y rehabilitar el Servicio	99,962	SIS	Buzón	02/01/2008	8H0	GP	1
6. Instalación/reparación de eEnergía regulada y Red de Datos: Recuperar y rehabilitar	99,975	SIS	LAN	24/06/2008	17H0	GP	10
7. Gestión de Respaldos: Recuperar y rehabilitar el Servicio	99,950	SIS	BD	24/06/2008	17H0	MC	2
8. Interbase (Datos del RCP): Recuperar y rehabilitar el Servicio	99,935	SIS	BD	03/06/2008	18H0	MO	2
9. Internet/Intranet: Recuperar y rehabilitar el Servicio	99,887	SIS	UCM	12/08/2008	8H0	BS, GP, Proveedor	40
					Total de horas utilizadas =		90

En el caso de los Servicios que exceden al tiempo de recuperación acordado, cabe dejar aclarado que se incumplió el plazo, sin embargo, la interrupción del Servicio fue parcial y no incidió negativamente en la disponibilidad, confiabilidad y continuidad de las operaciones de la Institución y por lo tanto su importancia fue baja y sí se precautelaron los intereses Institucionales al no afectar a la rentabilidad socio-económica.

3.2.2 Observación de los Resultados Obtenidos

La Institución en la que se realizó el Caso de estudio es PETROECUADOR y la dependencia responsable de las Comunicaciones y Tecnologías de la Información es la Unidad de Sistemas que depende de la Gerencia Administrativa, como se puede ver en el organigrama de la página siguiente. La información actualizada disponible de PETROECUADOR se encuentra disponible en la dirección URL: http://www.petroecuador.com.ec

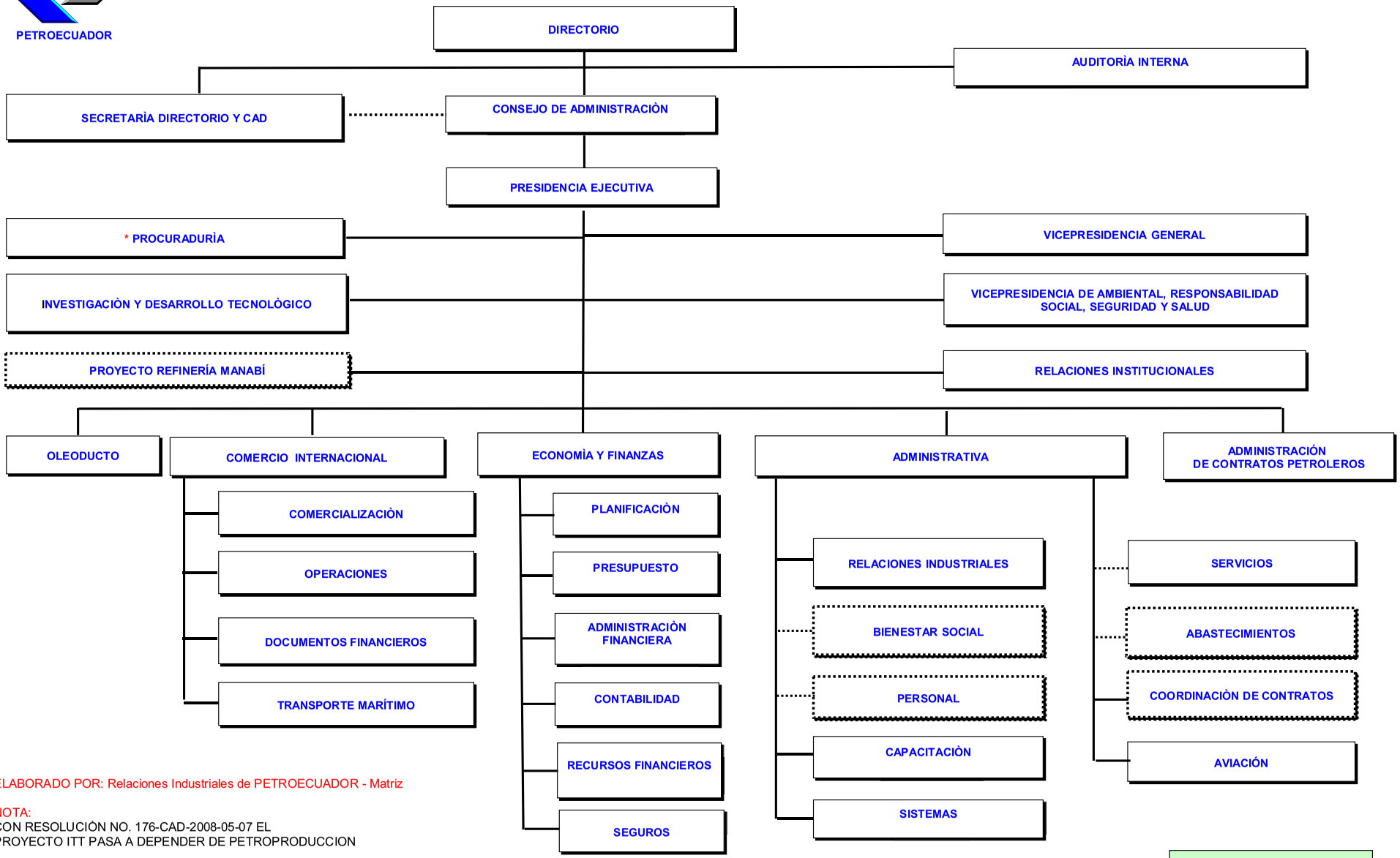
Cabe indicar que PETROECUADOR disponía de personal suficiente y competente, para administrar las comunicaciones y tecnologías de la Información, de modo centralizado utilizando un mainframe o Host el IBM 4381 R14, con aproximadamente 200 usuarios y las siguientes funcionalidades:

- Comunicaciones: Ocho Especialistas.
- Tareas de Tiempo compartido: Dos especialistas.
- Base de datos: Dos especialistas.
- Tiempo real, procesamiento de transacciones: Dos especialistas.
- Seguridades: Dos especialistas.
- Operación: Cinco especialistas.
- Desarrollo: 15 especialistas.

Al Cambiar de estructura de una sola Empresa a un Holding con una Matriz, una Gerencia Operativa y tres Filiales, dicho personal se repartió en cada una de ellas, razón por la cual desde el año de la Creación de PETROECUADOR se perdió el concepto de equipo y de personal de respaldo y apoyo, hecho que se ha agravado aún más con las renuncias voluntarias del personal de Sistemas, que ha causado la acumulación de funciones y consecuentemente la falta de tiempo para el trabajo importante y proactivo, todos estos hechos han incrementado los riesgos y por lo tanto, es vital un Plan de Continuidad de los Servicios Críticos de TI.

PETROECUADOR

ORGANIGRAMA ESTRUCTURAL DE P E T R O E C U A D O R - M A T R I Z



ELABORADO POR: Relaciones Industriales de PETROECUADOR - Matriz

NOTA:
CON RESOLUCIÓN NO. 176-CAD-2008-05-07 EL
PROYECTO ITT PASA A DEPENDER DE PETROPRODUCCION

* **GRUPO DE TRABAJO PROCURADURÍA GENERAL: ASESORÍAS Y CONTRATOS Y PROCESOS JUDICIALES**
* SE ENCUENTRA EN PROCESO POR PARTE DEL DIRECTORIO EL TRASLADO DEL PROYECTO ITT A PETROPRODUCCIÓN

ÀREAS INFORMALES:

Actualizado al 6 de Junio de 2008

La estructura actual de la Unidad de Sistemas es plana, atiende a aproximadamente 600 usuarios y cubre 10 servidores con las siguientes funcionalidades:

- Comunicaciones y mantenimiento: Cuatro Especialistas.
- Tareas de Tiempo compartido: Dos especialistas a tiempo parcial.
- Base de datos: Dos especialistas a tiempo parcial.
- Tiempo real, procesamiento de transacciones: No hay especialistas.
- Seguridades: No hay especialistas.
- Operación: Dos especialistas.
- Desarrollo: Seis especialistas.

Datos que evidencian tanto el crecimiento en servidores y usuarios, como la disminución del personal, razón por la cual, antes de la Investigación realizada en esta Tesis PETROECUADOR:

- No disponía de un Catálogo de Servicios Críticos de TI.
- No disponía de un Plan de Continuidad de Servicios Críticos.
- No disponía de experiencia y conocimientos necesarios para elaborar el Plan de Continuidad de Servicios Críticos considerando impacto, riesgos, cuadro de mando integral, etc.
- Había contratado la implementación de una solución de Empresa por Resultados (EPR), y estaba en proceso el definir un proyecto de un Sistema Integrado de Información (SII) que incluye la correspondiente Administración del Cambio, Organización por Procesos, una Solución empresarial tipo Enterprise Resource Planning (ERP), Cuadro de Mando Integral (CMI), etc., que cubran las necesidades de las áreas administrativas, financieras y técnicas.
- Tiene que cumplir las recomendaciones del Examen Especial PEC-AIN-002-2008, al “Inventario y Funcionamiento de la Infraestructura Informática y Tecnológica en el Sistema PETROECUADOR”, por el período comprendido entre el 1 de enero de 2006 al 31 de julio de 2007, porque el artículo 92 de la Ley Orgánica de la Contraloría General del Estado dispone que “*Las recomendaciones de auditoría, una vez comunicadas a las*

instituciones del Estado y a sus servidores, deben ser aplicadas de manera inmediata y con el carácter de obligatorio; serán objeto de seguimiento y su inobservancia será sancionada por la Contraloría General del Estado". Las recomendaciones que tienen relación con este tema son:

Recomendación No. 1 dirigida al Gerente Administrativo: "*Dispondrá al Jefe de la Unidad de Sistemas de PETROECUADOR, que con el apoyo de los Jefes de las Unidades de Sistemas y Telecomunicaciones del Sistema, conformen una comisión que analice la organización interna y las funciones de estas unidades, y su ubicación en la estructura de las empresas del Holding. Sobre la base del resultado de su análisis, esta comisión presentará al Presidente Ejecutivo, por intermedio de la Gerencia Administrativa, una propuesta de revisión a la ubicación en la estructura orgánica de las mencionadas unidades, buscando homogeneidad funcional, y con una coordinación para la formulación de políticas y estándares en materia de informática, liderada por la Unidad de Sistemas de PETROECUADOR".* Tiene un plazo de 60 días calendario para su cumplimiento.

La Recomendación No. 1 tiene un plazo de 60 días contados a partir de la notificación es decir desde el 2008-07-30 hasta el 2008-09-30.

Recomendación No. 4 dirigida al Gerente Administrativo: "*Dispondrán y facilitarán de los recursos necesarios para que los Jefes de las Unidades de Sistemas y Telecomunicaciones del Sistema PEC elaboren y presenten para su aprobación planes de contingencia y continuidad de negocio para sus respectivas áreas. Para ello, deberá existir una coordinación entre los jefes de las mencionadas unidades del Sistema PETROECUADOR, a fin de mantener criterios corporativos, y procurar el apoyo con la tecnología de unas filiales en el caso de presentarse contingencias en otras. Posterior a la aprobación, realizarán el seguimiento para asegurar la implementación y difusión de estos planes entre el personal de sus respectivas unidades*".

Tiene un plazo de 180 días calendario a partir del cumplimiento de la recomendación 1.

La Recomendación No. 4 tiene un plazo de 180 días contados a partir del cumplimiento de la Recomendación No.1, que se contaría a partir del 2008-10-01, debiendo concluir aproximadamente el 2009-03-28, lo cual es concordante con la Planificación anual 2008 y 2009.

El Procedimiento de Implementación del Plan de Continuidad de Servicios Críticos de TI, y el trabajo en equipo desarrollado para elaborar esta Tesis incluyó: la designación de un responsable del proceso, la definición de una Política, Objetivo, Alcance, Evaluación del Impacto en la Institución de la interrupción de los Servicios de TI, Evaluación de los Riesgos de interrupción de los Servicios Críticos de TI, Acordar el Nivel de Servicio que asegure la continuidad, Evaluar cada situación para definir la estrategia de Continuidad de Servicios Críticos de TI, Asignar responsables a cada uno de los Servicios Críticos de TI, Conformar el Equipo de Emergencia, Aplicar las estrategias en los escenarios antes, durante y después de una emergencia.

Se consideró a cada uno de los siguientes Servicios Críticos de TI y para cada uno de ellos se elaboró la documentación mínima.

Id. Servicios Críticos de TI:

1. Reactivación Contraseña
2. Provisión de telecomunicaciones
3. Provisión / Renovación Telefonía móvil
4. Creación / Accesos Usuarios
5. Correo Electrónico
6. Instalación / reparación de Energía regulada y Red de Datos
7. Gestión de Respaldos desde 1980-
8. Interbase (Datos del RCP)
9. Internet/Intranet

Documentación mínima:

1.x.1 Un diagrama de bloque que incluya la Planificación y Ejecución

1.x.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

1.x.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

1.x.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

1.x.5 Acta de ER del retorno a la normalidad.

PETROECUADOR gracias a la implementación del Procedimiento de Implementación del Plan de Continuidad de Servicios Críticos de TI, y al trabajo en equipo pudo lograr:

- Definir y elaborar el Catálogo de Servicios Críticos de TI.
- Incorporar en los términos de referencia y contratos, las cláusulas de respaldo, restauración y recuperación acordes al Plan de Continuidad de Servicios Críticos de TI, tales como ERP y Mantenimiento de Equipos, etc.
- Tener el conocimiento y experiencia necesarios y suficientes para definir, elaborar, desarrollar, implantar y probar periódicamente el Plan de Continuidad de los Servicios Críticos de TI.
- Empezar una etapa de mejoramiento continuo del Sistema de Control Interno, para lo cual el Gerente Administrativo mediante nota inserta en el memorando 342-AIN-2008 de 2008-07-16 dispuso a “REI: Cagar la matriz de recomendaciones al sistema y preparar comunicaciones a las unidades que correspondan para firma de GAD” fecha 2008-07-22. El Gerente mediante memorando NO.332-REI-2008 de 2008-07-30 dispuso el cumplimiento de las recomendaciones de Auditoría, para disponer del Plan

de Continuidad de Servicios Críticos considerando impacto, riesgos, cuadro de mando integral, etc., hasta el 2009-04-12.

Servicios Críticos recuperados: 1 y 4. Creación / Accesos Usuarios y Reactivación Contraseña:

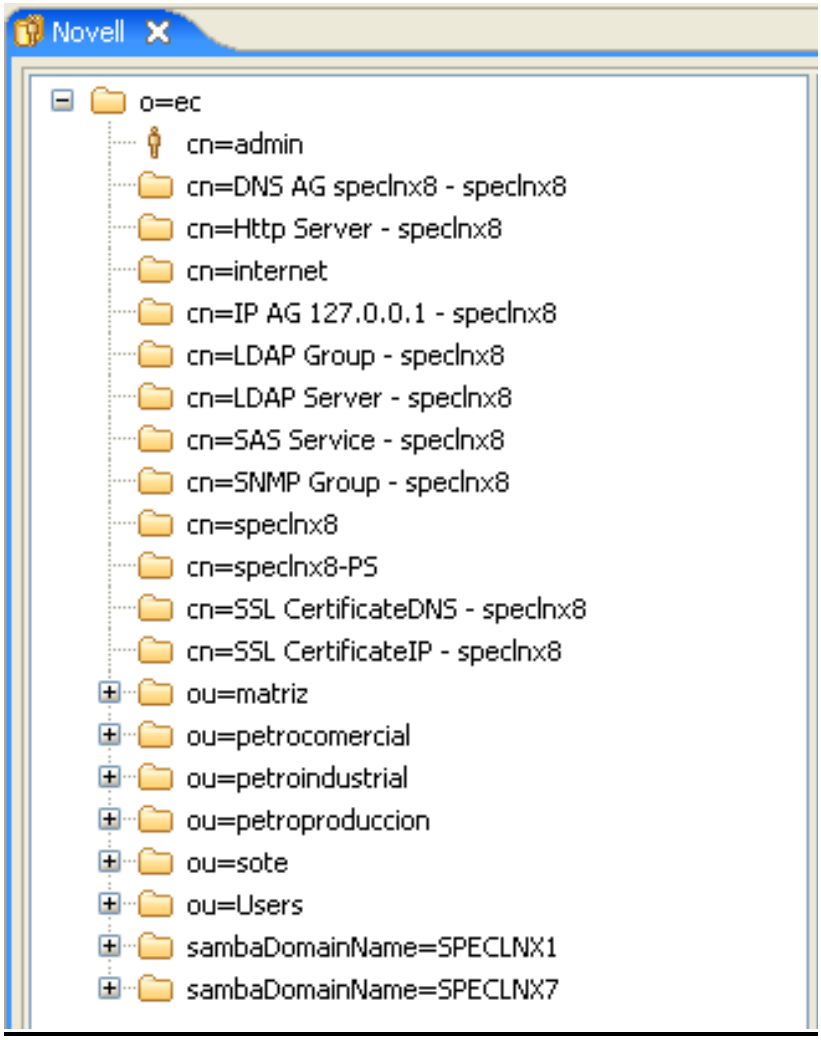
Los Grupos de usuarios, usuario y listas de autorización y acceso que dispone PETROECUADOR corresponden a los servidores de Red y el AS/400, mediante los cuales se prestan los Servicios de TI a las áreas administrativas, financieras y técnicas.

Los usuarios se crean bajo pedido escrito del Jefe del área que lo solicita, en el cual se especifica la aplicación, la autorización y accesos requeridos. La Unidad de Personal notifica apenas se produce una incorporación de nuevo personal o la salida del mismo, a fin de que se inhabiliten las cuentas de dichos usuarios.

La administración de las autorizaciones y accesos en la Red se la realiza con eDirectory y Secure Login, mediante un árbol de recursos que se muestra a continuación, que está replicado en varios servidores para recuperarse de inmediato ante fallas del servidor principal. El número de usuarios registrados es de 611. En cambio en el AS/400 se lo realiza con las facilidades del sistema operativo OS/400. El número de usuarios registrados es de 151.

Los nombres de los usuarios se estandarizaron utilizando la inicial del nombre y todo el apellido, al crear el usuario se le asigna como contraseña el mismo “user ID” y se le obliga a cambiarla en el primer ingreso al sistema.

Las contraseñas expiran cada 30 días. La cuenta del usuario se bloquea luego del tercer intento de ingreso fallido.



Árbol de Recursos

Servicio Crítico recuperado: 2. Provisión de Telecomunicaciones:

Los enlaces de radio que dispone PETROECUADOR son los siguientes

EQUIPOS DE TELECOMUNICACIONES SISTEMA PETROECUADOR MATRIZ

NO.	ENLACE	MARCA	MODELO	TECNOLOGÍA	DISTANCIA km	CAPACIDAD DEL EQUIPO	CAPACIDAD INSTALADA	CAPACIDAD UTILIZADA	CAPACIDAD DISPONIBLE	Bw AUTORIZADO SENATEL (MHz)
1	ALPALLANA - CERRO PICHINCHA	HARRIS	TRUEPOINT 4040	PORTADORA FIJA	5,55	16E1	16E1	16E1	NINGUNA	28
2	CAPACITACION - CERRO PICHINCHA	HARRIS	TRUEPOINT 4040	PORTADORA FIJA	5,63	8E1	2E1	2E1	14E1	3,5
3	DISPE. MEDICO - CERRO PICHINCHA	HARRIS	TRUEPOINT 4040	PORTADORA FIJA	6,06	8E1	2E1	2E1	14E1	3,5
4	TRASPORTES - CERRO PICHINCHA	HARRIS	TRUEPOINT 4040	PORTADORA FIJA	4,69	8E1	2E1	2E1	14E1	3,5
5	VIC. AMBIENTAL - CERRO PICHINCHA	HARRIS	TRUEPOINT 4040	PORTADORA FIJA	4,22	8E1	2E1	2E1	14E1	3,5
6	ADM. CONTRATOS - CERRO PICHINCHA	HARRIS	TRUEPOINT 4040	PORTADORA FIJA	4,48	8E1	2E1	2E1	14E1	3,5
7	AVIACION - CERRO PICHINCHA	HARRIS	TRUEPOINT 4040	PORTADORA FIJA	4,72	8E1	2E1	2E1	14E1	3,5

El enlace Alpallana – Cerro Pichincha tiene un "Sistema 1+1", para que en caso de falla del primero tome el control el segundo radio transmisor de microondas en

forma automática y avisa al Administrador que un equipo está dañado. No hay respaldo para la antena, porque de acuerdo a la experiencia hay muy poca probabilidad de que se dañe.

En la repetidora del Pichincha las seguridades existentes cubren el acceso a la Estación que Petrocomercial asignó, hay un control del dueño de la Hacienda, con llave de la puerta y cadena, registro de bitácora, malla de protección alrededor de la estación y las 24 horas un Guardia de Seguridad de Petrocomercial que lleva otra bitácora. La energía eléctrica es de la acometida de la Red de energía Pública, se dispone además de un generador de emergencia y un sistema de baterías. El Switch capa 2 que hace la conmutación a todas las estaciones está protegido por UPS. Como repuestos del Sistema de Telecomunicaciones hay un Radio Frequency Unit (RFU) y un equipo Signal Processing Unit (SPU) de respaldo para. Los equipos están bajo el período de garantía y el mantenimiento preventivo es trimestral.

Con estas acciones se han atendido oportunamente los casos de emergencia que se han presentado.

Servicio Crítico recuperado: 3. Provisión / Renovación Telefonía Móvil:

En cumplimiento de la disposición Gubernamental y del Ministro de Minas y Petróleos dada mediante oficio 462-ADM-2008, que se terminen todos los contratos de telefonía celular que mantenga PETROECUADOR y sus Empresas Filiales y se proceda a contratar dicho servicio con Alegro (TELECSA), para el efecto se realizaron los trámites pertinentes, producto de lo cual, Alegro en lo referente a su cobertura GSM informó: que cubre todo el país incluyendo las provincias en las cuales PETROECUADOR opera, tales como, Galápagos, Esmeraldas, Sucumbíos, Orellana, Napo, Pastaza, Morona Santiago y Zamora Chinchipe; que cuenta con Radiobases de todo el país; que llega a 13 millones de ecuatorianos; que cubre las carreteras del país; el portafolio de equipos; sus tarifas nacionales: Alegro – Alegro a US$0,060, Alegro a Movistar o Porta a

US$0,120, llamadas a teléfonos fijos US$0,075, tarifas internacionales con Mondo: USA, Canadá y demás países del plan a US$0,090, llamadas a teléfonos fijos US$0,140 y a teléfonos móviles US$0,280; las características de sus planes; y, los servicios adicionales que presta.

En la invitación a cotizar, la oferta de Alegro fue la más ventajosa para PETROECUADOR, tanto en costo por minuto, como en los servicios de valor agregado, por lo que no se renovará el plan con Movistar que venció el 2008-06-21[11].

Los resultados obtenidos son que PETROECDUADOR dispone de 17 líneas contratadas con Alegro que operan a su entera satisfacción y una línea de teléfono Black Berry contratada a Movistar, hasta que Alegro notifique que ya puede brindar dicho servicio.

Servicio Crítico recuperado: 5. Correo Electrónico

El Servicio de Correo Electrónico se lo presta a través de Sendmail del servidor speclnx2 bajo Linux Red Hat Advanced Server versión 3, que está instalado en un servidor HP Proliant DL580 con 6GB de RAM, dos procesadores Xeon de 1.60ghz, adquirido en 2003-04-03, tipo rack, cuyo respaldo se obtiene a través la librería SL500 marca de con dos drivers LTO4, se activa, desactiva, verifica el estado y reinicia, mediante “sendmail.LK {start, stop, status, restart}” y se lo monitorea en forma manual y automática mediante IPCHECK: “http://*ip:pórtico.*”.

La Versión de Sendmail e la 8.12.11, está por migrarse a la última que es la 8.13.8 que viene en la versión AS 5) la limitante de la actualización es el hecho de que se trabaja con Lifekeeper v2.1
El Sendmail interactúa con soluciones de trabajo colaborativo tales como Teamware y Universal Content Management: Portal e Intranet, así como también

[11] Memorando 920-SIS-2008 de 2008-07-03, de Gerente Administrativo a Ejecutiva de cuenta de Movistar (Octecel S.A.) y anexos, 55 p.

con NetScape para tratamiento personalizado de carpetas de correo electrónico. Send mail le hace el envío del correo a Teamware, recibe y reparte a los servidores de Administración de Contratos Petroleros (ACP), Vicepresidencia Ambiental (VAS), Gerencia de Oleoducto (OLE), Unidad de Capacitación (CAP), Teamware.

El Sendmail está instalado y parametrizado en dos servidores adicionales, a fin de cubrir cualquier emergencia, y subir automáticamente y de inmediato el servicio, gracias a las facilidades de fail over de Lifekeeper v.2.1 Además está también integrado a los Sendmail de los servidores ubicados en los demás edificios en los que funcionan las demás dependencias de PETROECUADOR.

La capacidad de recuperación automática está implementada mediante Lifekeeper, fail over, quien a través de un cluster sabe si un servidor deja de prestar el servicio y automáticamente pasaría del Speclnx2 al speclnx1, y únicamente habría que montar la partición compartida en el speclnx1 así: #mount /cluster2
El Sendmail es exclusivo y excelente para MTA (mail transport Agent) y para servidor de correo.

El Sendmail opera bajo la protección de las Políticas de seguridad del FortiGate *100* (1K), Forti OS 3.0, para bloqueo anti-spam, antivirus, IPS, Firewall, IPS, IDC, debidamente configurado, además está integrado a abuse.net que permite confirmar que el servidor sí está protegido ante las vulnerabilidades que allí detectan. También está integrado con el LDAP (archivo sendmail.cf), Intranet e internet.

Desde 1999 está operativo, todos los correos están en el servidor, por lo que hay que monitorear el uso del disco. El servidor de correo está protegido por el antivirus Trend Micro Server Protect.

Servicio Crítico recuperado: 6. Instalación / Reparación de Energía Regulada y Red de Datos:

Las redes de Energía regulada que posee Petroecuador cubren las necesidades de los clientes, fue construida este año. La Red de Datos de la Gerencia de Comercio Internacional, las Unidades de Sistemas, Procuraduría, Auditoría y Coordinación de Contratos también fue construida este año, y cuenta con equipos Cisco que soportan la demanda de servicio actual y futura.

Se cuenta con conexiones de Fibra Óptica a Petrocomercial, Petroindustrial y el edificio El PINAR, Las demás son 1Gbit y de 100MBps, se cuenta con switches y gabinetes de piso.

Se dispone de una Storage Area Network que conecta a un Storage 9970V Hitachi, seis HP Proliant DL560, dos HP Proliant DL360, un Blade, una Librería StorageTek SL500.

Las redes se ven afectadas por las adecuaciones que se realizan en los pisos, así como también por cambios radicales en la distribución de las estaciones de trabajo, que se alejan de los puntos de energía y/o de datos existentes.

Se disponen de switches Cisco de repuesto para reemplazar los dañados, hasta que sean reparados o se los reemplace definitivamente, y se adquieran otros de repuesto.

Servicio Crítico recuperado: 7. Gestión de Respaldos:

Los respaldos se vienen realizando conforme al Plan, esto es en forma diaria, semanal, mensual, anual y especiales, sin embargo el cambio de unidades de respaldo desde Exabyte Mammoth-2 con cartucho de 60GB sin comprimir y 150GB en formato comprimido, que deben ser pasados a los cartuchos de 800GB sin comprimir y 1600GB en formato comprimido.

Además aún no se realiza la Administración del ciclo de vida de los datos, que permita considerar el período de retención, el tiempo de vida útil de los cartuchos, la naturaleza de los datos, la validez de los mismos, su descarte, etc.
La falta de espacio de disco como área de trabajo para pruebas de validez de los respaldos, fusiones, o descarte, no ha permitido aún el mantenimiento proactivo de los mismos.

Aún no se ha planificado la forma de obtener los respaldos completos, incrementales (sólo lo cambiado a partir del último respaldo completo o incremental) y diferenciales (sólo lo cambiado a partir del último respaldo completo).

Ya se han incorporado las facilidades de respaldar archivos abiertos, archivos de Base de Datos Oracle compatible 100% con RMAN, archivos a través de la SAN, archivos de Desktops y Laptops a través de la Red LAN bajo los sistemas operativos Windows y Linux RedHat, y Librerías y objetos de AS/400.

Servicio Crítico recuperado: 8. Interbase (datos del RCP):

Por disposición del Consejo de Administración de PETROECUADOR se cambió el nombre de Sistema Único de Calificación de Oferentes (SUCO) por el RCP.

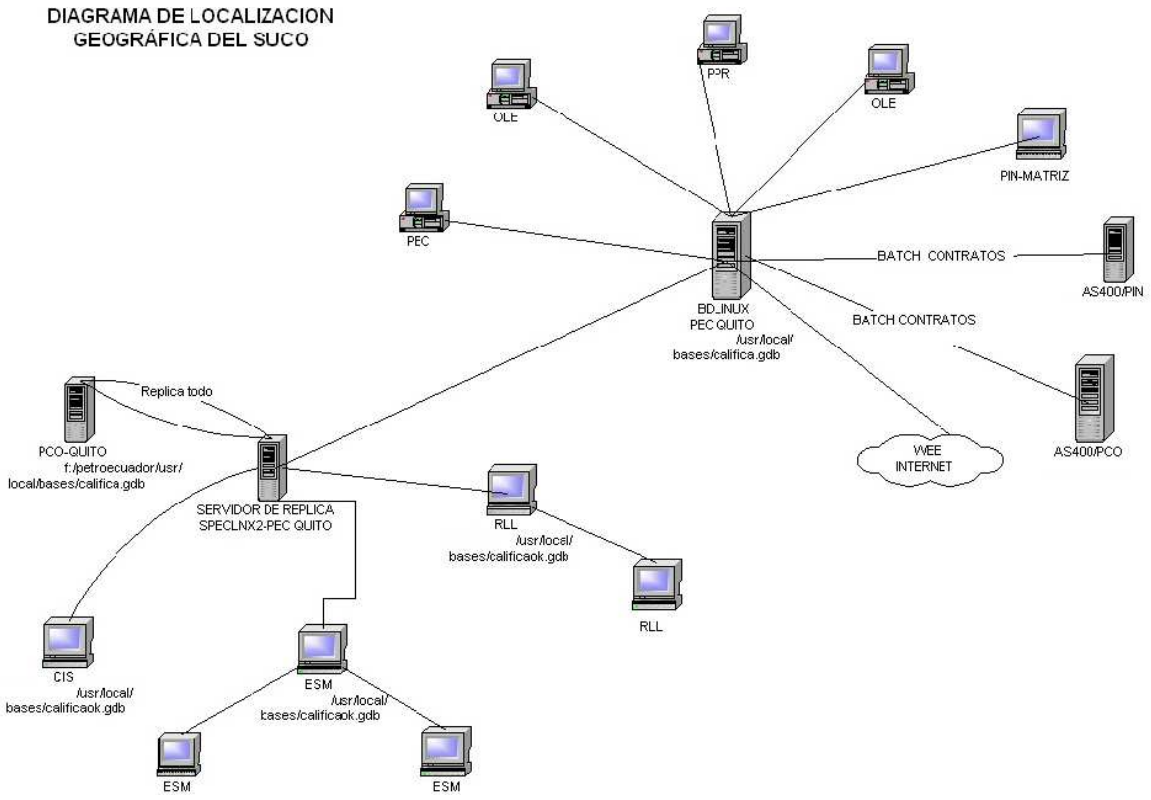
La Resolución 525-CAD-2007 del 20 de Diciembre de 2007, mediante la cual el Consejo de Administración de PETROECUADOR aprobó el nuevo “Instructivo para la Contratación para Obras, Bienes y Servicios específicos de la empresa Estatal Petróleos del Ecuador y sus empresas filiales”, dispuso la creación del Registro Corporativo de Proveedores de PETROECUADOR, RCP, estableciendo que en el término de veinte días para que se implemente este nuevo sistema en la página WEB; de igual manera dispuso que hasta que se disponga de la nueva herramienta PETROECUADOR y sus Empresas Filiales continuarán utilizando el

SUCO, y una vez haya vencido el término el Sistema Único de Calificación de Oferentes, SUCO, perderá su vigencia.

La disposición emanada del CAD, generó un requerimiento de cambio a los procesos de registro y mantenimiento de oferentes, y por lo tanto en programas, procedimientos de réplicas, así como en la estructura de las base de datos disponibles a la fecha; de igual manera la disposición involucró un nuevo enfoque a la previsión de migración del sistema SUCO, ya que debía dejarse de utilizar. Este pedido fue oportunamente atendido en el corto lapso de tiempo que se dispuso, por cuanto se aprovecho la infraestructura existente y lo ya migrado del SUCO al entorno WEB, como el nuevo Sistema de Registro Corporativo de Proveedores (RCP).

A partir del 20 de Enero de 2008 se dispuso del sistema RCP, un sistema integral para registro de oferentes a través de la página Web, y que también permite el tratamiento de invitaciones en base el sistema RCP cliente servidor, el cual atiende a los distritos con el proceso diario de replicación, y a través de la intranet viabiliza los procesos de consulta y envío de correos electrónicos.

Por diseño y de acuerdo a las necesidades del área usuaria, el tratamiento de invitaciones a ofertar, debe realizarse en ambiente Cliente/Servidor (C/S), lo cual representa el 5%, dando un total de ejecución del 100%. El acta se suscribió el 2008-05-30, a pesar de que el RCP estuvo en funcionamiento desde Enero.



Servicio Crítico recuperado: 9. Internet / Intranet:

El Portal de PETROECUADOR dispone de:

- El Look & Feel sobre la base de un estándar y colores institucionales.
- Interfaces intuitivos y personalizables.
- Contenido personalizado y facilidad de descarga de documentos.
- Seguridad de la información al interior y exterior.
- Facilidades de comunicación y colaboración tanto en Intranet como en Internet en sus secciones de contenido:
- La información estática y dinámica que la Empresa desea presentar, así como las aplicaciones con las que se mantendrá un interfaz activo.
- Un servidor de hosting proporcionado por PETROECUADOR.
- La funcionalidad de suscribirse a la distribución de boletines o contenidos a través del “SendMail”, así como para cancelar su suscripción.

- Pistas de auditoría que incluyan la identificación del usuario, fecha, hora, acción y sección sobre la que realizaron cambios al Portal y/o a su contenido, así como, de reportes por acción, período de tiempo y usuarios.

El ISP es IMPSAT.

La protección la provee el fortigate y además permite recibir correos en el Internet y enviarlos a sendmail.petroecuadopr.com.ec
Se presta el servicio de Dominio a la Gerencia de Oleoducto y PETROECUADOR Matriz.

Se presta el servicio de Internet a Petroindustrial (PIN) y Gerencia de Oleoducto (OLE) con servidores proxy y liberación directa. El servidor proxy permite hacer web caching con las páginas, URLs accesados por otros usuarios, a fin de que estén disponibles para los demás usuarios, al almacenarlas en memoria y disco. El servicio del proxy se puede arrancar, detener, ver el estado y arrancarlo nuevamente: Squid {start, stop, status, restart}. Se utiliza Apache asociado a TOMCat y UCM, debidamente integrado con LDAP para Intranet.

El UCM tiene todo lo necesario para sacar el respaldo, restauración y recuperación del Portal. El respaldo, restauración y recuperación del Portal, sus componentes y configuración es manual.

Si bien es cierto que el Plan de Continuidad de Servicios Críticos de TI, pude convertirse en una obligación importante que requiere de pruebas periódicas y actualización permanente de sus componentes, realmente es el único que asegura y garantiza la continuidad de dichos Servicios, por lo tanto ese costo será siempre menor al beneficio que proveerá ante emergencias, a pesar de todas las limitaciones de tiempo y personal que existan.

En general se observó que:

Factor Tiempo: El tiempo transcurrido para completar las tareas preestablecidas para cada escenario, entrega de equipo, reuniones, transporte, desempeño, solución de las emergencias, fue el adecuado.

Factor Cantidad: Cantidad de trabajo realizado por el personal antes, durante y después de las emergencias ha sido debidamente considerado.

Factor Cuadre: Los registros vitales considerados sí permitieron realizar las recuperaciones de los Servicios Críticos, en cada una de las emergencias producidas, las mismas que se referencian en el Acuerdo de Nivel de Servicio. Además estuvieron bien dimensionados los suministros y de equipos de repuesto utilizadas.

Factor Exactitud: La exactitud de la entrega y entrada de datos en el sitio de recuperación versus la exactitud lograda en condiciones normales, se consideró la adecuada y útil para la recuperación de la Continuidad de los Servicios Críticos de TI, en forma previa a su retorno a la normalidad.

El Plan de Continuidad de Servicios Críticos de TI fue debidamente mantenido, gracias a la revisión y actualización cronológica en sus tres escenarios, considerando:

- La ratificación o cambio en la estrategia para adecuarla a variaciones en las necesidades de la Institución.
- La incorporación de nuevas aplicaciones.
- El cambio en los recursos del Servicio Crítico de TI.
- La renovación tecnológica de la infraestructura de TI.
- La incorporar observaciones y comentarios al plan.
- La actualización del cronograma de pruebas programadas del Plan de Continuidad de Servicios Críticos de TI.

- La capacitación al personal de respaldo, restauración y recuperación de los Servicios Críticos de TI.
- El registro oportuno de las actividades de mantenimiento del Plan de Continuidad de Servicios Críticos de TI, así como también de la realización de pruebas, entrenamiento y revisiones.
- La actualización del directorio de notificación con todos los cambios del personal incluyendo números de teléfono convencional y celular, radio, responsabilidades o situación dentro de la Institución.

CAPÍTULO 4. CONCLUSIONES Y RECOMENDACIONES

En este capítulo se resumen las conclusiones derivadas de la investigación y del aporte a la gestión realizadas en esta tesis.

4.1 CONCLUSIONES Y RECOMENDACIONES

- Se concluye que el punto de partida para asegurar el éxito de las estrategias de Continuidad de los Servicios de TI es la determinación de quienes son los Clientes, es decir áreas usuarias y/o personal, así como también cuales son los responsables principal y alterno para cada uno de los Servicios de TI. Esto posibilitó el trabajo en equipo con una visión compartida cuyo objetivo fue lograr y mantener la continuidad de los Servicios de TI, por lo tanto se recomienda que para disponer de la documentación de soporte y compromiso necesarios desde el principio se realicen sesiones de trabajo entre los involucrados, cuyo producto tangible de cada una de ellas sea una acta, en la que consten las responsabilidades de las partes, con el respectivo cronograma detallado de las tareas a ejecutar con sus correspondientes dueños, tiempos y si fuera el caso costos. Actas que se constituyen en el medio idóneo para el seguimiento y control de tales acuerdos.

- El Acuerdo de Nivel de Servicio (cuadro 11) es el instrumento idóneo para definir las características y condiciones requeridas por las partes para mantener la Continuidad de los Servicios de TI, por lo tanto se recomienda que para su elaboración se consideren las correspondientes evaluaciones de Riesgo (cuadro 10), que determinan cuales son los Servicios Críticos de TI (cuadro 9), a fin de que se conozca el entorno de cada Servicio de TI y sus componentes, elementos indispensables para definir las estrategias de recuperación para cada uno de los escenarios: antes, durante y después

de una situación de emergencia, para asegurar el cumplimiento de la disponibilidad acordada.

- El equipo de trabajo conformado por los responsables de cada Servicio de TI y sus Clientes, tiene que trabajar en equipo para elaborar en detalle las estrategias de respaldo, restauración y recuperación para cada uno de los escenarios: antes, durante y después de una situación de emergencia, primero considerando las tareas que constituyen el Servicio como tal en forma independiente y luego las actividades requeridas para pasar con éxito al siguiente escenario, de modo interdependiente de la estrategia para alcanzar la Continuidad de los Servicios de TI, por lo tanto se recomienda determinar en forma independiente las tareas que cada responsable debe realizar para cumplir con la prestación del Servicio y luego en forma interdependiente definir las tareas necesarias para asegurar la continuidad de las operaciones para la prestación del Servicio en cada escenario, hasta volver a la normalidad. Trabajo que será evaluado para mejorar tales estrategias.

- La participación de ejecutivos de las áreas involucradas en fundamental para asegurar el éxito en cada escenario y para aprovechar las enseñanzas de cada situación de emergencia para mejorar las estrategias implementadas, razón por la cual se recomienda dicha participación tanto en las pruebas que permiten validar y comprobar la idoneidad de las estrategias desarrolladas, así como también la incorporación de los ajustes y correcciones necesarias para asegurar su eficacia en situaciones reales de emergencia, creando así la confianza de ejecutivos y personal en dichas estrategias y Acuerdo de Nivel de Servicio, lo cual contribuye a motivar al personal, mejorar la cultura informática y la imagen de las áreas involucradas.

- El financiamiento de sitios externos de almacenamiento y respaldo son inversiones altamente rentables en Instituciones que tienen gran

importancia socio-económica, por lo tanto, se recomienda que PETROECUADOR establezca Acuerdos de Nivel de Servicio con proveedores externos a fin de que disponga de sitios externos de almacenamiento y respaldo para los Servicios Críticos de TI, considerando el impacto que su interrupción tendría sobre la Institución y el financiamiento del Presupuesto del Estado.

- La Continuidad de los Servicios de TI es importante para todas las Instituciones cuyas actividades se apalancan en TI, razón por la cual se recomienda que se realicen todas las pruebas necesarias hasta que se cree la confianza suficiente en las estrategias desarrolladas para los escenarios: antes, durante y después de una situación de emergencia, así como también auditorias ya que aportan con su visión independiente sobre la validez e idoneidad de las mismas. También es importante el realizar nuevas investigaciones tendientes a mejorar los procedimientos y estrategias así como para mantener en un nivel adecuado los respectivos costos.

- En el organigrama actual, la Unidad de Sistemas tiene una organización plana, sin embargo como aún se mantiene la organización funcional, está no contribuye al mejoramiento continuo ni a la racional utilización de los recursos, por lo tanto se recomienda adoptar los procesos de COBIT para que se realicen en forma horizontal a través de los equipos de trabajo existentes y/o nuevos que se requieran, gracias a COBIT los Servicios Críticos de TI se alinearán a las necesidades y objetivos empresariales, para contribuir a la eficiencia de los procesos y a la racional utilización de los recursos.

- Si se adopta COBIT y si el personal es insuficiente para realizar las procedimientos de los procesos, entonces se recomienda formular muy bien un Plan Operativo con el correspondiente análisis costo – beneficio y ROI, a fin de conseguir la contratación de personal a tiempo fijo por un año

o dos, hasta que se supere dicha brecha, con lo cual se tendrá la oportunidad de demostrar el valor agregado de TI a la Institución y apalancarla en lo que realmente le es importante.

- La aplicación del Procedimiento desarrollado en esta Tesis y demostrado en PETROECUADOR, permite cumplir a cabalidad la Recomendación No. 4 de Auditoría y por lo tanto es conveniente para los intereses de PETROECUADOR y en tal virtud se recomienda su aplicación.

- Las recomendaciones de las auditorías anuales que realizan a PETROECUADOR siempre servirán para mejorar los procedimientos y en tal virtud se debe conseguir opiniones debidamente sustentadas y recomendaciones factibles y proactivas tendientes al mejoramiento continuo del Sistema de Control Interno.

- Por lo observado hace falta fortalecer la cultura de comunicaciones y tecnologías de la información del personal de PETROECUADOR, lo cual contribuirá al bajar los riesgos y lograr mayor apoyo y compromiso con el Plan ce Continuidad de los Servicios de TI.

- Dado que las comunicaciones dependen de la repetidora del Pichincha se recomienda realizar observaciones periódicas a las seguridades físicas y al cumplimiento del mantenimiento preventivo respectivo.

- Como aún no se realiza la Administración del ciclo de vida de los datos, que permita considerar el período de retención, el tiempo de vida útil de los cartuchos, la naturaleza de los datos, la validez de los mismos, su descarte, etc., se recomienda incorporar la funcionalidad de Ad Administración del ciclo de vida de los datos para racionalizar su almacenamiento, utilización y acceso, así como también su vida útil.

- En razón de que los Servicios incorporados en el Plan de Continuidad son los Críticos, se recomienda que éstos sean monitoreados permanentemente a fin evitar y/o minimizar su impacto en casos de emergencia.

- Si bien es cierto que el Plan de Continuidad de Servicios Críticos de TI, puede convertirse en una obligación importante que requiere de pruebas periódicas y actualización permanente de sus componentes, se lo recomienda porque es realmente el único que asegura y garantiza la continuidad de dichos Servicios, por lo tanto ese costo será siempre menor al beneficio que proveerá ante emergencias, a pesar de todas las limitaciones de tiempo y personal que existan.

- Finalmente, los resultados obtenidos demostraron que las pruebas no fueron suficientes para asegurar el cumplimiento del Acuerdo de Nivel de Servicio en cuanto al tiempo en el cual se superó la emergencia y se retornó a la normalidad, lo cual amerita el mejoramiento de dichas estrategias, por lo tanto, se recomienda trabajar en forma proactiva para no reincidir en esta situación reactiva que implica entrar a analizar cada caso para tomar las medidas correctivas, que se habrían evitado con el trabajo proactivo, interdependiente y sinérgico de todas las áreas involucradas, fundamentado en el hecho indiscutible que la Continuidad de los Servicios de TI beneficia a todos, mejora la imagen Institucional y contribuye a incrementar la Continuidad de las Operaciones de la Institución y la consiguiente rentabilidad socio-económica, en beneficio del personal, ejecutivos, Institución, sector, Estado y sociedad en general.

REFERENCIAS BIBLIOGRÁFICAS

[5] ALEXANDER, Alberto G, Aplicación del ISO 9000 y cómo implementarlo, Addison -Wesley Iberoamericana S.A, Argentina 1995, p. 71, 189 p.

[12] APPLEGATE, Lynda M, MCFARLAN, F.Warren, MCKENNEY, James L, Corporate Information systems Management, McGraw-Hill, United States of America 1999, p.p. 337 y 338, 348 p.

[13] ARNELL, Alvin, Handbook Effective Disasters/Recovery Planning, McGraw-Hill, United States of America 1990, p.p. 12 y 13, 333 p.

[14] BROWNING, Tim, Capacity Planning for Computers Systems, AP PROFESSIONALS, United States of America 1995, p. p. 71 y 72, 216 p.

[15] CARTLIDGE, Alison, LILLYCROP, Mark, An Introductory Overview of ITIL v3, itSMF, United States of America 2007, p. p. 21 y 52, 56 p

[16] DE LA FUENTE, Reynaldo J, CRISCI, Nora, SERRA, Carlos, DE LA FUENTE, Juan A, DE LA FUENTE, Reynaldo C, ALVAREZ , Nicolás, FABIUS, Rafael, FERNANDEZ, Carlos, Claves para el Gobierno de los Sistemas de Información, Impresora Polo Ltda., Patria 716 2000, p. 287, 396 p.

[6] Directorio de PETROECUADOR, Resolución No. 09-DIR-2008-01-16: aprobación del Presupuesto y plan Operativo 2008, Quito-Ecuador, 1 p.

17] DIXON, Allen N, SALLSTROM, Laura, LEUNG, Ángela, WASNER DAMUNTH, Robert J, Los Beneficios Económicos y Sociales del uso de las TIC, ComTIA Public Pólice, Washington 2007, p.p. 1, 36 y 59, 80 p.

[3] E-Strategia Consulting Group, Empresa por resultados, San Pedro Garza, México, 1999-2008, p.p. 35, 38 y 41, 76 p.

[7] FLORES José Manuel, Director de Servicios y Consultoría, Integrando TI al negocio a través de las Mejores Prácticas de ITIL, Pink Elephant LAM, 2007, p. 51, 68 p.

[18] GOODSTEIN, Leonard D, NOLAN, Timothy M, PFEIFFER, J. William, Planeación Estratégica Aplicada, McGraw-Hill Interamericana S.A, Santafé de Bogotá Colombia 1998, p.p. 375 y 376, 442 p.

[19] GUTIERREZ, Juan José, Desarrollando Nuevas Habilidades Docentes (Aprendizaje Experimental en el aula universitaria), INCREA innovación & creatividad, Chile Febrero 2008, p. p. 4 y 133, 235 p.

[20] HAMMER, Michael, La Auditoría del Proceso, Harvard Business Review, Abril 2007, p.p. 114,115 y 127, 113 p.

[21] HARRINGTON, H.James, Mejoramiento de los Procesos de la Empresa, McGraw-Hill Interamericana S.A, Santafé de Bogotá Colombia 1993, p.p. 19 y 47, 309 p.

[22] HILES, Andrew, Business Continuity: Best Practices, DRI INTERNATIONAL, New York 2003, p. p. 29 y 31, 211 p."

[23] HMSO, Cramm Management Guide, Government National Security Authorities, London 1996, p. 5, 325. P.

[24] IBM del ECUADOR C.A, Plan de Contingencias y recuperación ante Desastres (material del estudiante), IBM, Quito Abril-2001, p. 5, 59 p.

[25] IBM Departamento de Educación, ¿Por Qué El plan de Recuperación de Negocios?, IBM de Colombia S.A, Colombia 1994, p. 36, 110 p.

[26] Information Systems Control Journal, Magazine for IT Governance Professionals Volume 3 2008, ISACA, Addressing Business Challenges, p.p. 54 y 55, 63 p.

[27] ISACA, Information System Control Journal Volume 1.3, ISACA and/or the IT Governance Institute, United States of America 2007, p. 23, 180 p.

[28] ISACA, IS Standards, Guidelines and Procedures for Auditing and Control Professionals, ISACA, United States of America 2007, p.p.159 y 160, 300 p.

[29] ISACA, Risks of Customer Relationship Management A Security, Control and Audit Approach, ISACA, United States of America 2003, p. 161, 180 p.

[2] IT GOVERNANCE INSTITUTE, Cobit 4.0, IT Governance Institute, United States of America 2005, 194. p.

[30] IT GOVERNANCE INSTITUTE, Cobit 4.1, IT Governance Institute, United States of America 2007, p. 114, 196 p.

[31] IT GOVERNANCE INSTITUTE, Cobit Mapping Overview of International IT Guidance, IT Governance Institute, United States of America 2004, p. 50, 56 p.

[32] IT GOVERNANCE INSTITUTE, IT Governance Using Cobit and Val IT (Student Book, 2nda edition), IT Governance Institute, United States of America 2007, p. 16, 127 p.

[33] IT GOVERNANCE INSTITUTE, Valor para la Empresa: Buen Gobierno de las Inversiones en TI el Marco “Val IT”, IT Governance Institute, United States of America 2006, p.p. 7 y 9, 44 p.

[34] KEMMERLING, Georges, PONDMAN, Dick, Gestión de Servicios TI: Una Introducción a ITIL, Van Haren Publishing (info@vanharen.net), Holanda 2004, p. 14, 226 p.

[35] KHADEM, Riaz, LORBERT, Robert, Administración en una Página, Grupo Editorial NORMA, Bogotá Colombia 1997, p.p. XII, 130, 140 p.

[36] MEYER, Sarah, Business Service Management: Fusión de los Servicios de TI y los Objetivos Empresariales, Transforming IT Management, EE.UU Abril 2007, p.p. 1 y 3, 11 p.

[37] Modelo de Política de Seguridad de la Información para los Organismos de la Administración Pública Nacional, ONTI (Oficina Nacional de Tecnologías de Informaciòn), Documento Publico, Versión 1 Julio 2005, p. 88, 99 p.

[38] MONTES, Gustavo Adolfo, Reingeniería de la Auditoria Informática, S y G Editores S.A, Coyoacàn (México) 1999, p. 147, 304 p.

[39] NATIONAL COMPUTING CENTRE, IT Governance developing a successful governance strategy, The National computing Centre, London 2003, p. 4, 70 p.

[**12**] OCHOA, Marco, Plan de Tesis elaborado en el Formulario para la presentación del plan de tesis de magister de la Escuela Politécnica Nacional, Coordinación de Postgrado: Maestría Gestión de las Comunicaciones y Tecnologías de la Información, Quito-Ecuador, 2006, p.1, 14 p.

[40] OFFICE OF GOVERMENT CONMMERCE, Best Practice for Service Delivery ITIL, TSO (The Stationery Office), London 2001. 378 p.

[41] OFFICE OF GOVERMENT CONMERSE, Best Practice for Service Support ITIL, TSO (The Stationery Office), London 2000, p. 15, 308 p.

[8] OLVE, Nils-Göran, El Cuadro de Mando en Acción: Equilibrando la Estrategia y Control, Ediciones Deusto, 2004, Barcelona-España, p. 19, 334 p. [10] Dirigidas a Kaplan y Norton (1996, 2001); Olve et al. (1999); u Olve y Sjöstrand (2002).

[9] Para el año 2000:
http://www.bain.com/bainweb/expertise/tools/mtt/balance_scorecard.asp

[42] Osiatis Espiñeira, Sheldon y Asociados, Formación ITIL Versión 3 Fundamentos de la Gestión del servicio de IT, Madrid 2005, Registro Mercantil de Madrid, Tomo 6803 Gral. Sección tercera del libro de Sociedades, Folio 77, Hoja 58144, p. 3, 40 p.

[43] PETROECUADOR, Manual de Organización y Funciones del Sistema PETROECUADOR, Unidad de Relaciones Institucionales, Quito, enero del 2000, 75 p.

[44] Presidente Ejecutivo, Plan Estratégico Corporativo 2008-12 de PETROECUADOR y sus Empresas Filiales, aprobado por el señor Presidente de la República el 2008-02-25, Quito-Ecuador, 158 p.p. 4. Noticia: Revista Petróleo Actualidad, año 8, No.7, marzo 2008.

[45] R.NIVEN, Paul, El Cuadro de Mando Integral paso a paso, John Willey & Sons Inc., New York 2002, p. 401, 414 p.

[46] RIZZO, María Estefanía, La Contribución del Balance Scorecard al Proceso de Gobierno de Tecnologías de Información (TI), Universidad del CEMA Máster en Dirección de Empresas, Buenos Aires, Argentina 2001, p. 6, 31 p.

[47] SENGE, Peter, La Quinta Disciplina el Arte y la Práctica de la Organización Abierta al Aprendizaje, Ediciones Juan Granica, Barcelona, 2003, 490p.

[48] SENGE, Peter, ROBERTS, Charlotte, ROSS, Richard, SMITH, Bryan, KLEINER, Art, La Quinta Disciplina en la Práctica, Ediciones Juan Granica, Buenos Aires, 1999, 593p.

[49] SIMONS, Robert, MANKINS, Michael C, QUINN, Robert E, DARLING, Marilyn, COLLINS, Jim, The High-Performance Organization, Harvard Business Review, *"United States of America Julio - Agosto 2005, p. 159, 196 p.*

[50] STEPHEN B, Page, Achieving 100% Compliance of Policies and Procedures, Book Masters, United States of America 2000, p. 127, 329 p.

[51] TOIGO, John William, Disaster Recovery Planning (For Computers and Communication Resources), John Wiley & Sons inc, United states of America 1996, p. 10, 329 p.

[53] VÁSCONEZ, Francisco, Comentarios de la Gerencia presentado por la firma Deloitte & Touche, resultantes de la Evaluación al Ambiente de Procesamiento de Datos de ETROECUADOR-Matriz, memorando No.145-CTR-2005, Gerencia de Economía y Finanzas de PETROECUADOR, Quito – Ecuador, 2005, 1p.

ANEXOS

Documentación mínima de cada Servicio crítico de TI

1.1. Creación / Accesos Usuarios y Reactivación Contraseña

- Doc.1.1.1 Un diagrama de bloque
- Doc.1.1.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0
- Doc.1.1.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles
- Doc.1.1.4 Lista de chequeo que incluye a los dos procedimientos anteriores.
- Doc.1.1.5 Acta de ER del retorno a la normalidad.

1.2. Provisión de telecomunicaciones

- Doc.1.2.1 Un diagrama de bloque
- Doc.1.2.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0
- Doc.1.2.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles
- Doc.1.2.4 Lista de chequeo que incluye a los dos procedimientos anteriores.
- Doc.1.2.5 Acta de ER del retorno a la normalidad.

1.3. Provisión / Renovación Telefonía móvil

- Doc.1.3.1 Un diagrama de bloque
- Doc.1.3.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

Doc.1.3.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

Doc.1.3.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

Doc.1.3.5 Acta de ER del retorno a la normalidad.

1.4. Correo Electrónico

Doc.1.4.1 Un diagrama de bloque

Doc.1.4.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

Doc.1.4.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

Doc.1.4.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

Doc.1.4.5 Acta de ER del retorno a la normalidad.

1.5. Instalación / reparación de Energía regulada y Red de Datos

Doc.1.5.1 Un diagrama de bloque

Doc.1.5.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

Doc.1.5.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

Doc.1.5.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

Doc.1.5.5 Acta de ER del retorno a la normalidad.

1.6. Gestión de Respaldos

Doc.1.6.1 Un diagrama de bloque

Doc.1.6.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

Doc.1.6.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

Doc.1.6.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

Doc.1.6.5 Acta de ER del retorno a la normalidad.

1.7. Interbase (Datos del RCP)

Doc.1.7.1 Un diagrama de bloque

Doc.1.7.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

Doc.1.7.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

Doc.1.7.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

Doc.1.7.5 Acta de ER del retorno a la normalidad.

1.8. Internet/Intranet

Doc.1.8.1 Un diagrama de bloque

Doc.1.8.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

Doc.1.8.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

Doc.1.8.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

Doc.1.8.5 Acta de ER del retorno a la normalidad.

ANEXO 1.1

Creación / Accesos Usuarios y Reactivación Contraseña

Documentación mínima:

1.1.1 Un diagrama de bloque que incluya la Planificación y Ejecución

1.1.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

1.1.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

1.1.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

1.1.5 Acta de ER del retorno a la normalidad.

Diagrama de Bloque

Doc.1.1.1

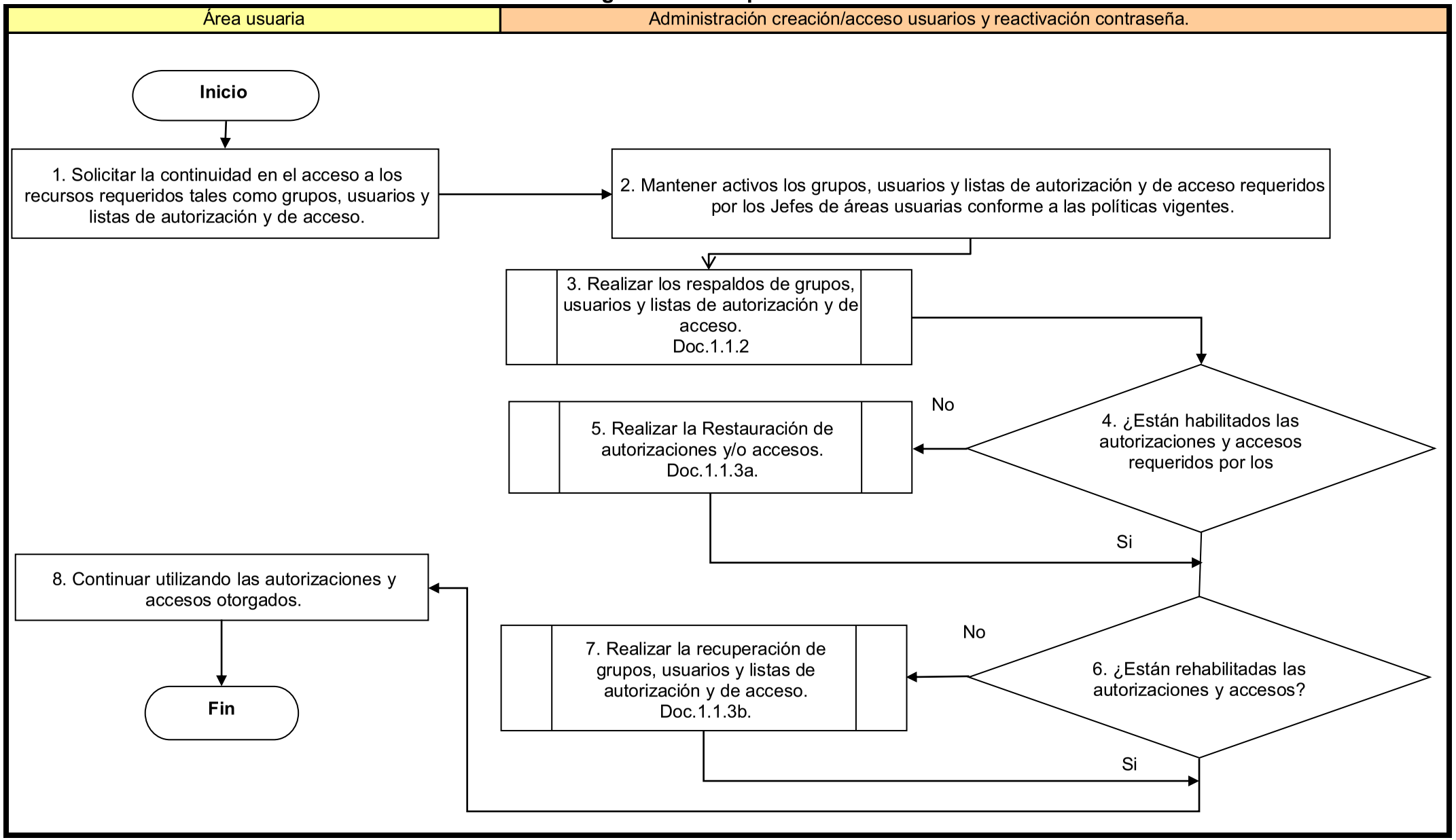
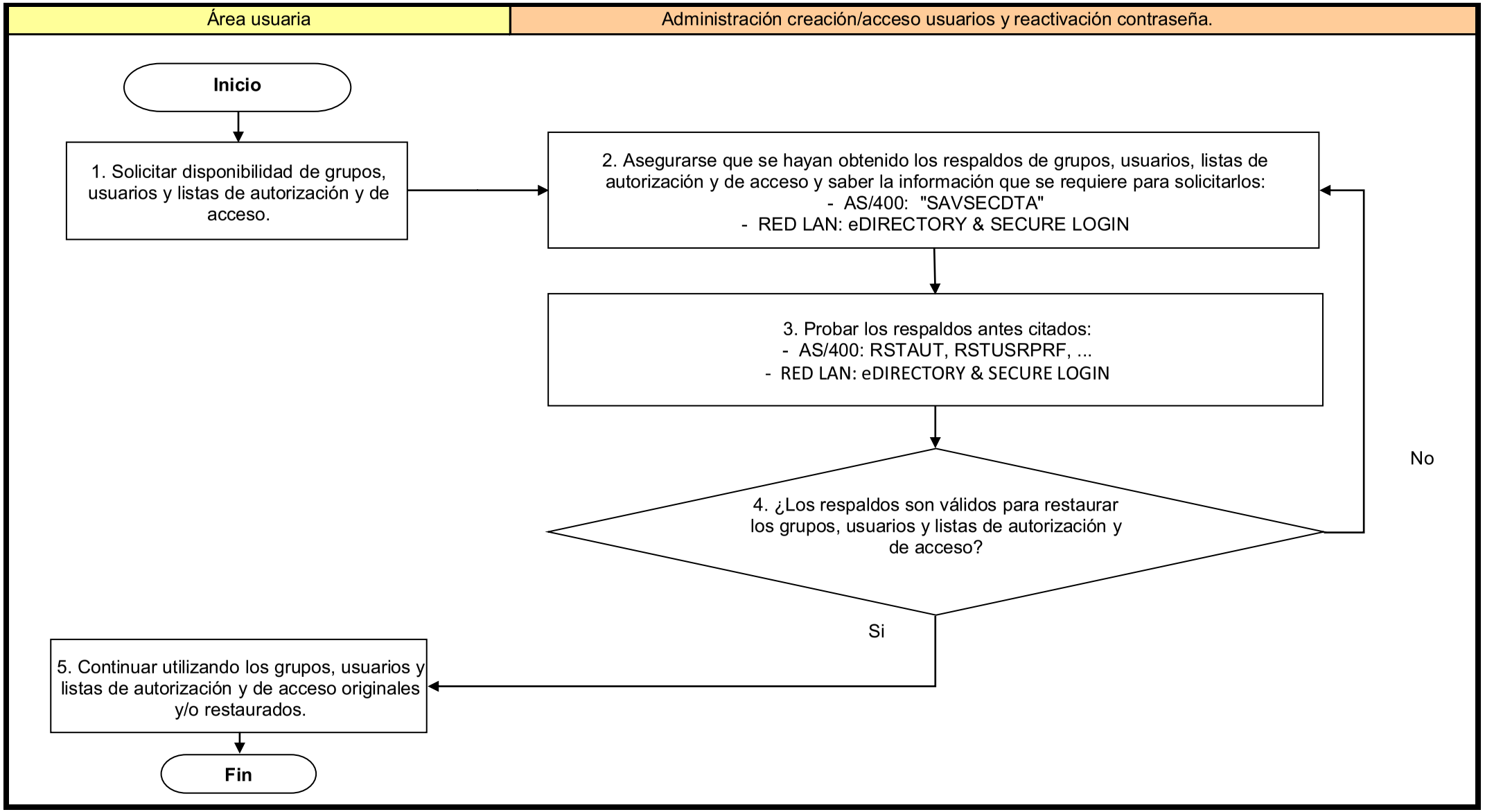


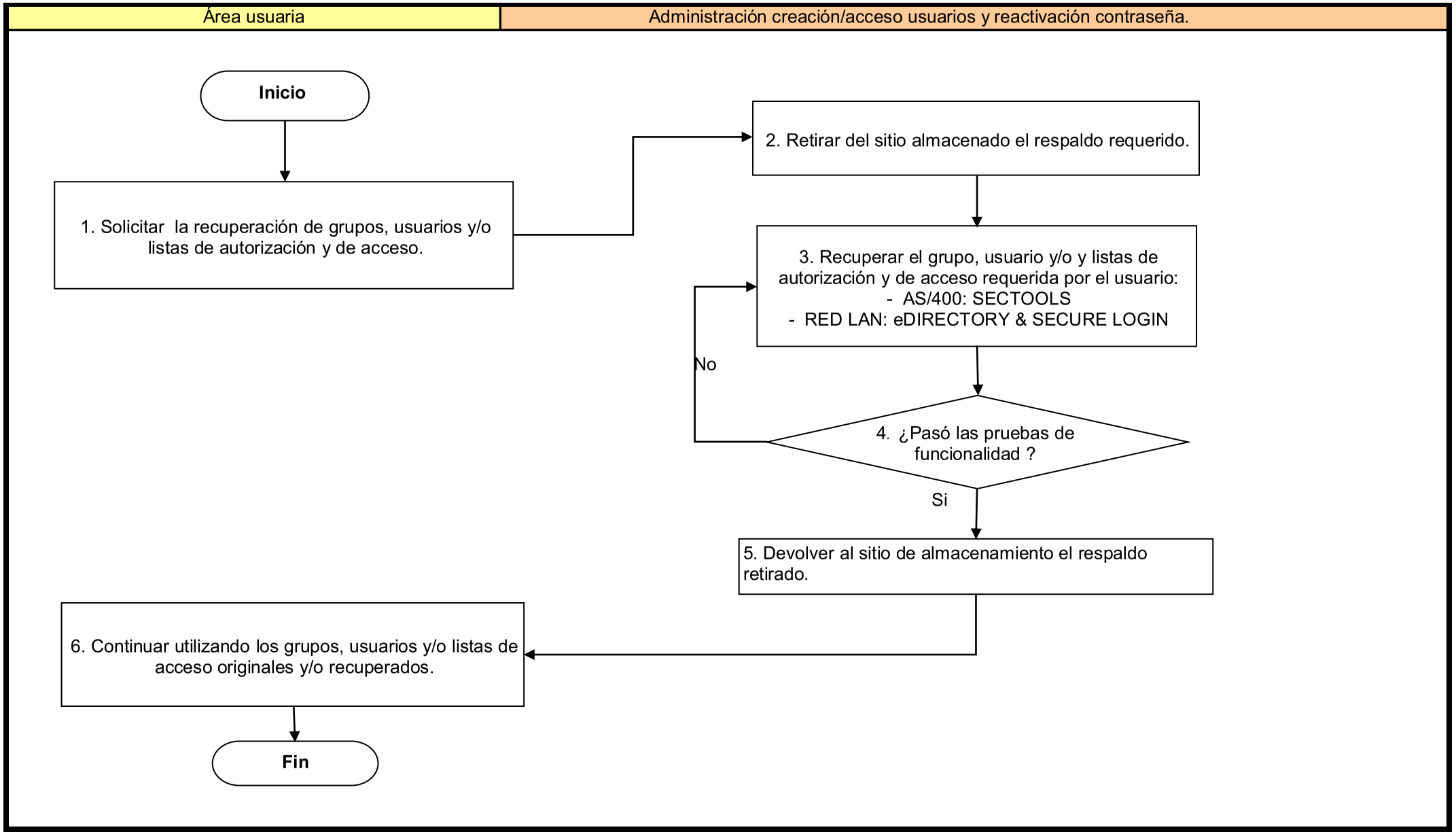
Diagrama del Procedimiento de Respaldo y Restauración

Doc.1.1.2



SERVICIO CRÍTICO: "CREACIÓN / ACCESOS USUARIOS Y REACTIVACIÓN CONTRASEÑA"
Diagrama del Procedimiento de Recuperación

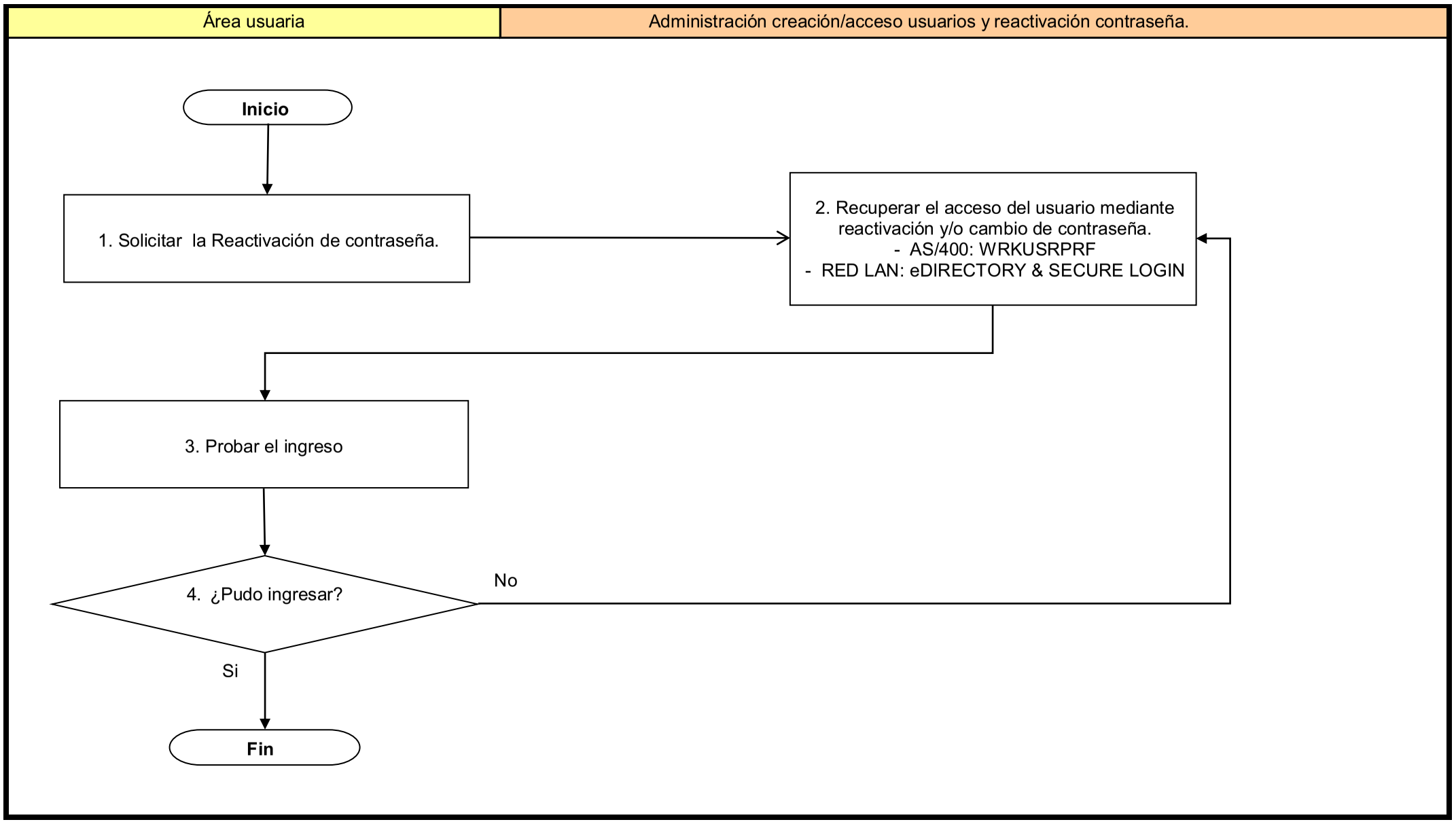
Doc.1.1.3a



SERVICIO CRÍTICO: "CREACIÓN / ACCESOS USUARIOS Y REACTIVACIÓN CONTRASEÑA"

Diagrama del Procedimiento de Reactivación de Contraseña

Doc.1.1.3b



SERVICIO CRITICO: "CREACION /ACCESO USUARIOS Y REACTIVACION CONTRASENA"
Lista de Chequeo

Fecha y hora de inicio: 2008-03-24 y 8h00 Fecha y hora de finalización: 2008-03-26 y 8h00 **Doc.1.1.4**

No	Procedimientos y pasos	Parámetros a controlar, comparar y evaluar. Parámetro	Valor	Cumplió Si	Par	No	Observaciones
	Doc.1.1.2 Procedimiento de Respaldos y Restauración						
1	1. Solicitar Disponibilidad de grupos, usuarios y listas de autorización y de acceso.						
2	2. Asegurarse que se hayan obtenido los respaldos de grupos, usuarios, listas de autorización y de acceso y saber la información que se requiere para solicitarlos. AS/400: "SAVSECDTA" RED LAN: eDIRECTORY & SECURE LOGIN						
3	3. Probar los respaldos antes citados. AS/400: RSTAUT, RSTUSRPRF, ... RED LAN: eDIRECTORY & SECURE LOGIN						
4	4. ¿Los respaldos son válidos para restaurar los grupos, usuarios y listas de autorización y de acceso?						
5	No. Continuar con el paso 2.						
6	Si. 5. Continuar utilizando los grupos, usuarios y listas de autorización de acceso originales y/o restaurados.						
	Doc.1.1.3a Procedimiento de Recuperación						
7	1. Solicitar la recuperación de grupos, usuarios y/o listas de acceso originales y/o recuperados.			si			
8	3. Recuperar el grupo, usuario y/o y listas de autorización y de acceso requerida por el usuario. AS/400: SECTOOLS RED LAN: eDIRECTORY & SECURE LOGIN			si			
9	3. Recuperar el grupo, usuario y/o y listas de acceso requerida por el usuario.			si			
10	4.¿Pasó las pruebas de funcionalidad ?						
11	No. Continuar con el paso 3.						
12	Si. 5. Devolver al sitio de almacenamiento el respaldo retirado.			si			
13	6. Continuar utilizando los grupos, usuarios y/o listas de acceso originales y/o recuperados.			si			
	Doc.1.1.3b Procedimiento Reactivación de Contraseña						
14	1. Solicitar la Reactivación de la contraseña.			si			
15	2. Recuperar el acceso del usuario mediante reactivación y/o cambio de contraseña. AS/400: WRKUSRPRF RED LAN: eDIRECTORY & SECURE LOGIN			si			
16	3. Probar el ingreso			si			
17	4. ¿Pudo ingresar ?						
18	No. Continuar con el paso 2.						
19	Si. Fin.			si			

Nivel de satisfacción del cliente : Total: Si ☐ Parcial: ☐ Insatisfecho: ☐

Por el Técnico encargado de rehabilitar el Servicio: Por el Responsable del Servicio:

Firma: _____ _____

Nombre: _____ _____

No. Rol o Cédula de Ciudadanía: _____ _____

SERVICIO CRÍTICO "CREACIÓN / ACCESOS USUARIOS Y REACTIVACIÓN CONTRASEÑA"

Fecha: 2008-03-24 **Acta de Entrega Recepción de Retorno a la Normalidad del Servicio Crítico de TI** **Doc.1.1.5**

Matriz, Filial o Distrito: PETROECUADOR y Unidad: Sistemas

En la ciudad de Quito se suscribe la presente Acta entre el Técnico que rehabilitó este Servicio y el Responsable del mismo, acta contenida en las siguientes cláusulas:

PRIMERA: OBJETIVO

Mantener la Continuidad del Servicio que apalanca a la Gestión Institucional y en caso de emergencia rehabilitarlo conforme a lo establecido en el Acuerdo de Nivel de Servicio.

SEGUNDA: ESCENARIOS DEL SERVICIO

2.1 Estado previo a la emergencia

Emergencia	Se daño el servidor en el que funcionaba el LDAP.
Diagnóstico	1. Reinstalar el eDirectory y Secure Login. 2. Recuperar el LDAP.

2.2 Estado del Servicio durante la emergencia

Solución	1. Disponer del cartucho de respaldo del LDAP más reciente. 2. Restaurar a disco el LDAP. 3. Renombrar el LDAP producto de la reinstalación. 4. Recuperar el LDAP en la nueva instalación.

2.3 Estado luego de la emergencia

Normalidad	Utilizar el LDAP, sin pérdida de datos.

TERCERA: DERECHOS Y OBLIGACIONES

3.1 El Responsable del Servicio comprobó que el Servicio está 100% operativo.

3.2 El Técnico alertó al Responsable de este Servicio sobre las características de crecimiento, novedades que se han encontrado y conveniencia del mantenimiento preventivo.

3.3 El funcionario que debido a cualquier causa se separe de la Unidad de Sistemas, como paso previo a la obtención de su liquidación, procederá a capacitar y entregar a otros funcionarios los procedimientos de Continuidad de los Servicios y otros que estuvieron a su cargo.

CUARTA: ALCANCE

Lograr la Continuidad del Servicio que se encontraba en estado de emergencia, aplicando los procedimientos disponibles y/o otros que se requirieron para este fin.

QUINTA: ACEPTACION DE LOS FUNCIONARIOS, PARA QUE PETROECUADOR PUEDA EXIGIR Y DEMANDAR EL CUMPLIMIENTO DE SUS RESPONSABILIDADES

5.1 Aceptar y asumir todas las responsabilidades pertenecientes a la aplicación de procedimientos de Respaldo, Restauración, Recuperación y/ otros tendientes a rehabilitar la Continuidad de este Servicio, así como, de controles y actualización de la documentación respectiva, que también es útil para efectos de auditoría, lo cual incluye la incorporación de los cambios efectuados a la documentación existente y de nuevos procedimientos.

5.2 Aceptar que al suscribir esta acta, son administrativa, personal y pecuniariamente responsables tanto del estado en el cual retorna a la normalidad el Servicio recibido, como por la validez y la actualización de la documentación de los procedimientos aplicados en este caso.

Para constancia y fe de conformidad con lo actuado, suscriben la presente acta en original y tres copias de igual contenido y valor.

ENTREGUÉ CONFORME	**RECIBÍ CONFORME**
Firma:	
Nombre:	
No. Rol. o Céd. Ciud.	

ANEXO 1.2

Provisión de telecomunicaciones

Documentación mínima:

1.2.1 Un diagrama de bloque que incluya la Planificación y Ejecución

1.2.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

1.2.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

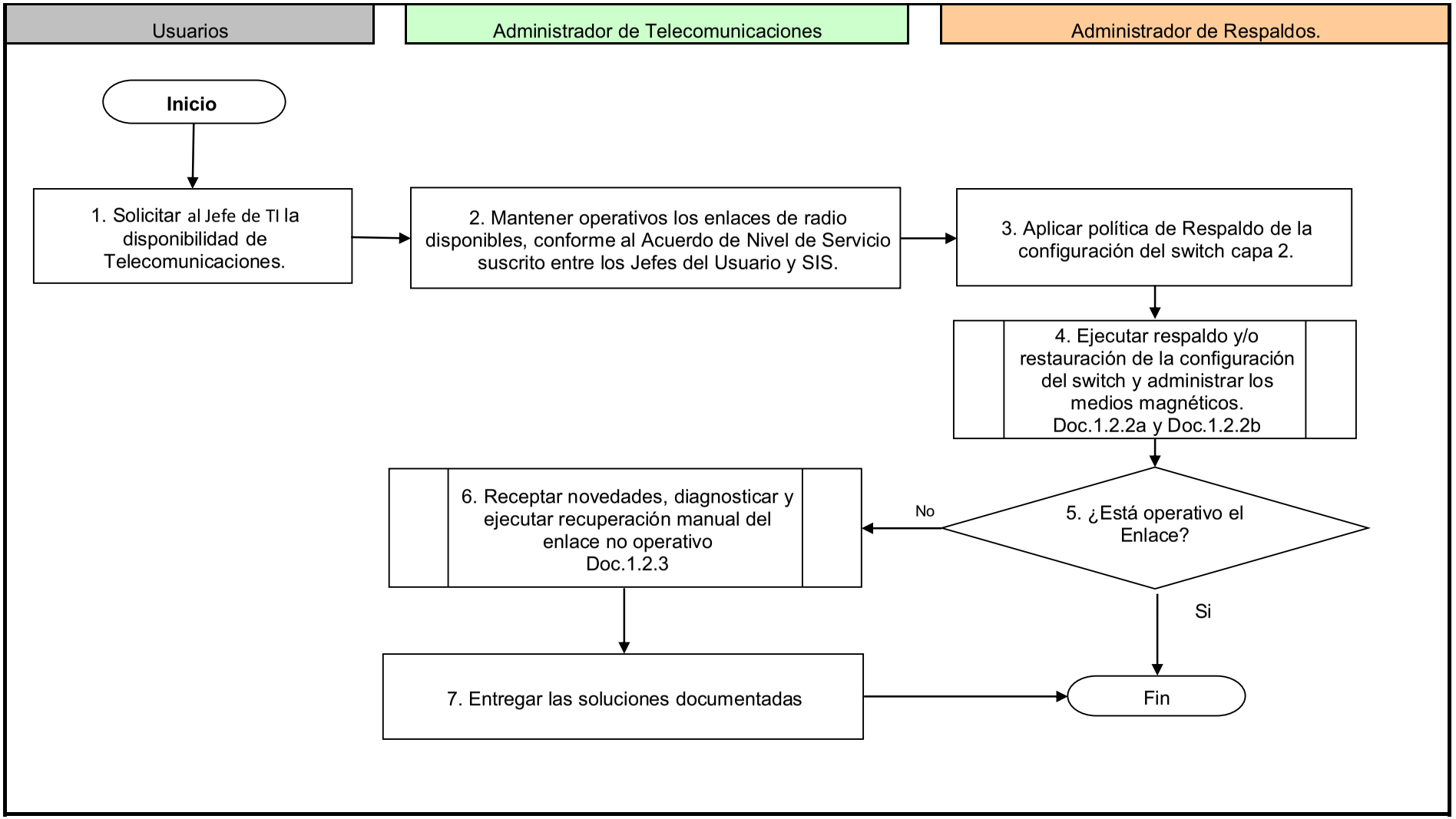
1.2.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

1.2.5 Acta de ER del retorno a la normalidad.

SERVICIO CRÍTICO: "PROVISIÓN DE TELECOMUNICACIONES"

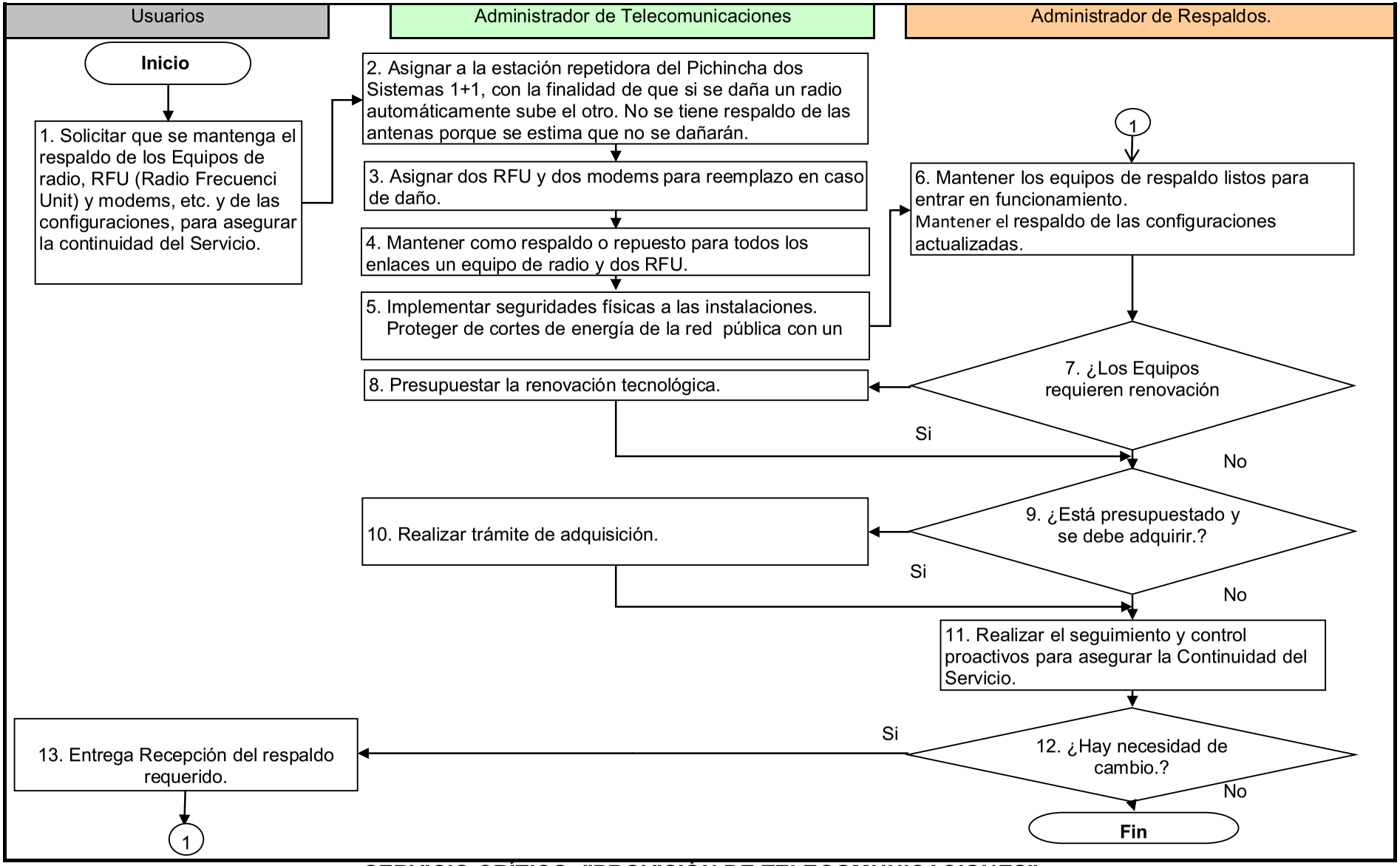
Diagrama de Bloque

Doc.1.2.1



SERVICIO CRÍTICO: "PROVISIÓN DE TELECOMUNICACIONES"
Diagrama del procedimiento de Respaldo

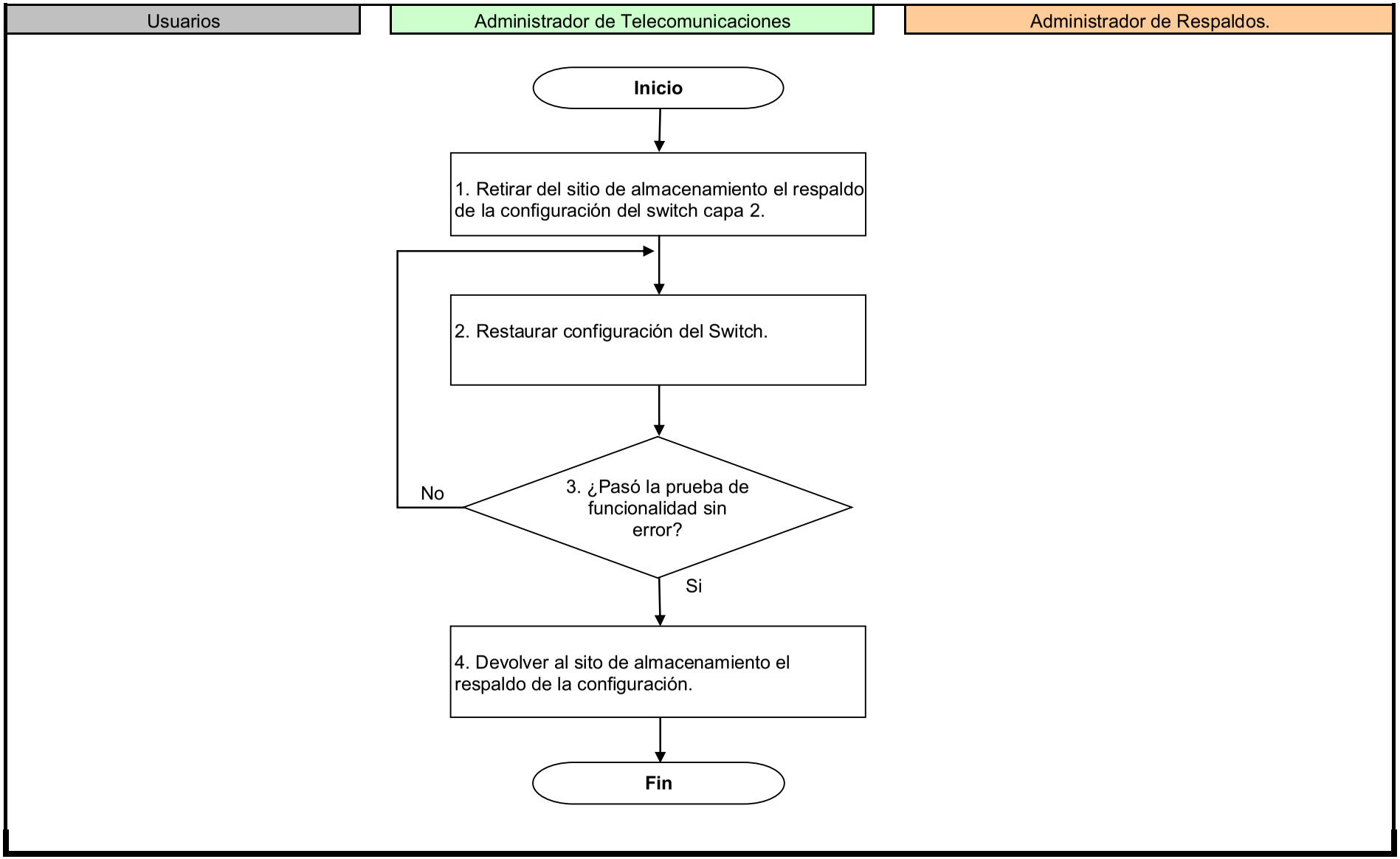
Doc.1.2.2a



SERVICIO CRÍTICO: "PROVISIÓN DE TELECOMUNICACIONES"

Diagrama del procedimiento Restauración

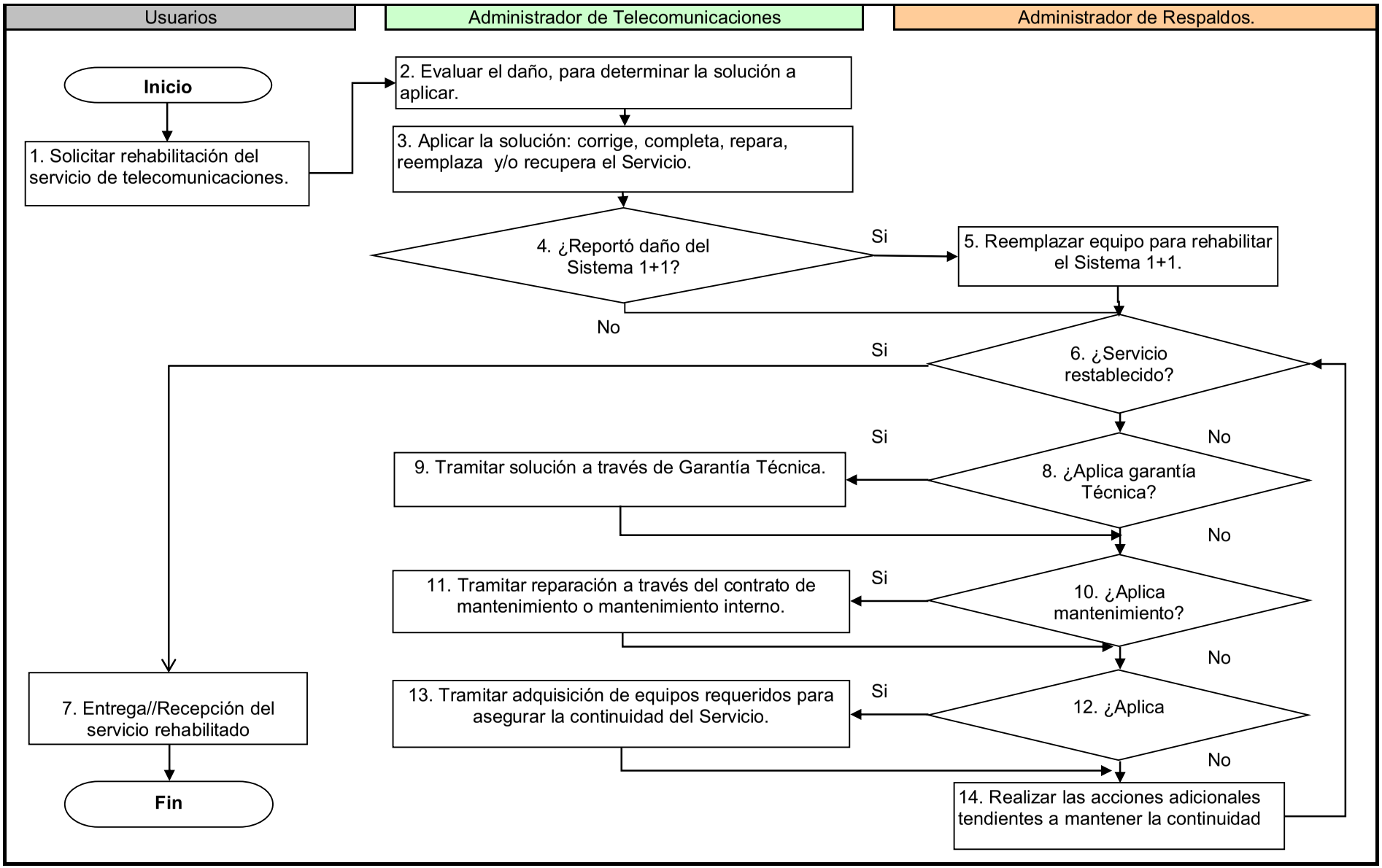
Doc.1.2.2b



SERVICIO CRÍTICO: "PROVISIÓN DE TELECOMUNICACIONES"

Diagrama del procedimiento de Recuperación

Doc.1.2.3



SERVICIO CRÍTICO: "PROVISIÓN DE TELECOMUNICACIONES"
Lista de Chequeo

Fecha y hora de inicio:2008-04-21 y 10h00 Fecha y hora de finalización:2008-04-21 y 14h00 **Doc.1.2.4**

No	Procedimientos y pasos	Parámetros a controlar, comparar y evaluar.		Cumplió			Observaciones
		Parámetro	Valor	Si	Par	No	
	Doc.1.2.2a Diagrama Procedimiento de Respaldo						
1	1. Solicitar que se mantengan los Equipos de radio, RFU (Radio Frecuenci Unit) y Modems, etc. y configuraciones, para asegurar la continuidad del servicio.			si			
2	2. Asignar a la estación repetidora del Pichincha 2 Sistemas 1+1, con la finalidad de que si se daña un radio automáticamente sube otro. No se tiene respaldo de las antenas porque se estima que no se dañarán.			si			
3	3. Asignar dos RFU y dos Modems para reemplazo en caso de daño.			si			
4	4. Mantener como respaldo o repuesto para todos los enlaces un equipo de radio y dos RFU de respuesta.						
5	5. Implementar seguridades físicas a las instalaciones. Proteger de cortes de energía de la red pública con un generador y sistema de baterías.			si			
6	6. Mantener los equipos de respaldo listos para entrar en funcionamiento. Mantener el respaldo de las configuraciones actualizadas.			si			
7	7. ¿Los Equipos requieren renovación tecnológica?			si			
8	Si. 8. Presupuestar la renovación tecnológica. Continuar con el paso 8.						
9	No.9. ¿Está presupuestado y se debe adquirir? Continuar con el paso 9.						
10	Si.10. Realizar trámite de adquisición.						
11	No.11. Realizar el seguimiento y control para realizar las acciones pertinentes. Continuar con el paso 11.						
12	12. ¿Hay un requerimiento de cambio.? No. Fin.						
13	Si.13. Entrega/Recepción del respaldo requerido.						
14	14. Continuar con el paso 6.						
	Doc.1.2.2b Diagrama del procedimiento Restauración						
15	1. Retirar del sitio de almacenamiento el respaldo de la configuración del switch capa 2.						
16	2. Restaurar Configuración del Switch.						
17	3. ¿Pasó la prueba de funcionalidad sin error?						
18	No. Continuar con paso 2.						
19	Si. 4. Devolver al sito de almacenamiento el respaldo de la configuración.						
	Doc.1.2.3 Diagrama del procedimiento Recuperación						
20	1. Solicitar rehabilitar el servicio de telecomunicaciones.			si			
21	2. Evaluar el daño, para determinar la solución a aplicar.			si			
22	3. Aplicar la solución: corrige, completa, repara, reemplaza y/o recupera el Servicio.			si			
23	4. ¿Reportó daño Sistema 1+1?			si			
24	Si. 5. Reemplazar Equipo para rehabilitar el Sistema 1+1.			si			
25	No. 6. ¿Servicio Restablecido?. Continuar con paso 6.						

26	Si. 7. Entrega/Recepción del servicio rehabilitado.			si			
27	No.8. ¿Aplica garantía Técnica?						
28	Si. 11. Tramitar reparación a través del contrato de mantenimiento o mantenimiento interno.			si			
29	No. 12. ¿Aplica mantenimiento?						
30	Si. 13. Tramitar adquisición de Equipos requeridos para asignar la continuidad del Servicio.			si			
31	No.14. Realizar las acciones adicionales tendientes a mantener la continuidad del servicio.						

Nivel de satisfacción del cliente :	Total: Si	Parcial: ☐	Insatisfecho: ☐

Por el Técnico encargado de rehabilitar el Servicio:

Firma: _____

Nombre: _____

No. Rol o Cédula de Ciudadanía: _____

Por el Responsable del Servicio:

_____

_____

_____

SERVICIO CRÍTICO "PROVISIÓN DE TELECOMUNICACIONES"

Fecha: 2008-04-21 **Acta de Entrega Recepción de Retorno a la Normalidad del Servicio Crítico de TI** **Doc.1.2.5**

Matriz, Filial o Distrito: PETROECUADOR y Unidad: Sistemas

En la ciudad de Quito se suscribe la presente Acta entre el Técnico que rehabilitó este Servicio y el Responsable del mismo, acta contenida en las siguientes cláusulas:

PRIMERA: OBJETIVO

Mantener la Continuidad del Servicio que apalanca a la Gestión Institucional y en caso de emergencia rehabilitarlo conforme a lo establecido en el Acuerdo de Nivel de Servicio.

SEGUNDA: ESCENARIOS DEL SERVICIO

2.1 Estado previo a la emergencia

Emergencia	A momentos se cortaba la comunicación del enlace de radio entre PETROECUADOR y el Dispensario.
Diagnóstico	1. Daño intermitente.

2.2 Estado del Servicio durante la emergencia

Solución	1. Realizar el mantenimiento de la conexión en la estación del Pichincha.

2.3 Estado luego de la emergencia

Normalidad	Utilizar el servicio de Comunicación en forma normal.

TERCERA: DERECHOS Y OBLIGACIONES

3.1 El Responsable del Servicio comprobó que el Servicio está 100% operativo.

3.2 El Técnico alertó al Responsable de este Servicio sobre las características de crecimiento, novedades que se han encontrado y conveniencia del mantenimiento preventivo.

3.3 El funcionario que debido a cualquier causa se separe de la Unidad de Sistemas, como paso previo a la obtención de su liquidación, procederá a capacitar y entregar a otros funcionarios los procedimientos de Continuidad de los Servicios y otros que estuvieron a su cargo.

CUARTA: ALCANCE

Lograr la Continuidad del Servicio que se encontraba en estado de emergencia, aplicando los procedimientos disponibles y/o otros que se requirieron para este fin.

QUINTA: ACEPTACION DE LOS FUNCIONARIOS, PARA QUE PETROECUADOR PUEDA EXIGIR Y DEMANDAR EL CUMPLIMIENTO DE SUS RESPONSABILIDADES

5.1 Aceptar y asumir todas las responsabilidades pertenecientes a la aplicación de procedimientos de Respaldo, Restauración, Recuperación y/ otros tendientes a rehabilitar la Continuidad de este Servicio, así como, de controles y actualización de la documentación respectiva, que también es útil para efectos de auditoría, lo cual incluye la incorporación de los cambios efectuados a la documentación existente y de nuevos procedimientos.

5.2 Aceptar que al suscribir esta acta, son administrativa, personal y pecuniariamente responsables tanto del estado en el cual retorna a la normalidad el Servicio recibido, como por la validez y la actualización de la documentación de los procedimientos aplicados en este caso.

Para constancia y fe de conformidad con lo actuado, suscriben la presente acta en original y tres copias de igual contenido y valor.

ENTREGUÉ CONFORME	**RECIBÍ CONFORME**
Firma y sello:	
Nombre:	
No. Rol. o Céd.Ciud.	

ANEXO 1.3

Provisión / Renovación Telefonía móvil

Documentación mínima:

1.3.1 Un diagrama de bloque que incluya la Planificación y Ejecución

1.3.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

1.3.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

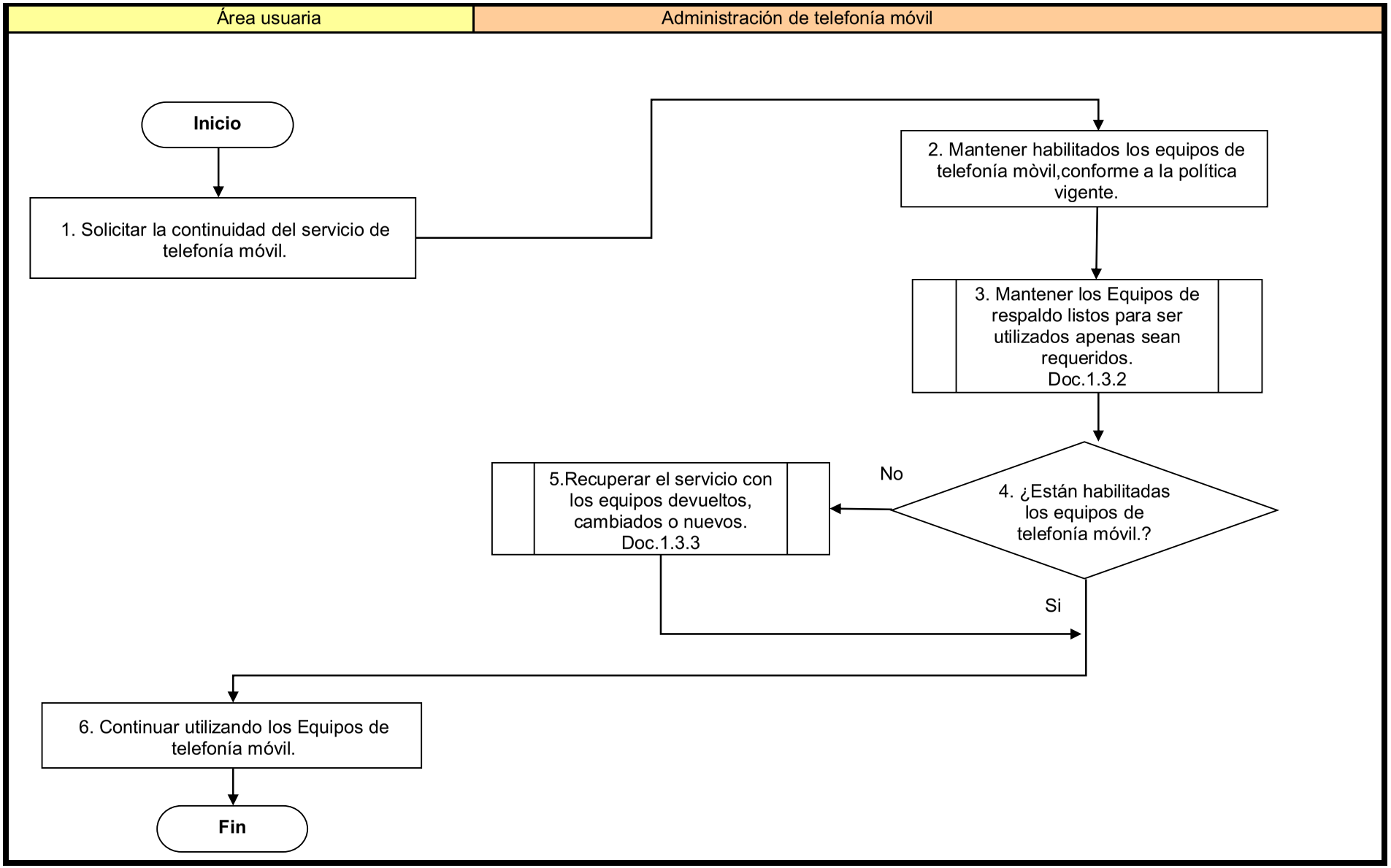
1.3.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

1.3.5 Acta de ER del retorno a la normalidad.

SERVICIO CRÍTICO: "PROVISIÓN / RENOVACION TELEFONÍA MOVIL"

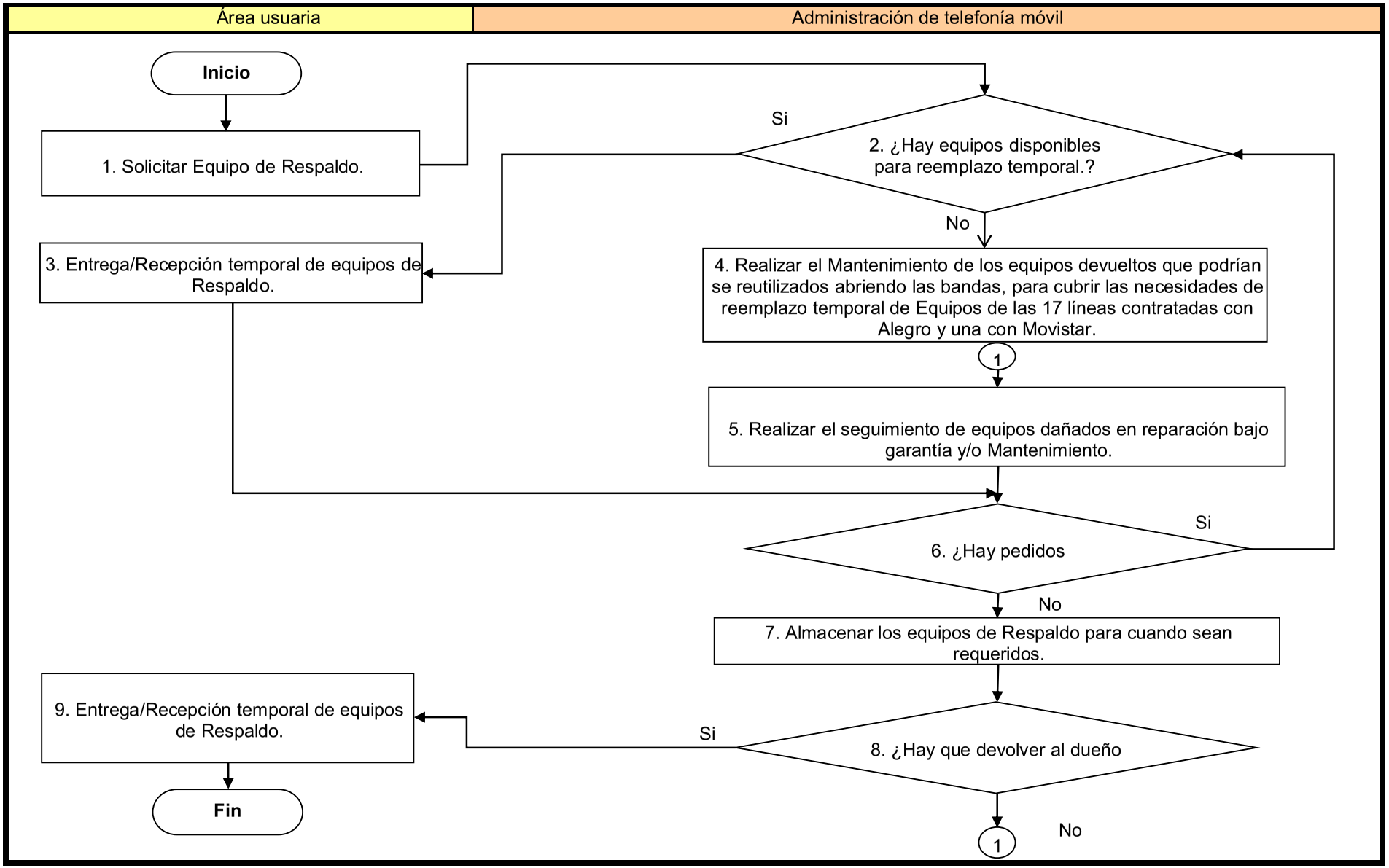
DIAGRAMA DE BLOQUE

Doc.1.3.1



SERVICIO CRÍTICO: "PROVISIÓN / RENOVACION TELEFONÍA MOVIL"
Diagrama del procedimiento de Respaldos y Restauración

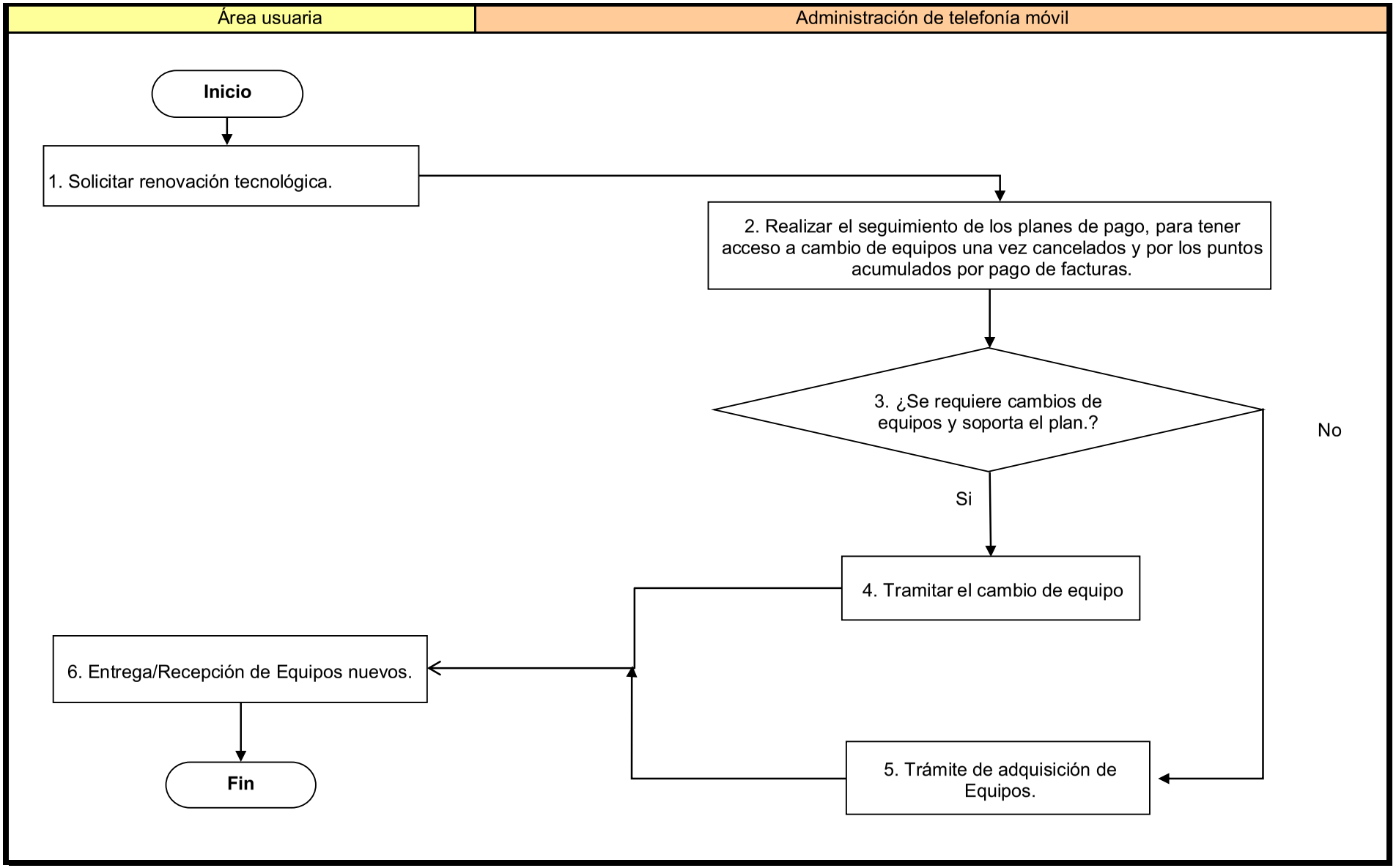
Doc.1.3.2



SERVICIO CRÍTICO: "PROVISIÓN / RENOVACION TELEFONÍA MOVIL"

Diagrama del procedimiento de Recuperación

Doc.1.3.3



SERVICIO CRÍTICO: "PROVISIÓN / RENOVACION TELEFONÍA MOVIL"
Lista de Chequeo

Fecha y hora de inicio:2008-05-13 y 11h00 Fecha y hora de finalización:2008-05-13 y 12h00 **Doc.1.3.4**

No	Procedimientos y pasos	Parámetros a controlar, comparar y evaluar.		Cumplió			Observaciones
		Parámetro	Valor	Si	Par	No	
	Doc.1.3.2 Procedimiento de Respaldos y Restauración						
1	1. Solicitar Equipo de Respaldo						
2	2. ¿Hay equipos disponibles para reemplazo temporal.?						
3	Si. 3. Entrega/Recepción temporal de equipos de Respaldo.						
4	No.4. Realizar el Mantenimiento de los equipos devueltos que podrían ser reutilizados abriendo las bandas, para cubrir las necesidades de reemplazo de Equipos por daño de las 17 líneas contratadas con Alegro y una con Movistar .						
5	5. Realizar el seguimiento de equipos dañados en reparación bajo garantía y/o Mantenimiento.						
6	6. ¿Hay pedidos pendientes.?						
7	Si. Continuar con el paso 2.						
8	No.7. Almacenar los equipos de Respaldo para cuando sean requeridos.						
9	8. ¿Hay que devolver al dueño el equipo reparado.?						
10	Si. 9. Entrega/Recepción temporal de equipos de Respaldo.						
11	No. Continuar con el paso 4.						
	Doc.1.3.3. Diagrama del procedimiento de Recuperaciòn						
12	1. Solicitar renovación tecnológica.			si			
13	2. Realizar el seguimiento de los planes de pago, para tener acceso a cambio de equipos una vez cancelados y por los puntos acumulados por pago de facturas.			si			
14	3. ¿Se requiere cambios de equipos y soporta el plan.?			si			
15	Si.4. Tramitar el cambio de equipo.			si			
16	No.5. Trámite de adquisición de Equipos.						
17	6. Entrega/Recepción de Equipos nuevos.			si			

Nivel de satisfacción del cliente : Total: Si Parcial: ☐ Insatisfecho: ☐

Por el Técnico encargado de rehabilitar el Servicio: Por el Responsable del Servicio:

Firma: _____ _____

Nombre: _____ _____

No. Rol o Cédula de Ciudadanía: _____ _____

SERVICIO CRÍTICO "PROVISIÓN / RENOVACIÓN TELEFONÍA MÓVIL"

Fecha: 2008-05-13 **Acta de Entrega Recepción de Retorno a la Normalidad del Servicio Crítico de TI** **Doc.1.3.5**

Matriz, Filial o Distrito: PETROECUADOR y Unidad: Sistemas

En la ciudad de Quito se suscribe la presente Acta entre el Técnico que rehabilitó este Servicio y el Responsable del mismo, acta contenida en las siguientes cláusulas:

PRIMERA: OBJETIVO

Mantener la Continuidad del Servicio que apalanca a la Gestión Institucional y en caso de emergencia rehabilitarlo conforme a lo establecido en el Acuerdo de Nivel de Servicio.

SEGUNDA: ESCENARIOS DEL SERVICIO

2.1 Estado previo a la emergencia

Emergencia	Se daño el Celular del Gerente Corporativo
Diagnóstico	1. Mantenimiento del Equipo.

2.2 Estado del Servicio durante la emergencia

Solución	1. Realizar el mantenimiento de Equipo.

2.3 Estado luego de la emergencia

Normalidad	Utilizar el servicio de Telefonía móvil en forma normal.

TERCERA: DERECHOS Y OBLIGACIONES

3.1 El Responsable del Servicio comprobó que el Servicio está 100% operativo.

3.2 El Técnico alertó al Responsable de este Servicio sobre las características de crecimiento, novedades que se han encontrado y conveniencia del mantenimiento preventivo.

3.3 El funcionario que debido a cualquier causa se separe de la Unidad de Sistemas, como paso previo a la obtención de su liquidación, procederá a capacitar y entregar a otros funcionarios los procedimientos de Continuidad de los Servicios y otros que estuvieron a su cargo.

CUARTA: ALCANCE

Lograr la Continuidad del Servicio que se encontraba en estado de emergencia, aplicando los procedimientos disponibles y/o otros que se requirieron para este fin.

QUINTA: ACEPTACION DE LOS FUNCIONARIOS, PARA QUE PETROECUADOR PUEDA EXIGIR Y DEMANDAR EL CUMPLIMIENTO DE SUS RESPONSABILIDADES

5.1 Aceptar y asumir todas las responsabilidades pertenecientes a la aplicación de procedimientos de Respaldo, Restauración, Recuperación y/ otros tendientes a rehabilitar la Continuidad de este Servicio, así como, de controles y actualización de la documentación respectiva, que también es útil para efectos de auditoría, lo cual incluye la incorporación de los cambios efectuados a la documentación existente y de nuevos procedimientos.

5.2 Aceptar que al suscribir esta acta, son administrativa, personal y pecuniariamente responsables tanto del estado en el cual retorna a la normalidad el Servicio recibido, como por la validez y la actualización de la documentación de los procedimientos aplicados en este caso.

Para constancia y fe de conformidad con lo actuado, suscriben la presente acta en original y tres copias de igual contenido y valor.

ENTREGUÉ CONFORME	**RECIBÍ CONFORME**
Firma y sello:	
Nombre:	
No. Rol. o Céd.Ciud.	

ANEXO 1.4

Correo Electrónico

Documentación mínima:

1.4.1 Un diagrama de bloque que incluya la Planificación y Ejecución

1.4.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

1.4.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

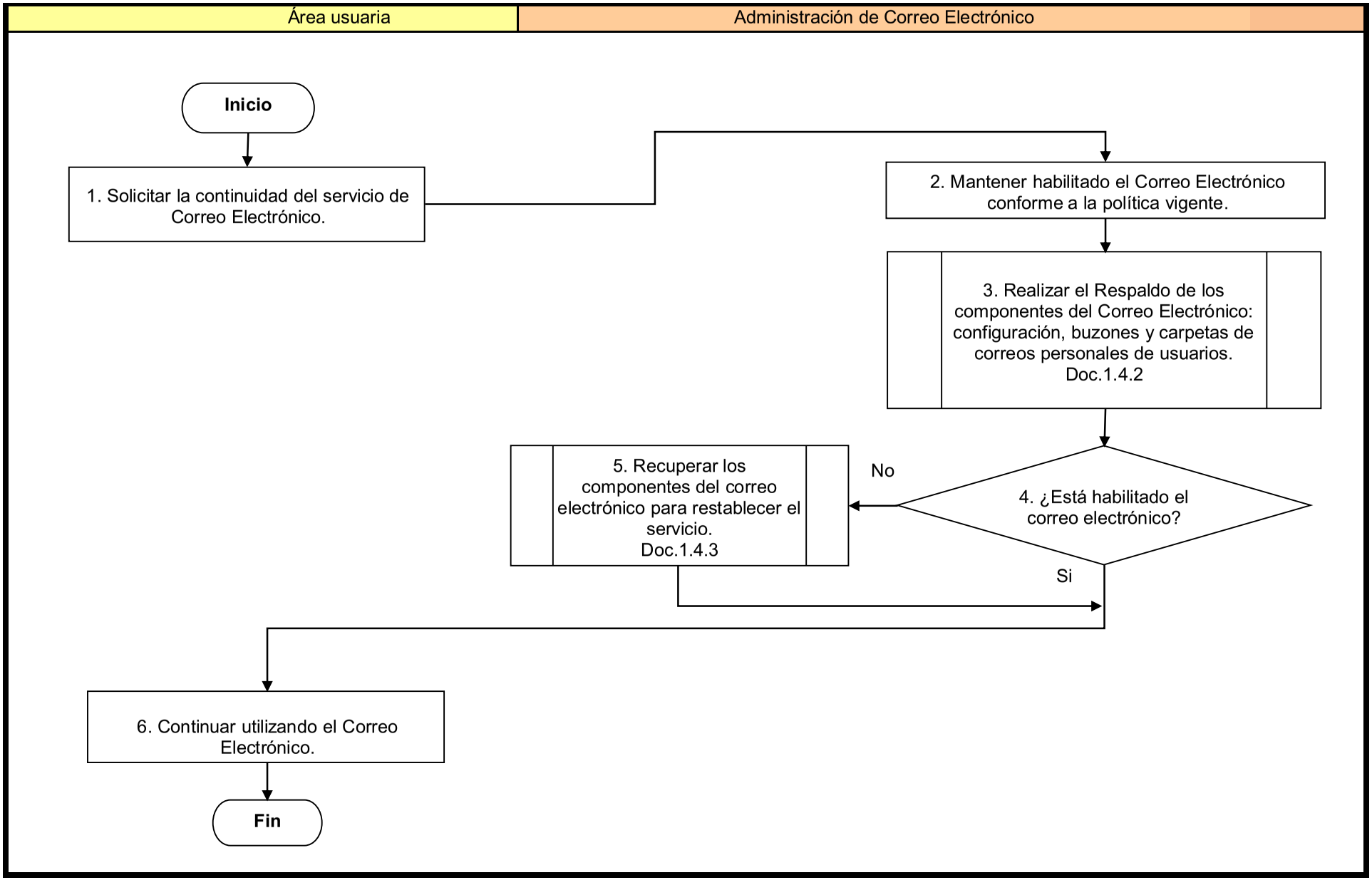
1.4.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

1.4.5 Acta de ER del retorno a la normalidad.

SERVICIO CRÍTICO: "CORREO ELECTRÓNICO."

Diagrama de Bloque

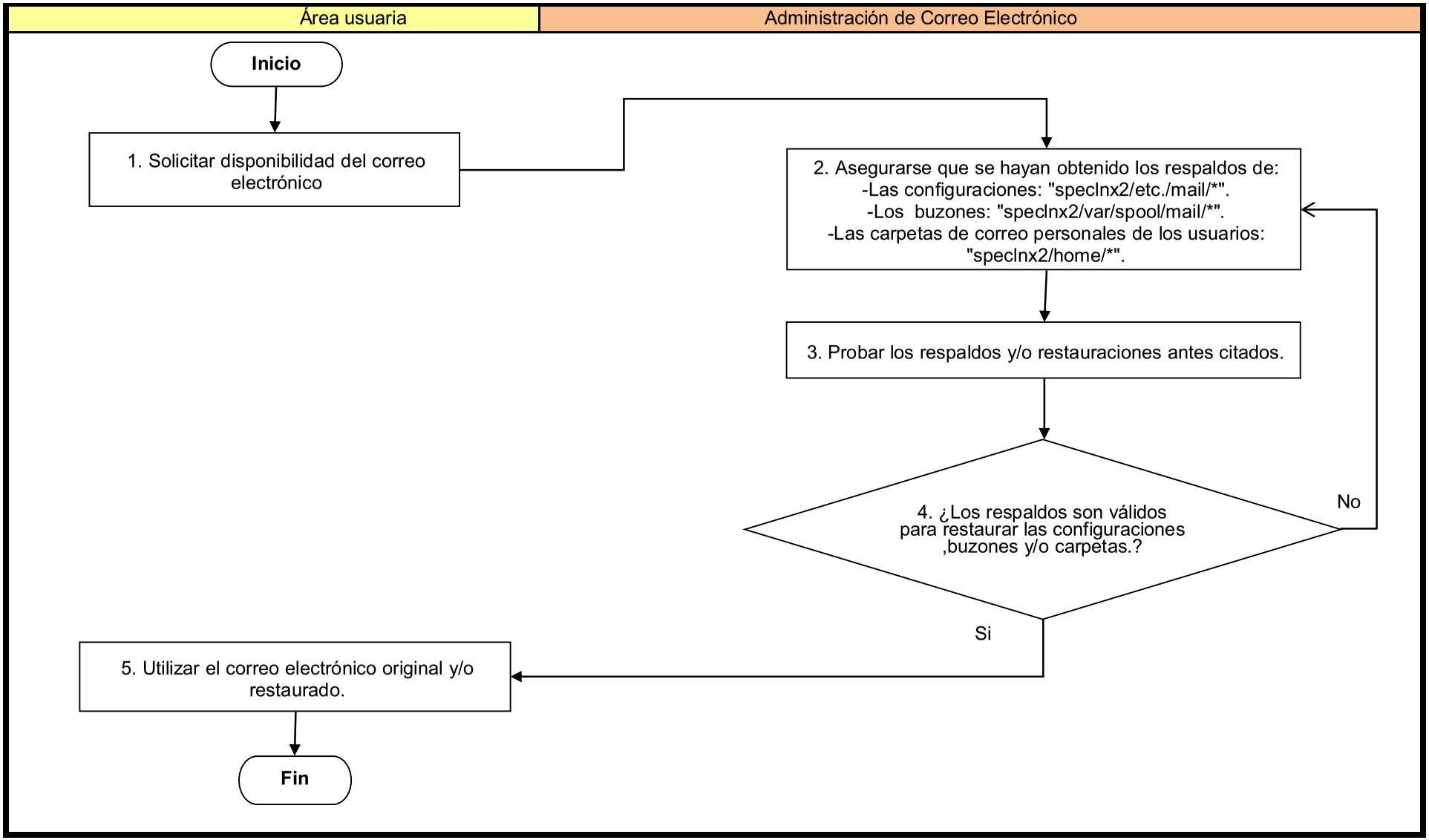
Doc.1.4.1



SERVICIO CRÍTICO: "CORREO ELECTRÓNICO."

Diagrama del procedimiento de Respaldos y Restauración

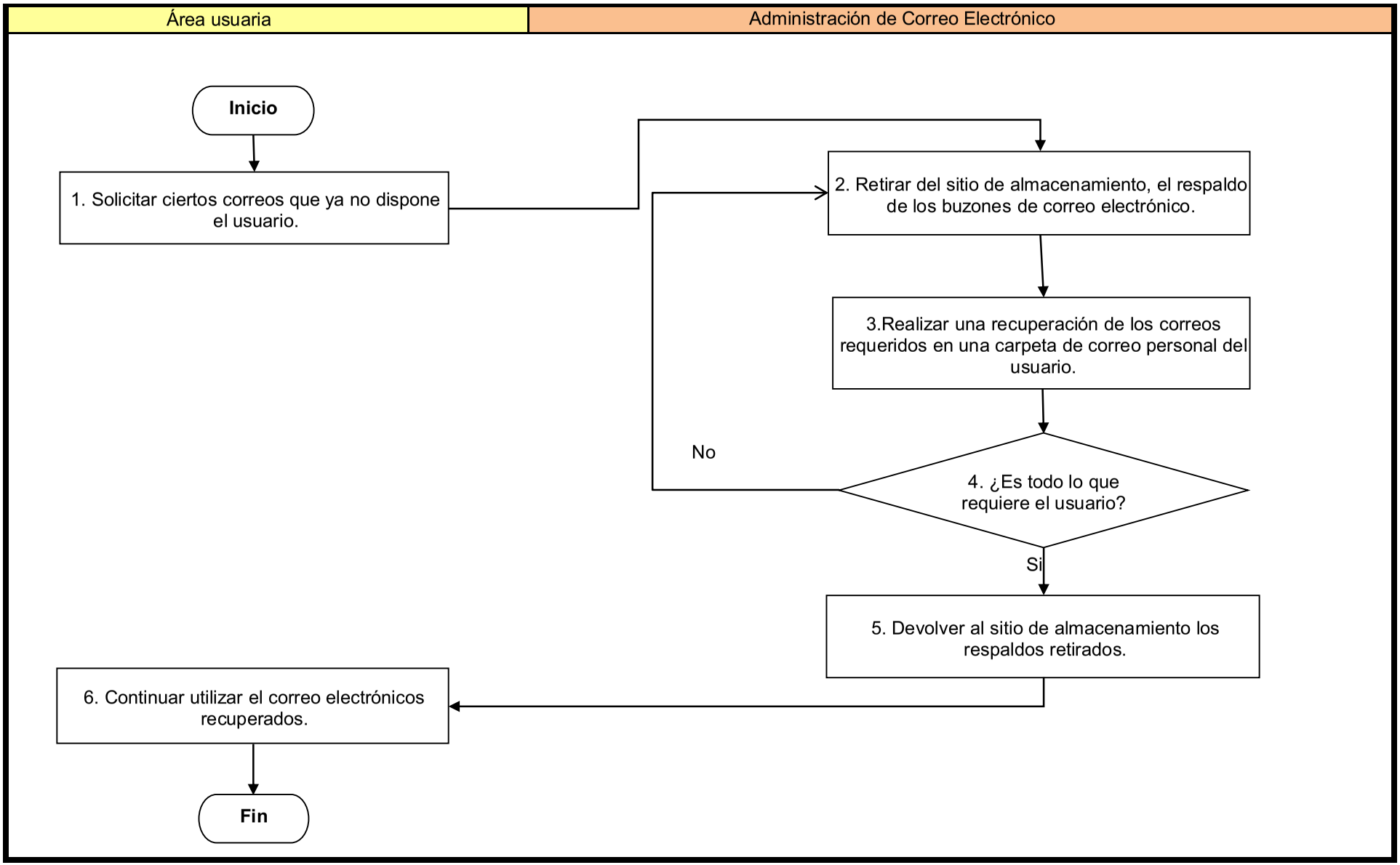
Doc.1.4.2



SERVICIO CRÍTICO: "CORREO ELECTRÓNICO."

Diagrama del procedimiento de Recuperación

Doc.1.4.3



SERVICIO CRÍTICO: "CORREO ELECTRÓNICO."
Lista de Chequeo

Fecha y hora de inicio:2008-01-02 y 8h00 Fecha y hora de finalización:2008-01-02 y 9h00 **Doc.1.4.4**

No	Procedimientos y pasos	Parámetros a controlar, comparar y evaluar.		Cumplió			Observaciones
		Parámetro	Valor	Si	Par	No	
	Doc.1.4.2 Procedimiento de Respaldos y Restauración						
1	1. Solicitar disponibilidad del correo electrónico.						
2	2. Asegurarse que se hayan obtenido los respaldos de: -Las configuraciones: "speclnx2/etc./mail/*". -En buzones: "speclnx2/var/spool/mail/*". -Las carpetas de correo personales de los usuarios: "speclnx2/home/*".						
3	3. Probar los respaldos y/o restauraciones antes citados.						
4	4. ¿Los respaldos son válidos para restaurar las configuraciones ,buzones y/o carpetas.?						
5	No. Continuar con el paso 2.						
6	Si.5. Utilizar el correo electrónico original y/o restaurado.						
	1.4.3 Diagrama del procedimiento de Recuperación						
7	1. Solicitar ciertos correos que ya no dispone el usuario.			si			
8	2. Retirar del sitio de almacenamiento, el respaldo de los buzones de correo electrónico.			si			
9	3.Realizar una recuperación de los correos requeridos en una carpeta de correo personal del usuario.			si			
10	4. ¿Es todo lo que requiere el usuario.?			si			
11	No. Continuar con el paso 2.						
12	5. Devolver al sitio de almacenamiento los respaldos retirados.			si			
13	6. Continuar utilizar el correo electrónico recuperado.			si			

Nivel de satisfacción del cliente : Total: Si ☐ Parcial: ☐ Insatisfecho: ☐

Por el Técnico encargado de rehabilitar el Servicio:

Firma: _____
Nombre: _____
No. Rol o Cédula de Ciudadanía: _____

Por el Responsable del Servicio:

_____
_____
_____

SERVICIO CRÍTICO "CORREO ELECTRÓNICO"

Fecha: 2008-01-02 **Acta de Entrega Recepción de Retorno a la Normalidad del Servicio Crítico de TI** **Doc.1.4.5**

Matriz, Filial o Distrito: PETROECUADOR y Unidad: Sistemas

En la ciudad de Quito se suscribe la presente Acta entre el Técnico que rehabilitó este Servicio y el Responsable del mismo, acta contenida en las siguientes cláusulas:

PRIMERA: OBJETIVO

Mantener la Continuidad del Servicio que apalanca a la Gestión Institucional y en caso de emergencia rehabilitarlo conforme a lo establecido en el Acuerdo de Nivel de Servicio.

SEGUNDA: ESCENARIOS DEL SERVICIO

2.1 Estado previo a la emergencia

Emergencia	Se borraron correos del buzón del Gerente Corporativo
Diagnóstico	1. Restauración de buzones hasta encontrar los correos borrados.

2.2 Estado del Servicio durante la emergencia

Solución	1. Realizar una recuperación parcial del Buzón para copiar los correos requeridos a una carpeta de correo personal del usuario.

2.3 Estado luego de la emergencia

Normalidad	Acceder a la carpeta creada para disponer de los correos que fueron recuperados.

TERCERA: DERECHOS Y OBLIGACIONES

3.1 El Responsable del Servicio comprobó que el Servicio está 100% operativo.

3.2 El Técnico alertó al Responsable de este Servicio sobre las características de crecimiento, novedades que se han encontrado y conveniencia del mantenimiento preventivo.

3.3 El funcionario que debido a cualquier causa se separe de la Unidad de Sistemas, como paso previo a la obtención de su liquidación, procederá a capacitar y entregar a otros funcionarios los procedimientos de Continuidad de los Servicios y otros que estuvieron a su cargo.

CUARTA: ALCANCE

Lograr la Continuidad del Servicio que se encontraba en estado de emergencia, aplicando los procedimientos disponibles y/o otros que se requirieron para este fin.

QUINTA: ACEPTACION DE LOS FUNCIONARIOS, PARA QUE PETROECUADOR PUEDA EXIGIR Y DEMANDAR EL CUMPLIMIENTO DE SUS RESPONSABILIDADES

5.1 Aceptar y asumir todas las responsabilidades pertenecientes a la aplicación de procedimientos de Respaldo, Restauración, Recuperación y/ otros tendientes a rehabilitar la Continuidad de este Servicio, así como, de controles y actualización de la documentación respectiva, que también es útil para efectos de auditoría, lo cual incluye la incorporación de los cambios efectuados a la documentación existente y de nuevos procedimientos.

5.2 Aceptar que al suscribir esta acta, son administrativa, personal y pecuniariamente responsables tanto del estado en el cual retorna a la normalidad el Servicio recibido, como por la validez y la actualización de la documentación de los procedimientos aplicados en este caso.

Para constancia y fe de conformidad con lo actuado, suscriben la presente acta en original y tres copias de igual contenido y valor.

ENTREGUÉ CONFORME	**RECIBÍ CONFORME**
Firma y sello:	
Nombre:	
No. Rol. o Céd.Ciud.	

ANEXO 1.5

Instalación / reparación de Energía regulada y Red de Datos

Documentación mínima:

1.5.1 Un diagrama de bloque que incluya la Planificación y Ejecución

1.5.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

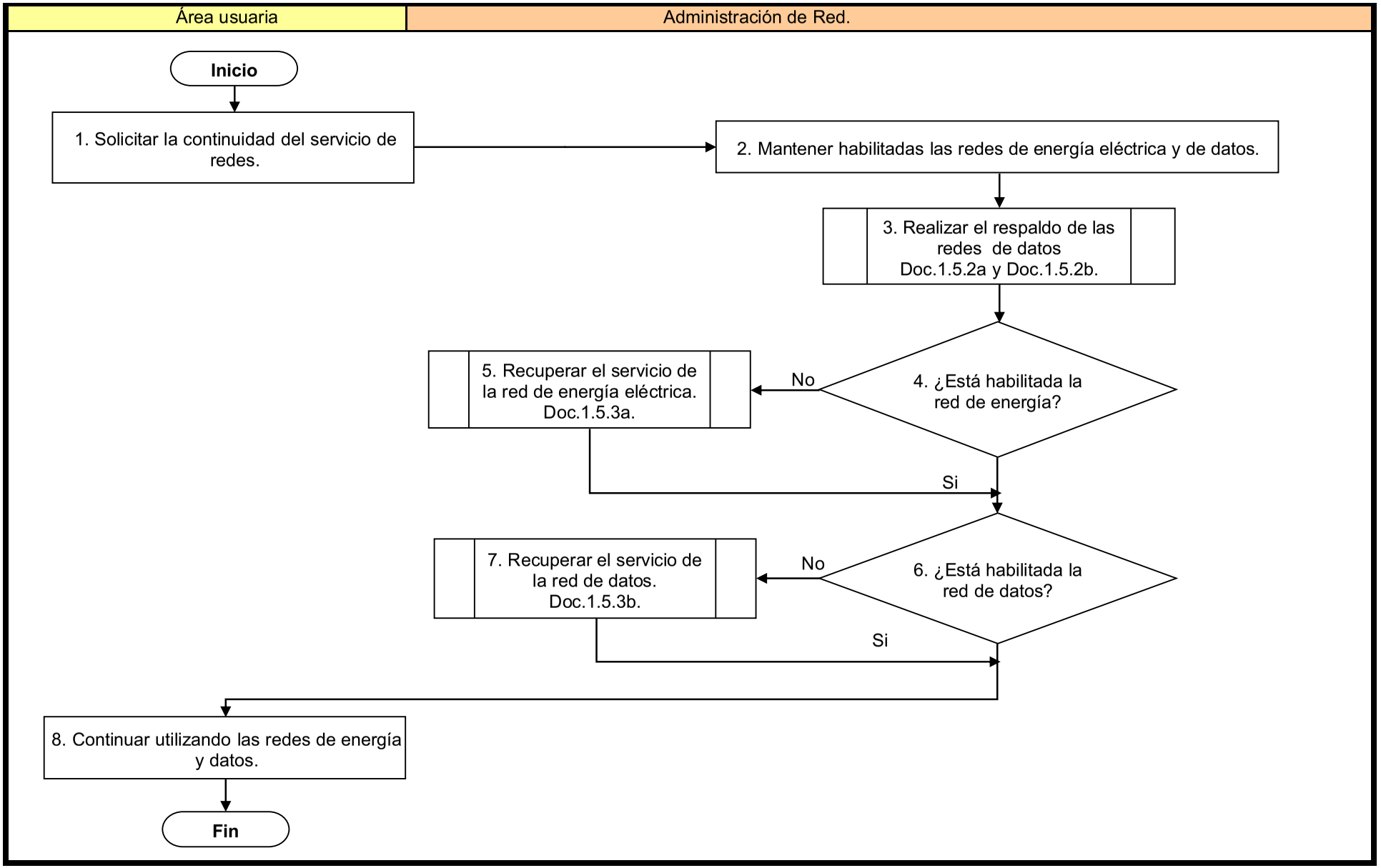
1.5.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

1.5.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

1.5.5 Acta de ER del retorno a la normalidad.

SERVICIO CRITICO:"INSTALACIÓN/ REPARACIÓN DE ENERGÍA REGULADA Y RED DE DATOS"

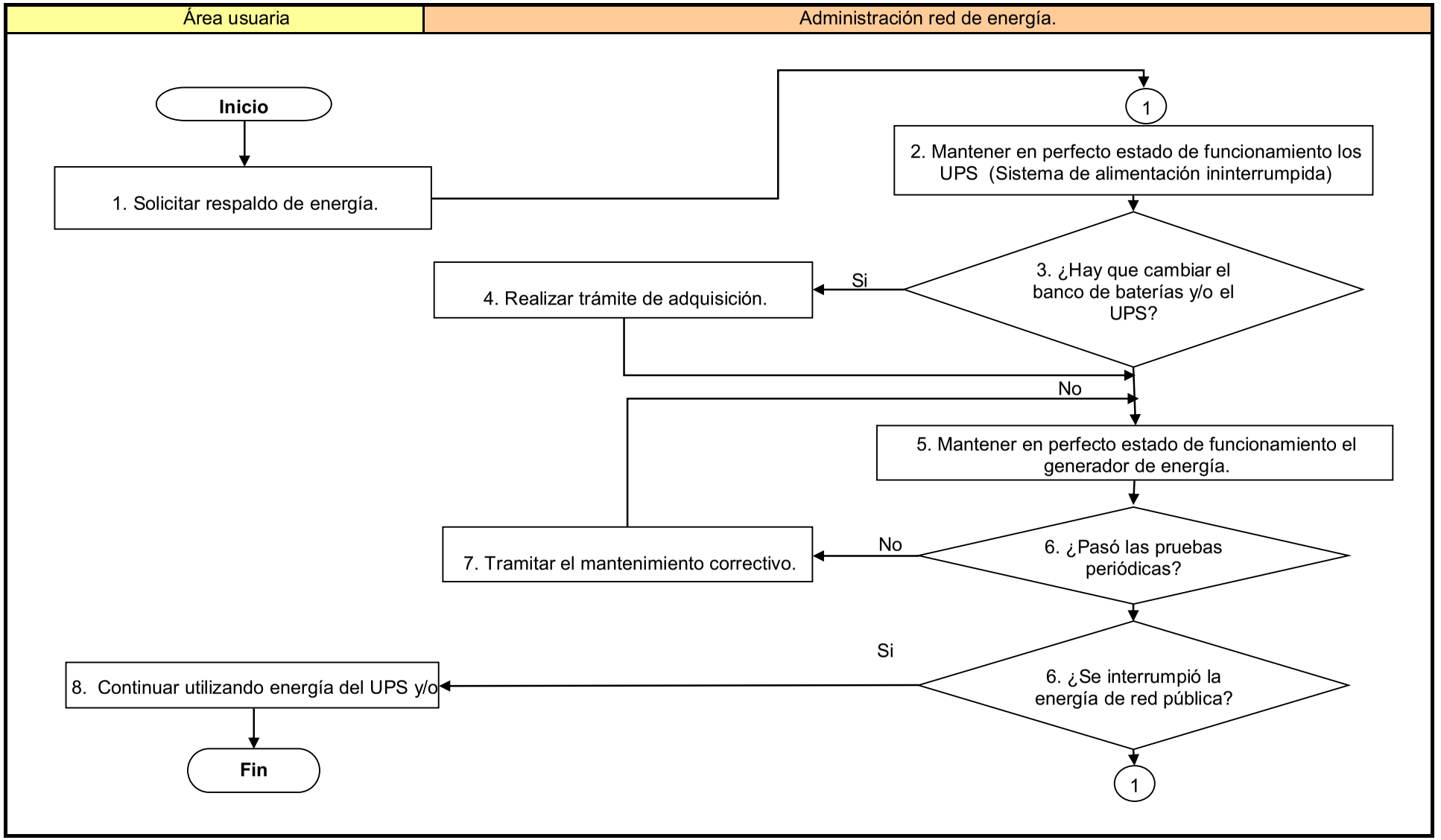
Diagrama de Bloque **Doc.1.5.1**



SERVICIO CRITICO:"INSTALACIÓN/ REPARACIÓN DE ENERGÍA REGULADA Y RED DE DATOS"

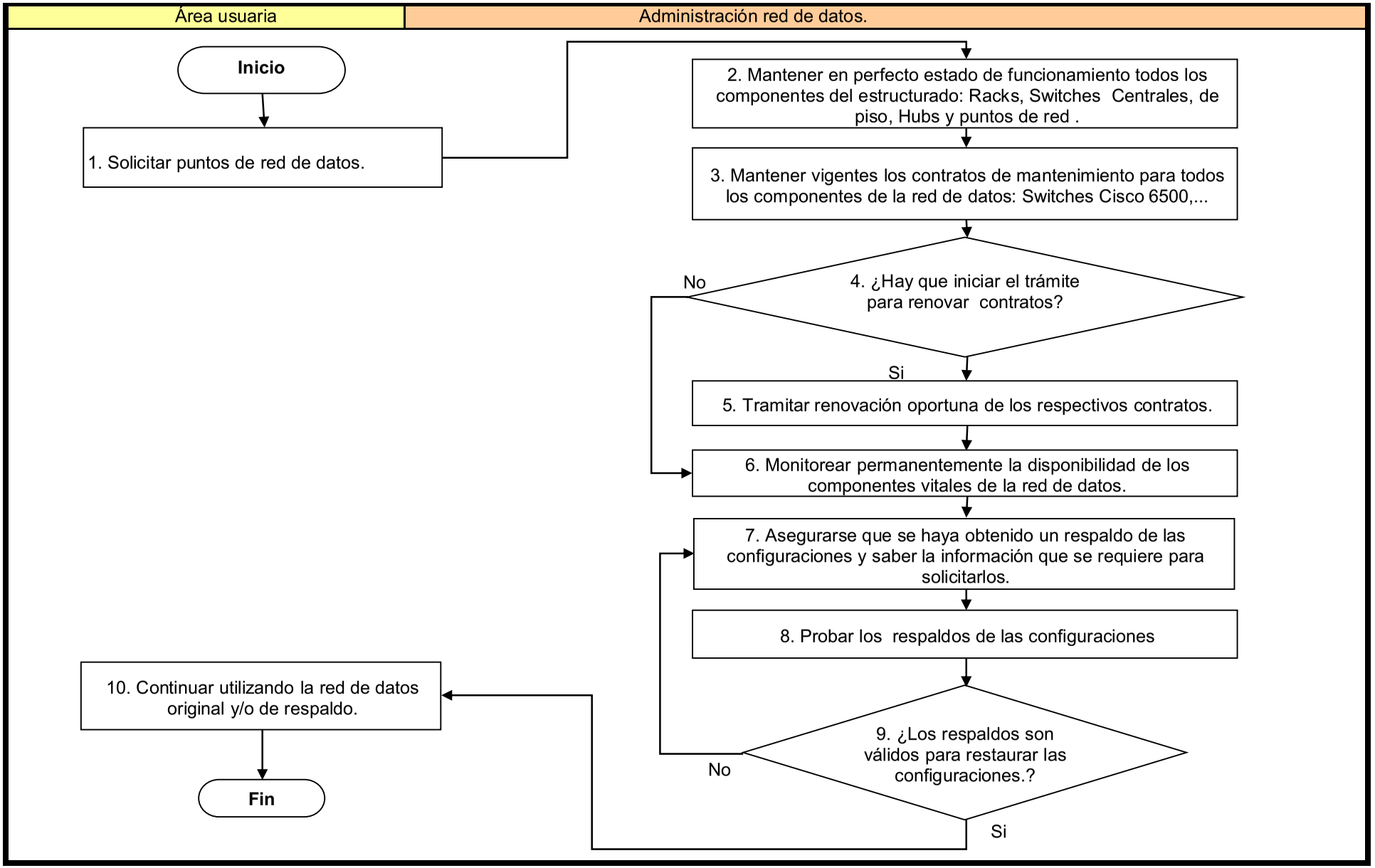
Diagrama del procedimiento de Respaldos y Restauración

Doc.1.5.2.a.



SERVICIO CRITICO:"INSTALACIÓN/ REPARACIÓN DE ENERGÍA REGULADA Y RED DE DATOS"
Diagrama del procedimiento de Respaldos y Restauración

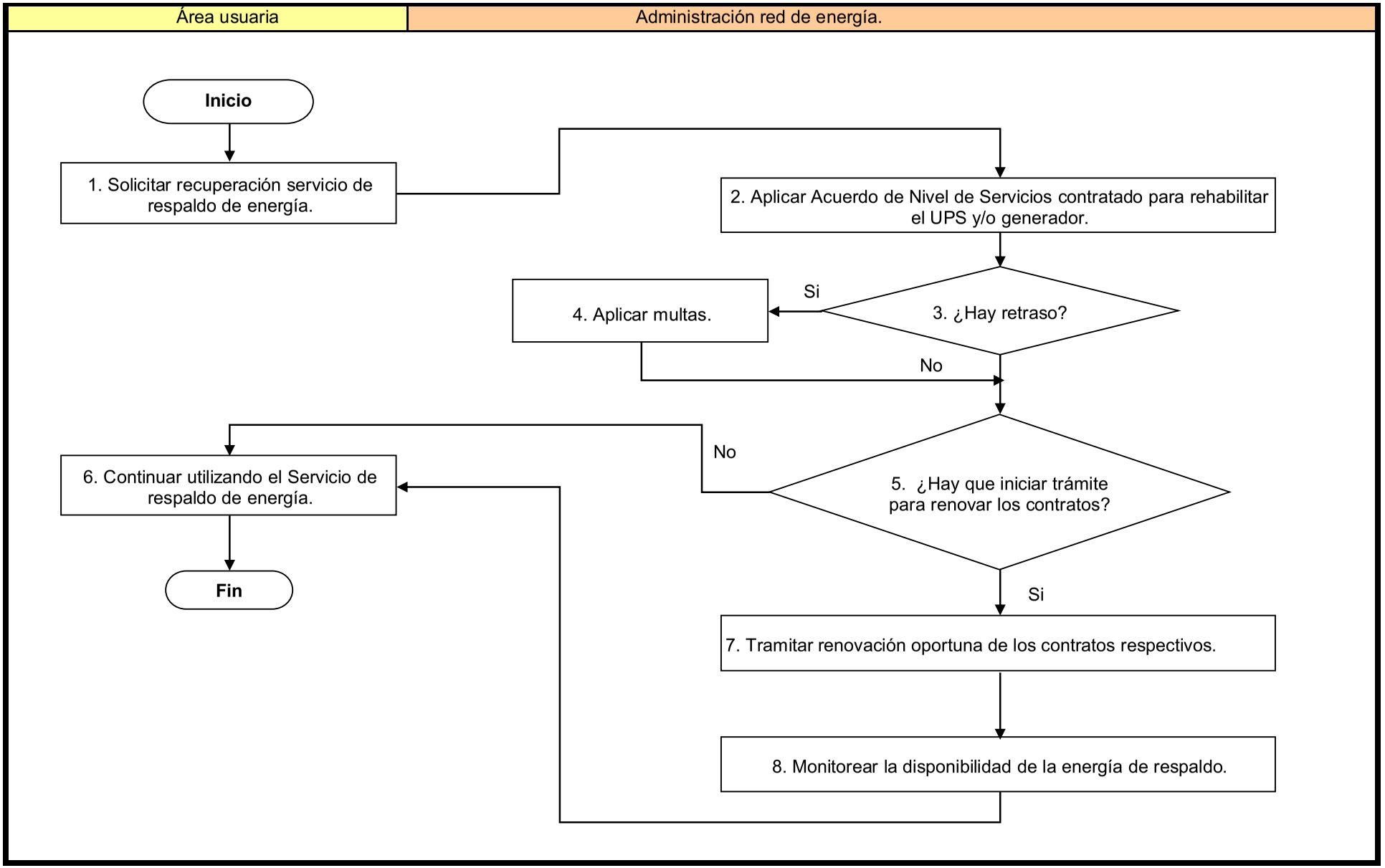
Doc.1.5.2.b.



SERVICIO CRITICO:"INSTALACIÓN/ REPARACIÓN DE ENERGÍA REGULADA Y RED DE DATOS"

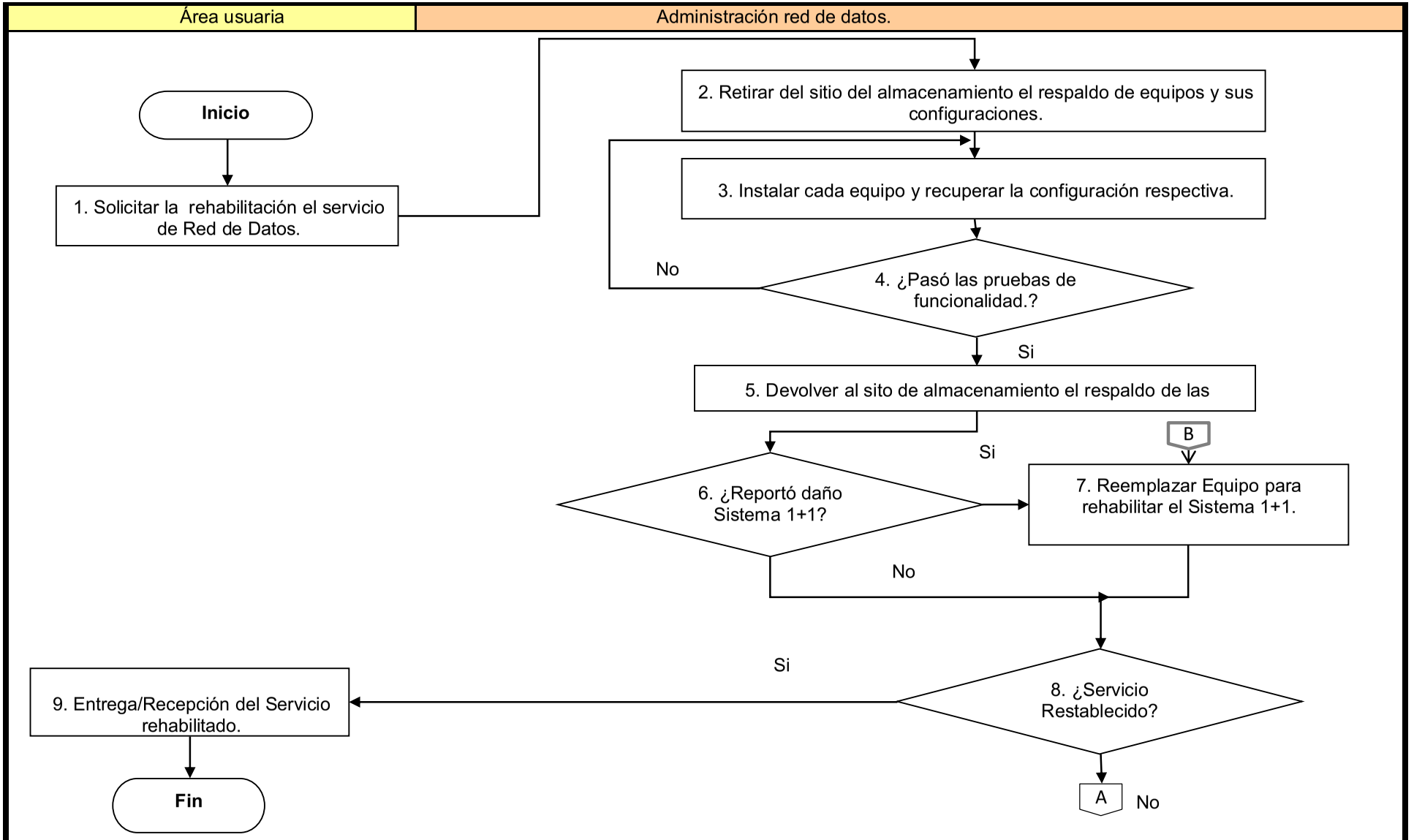
Diagrama del procedimiento de Recuperación.

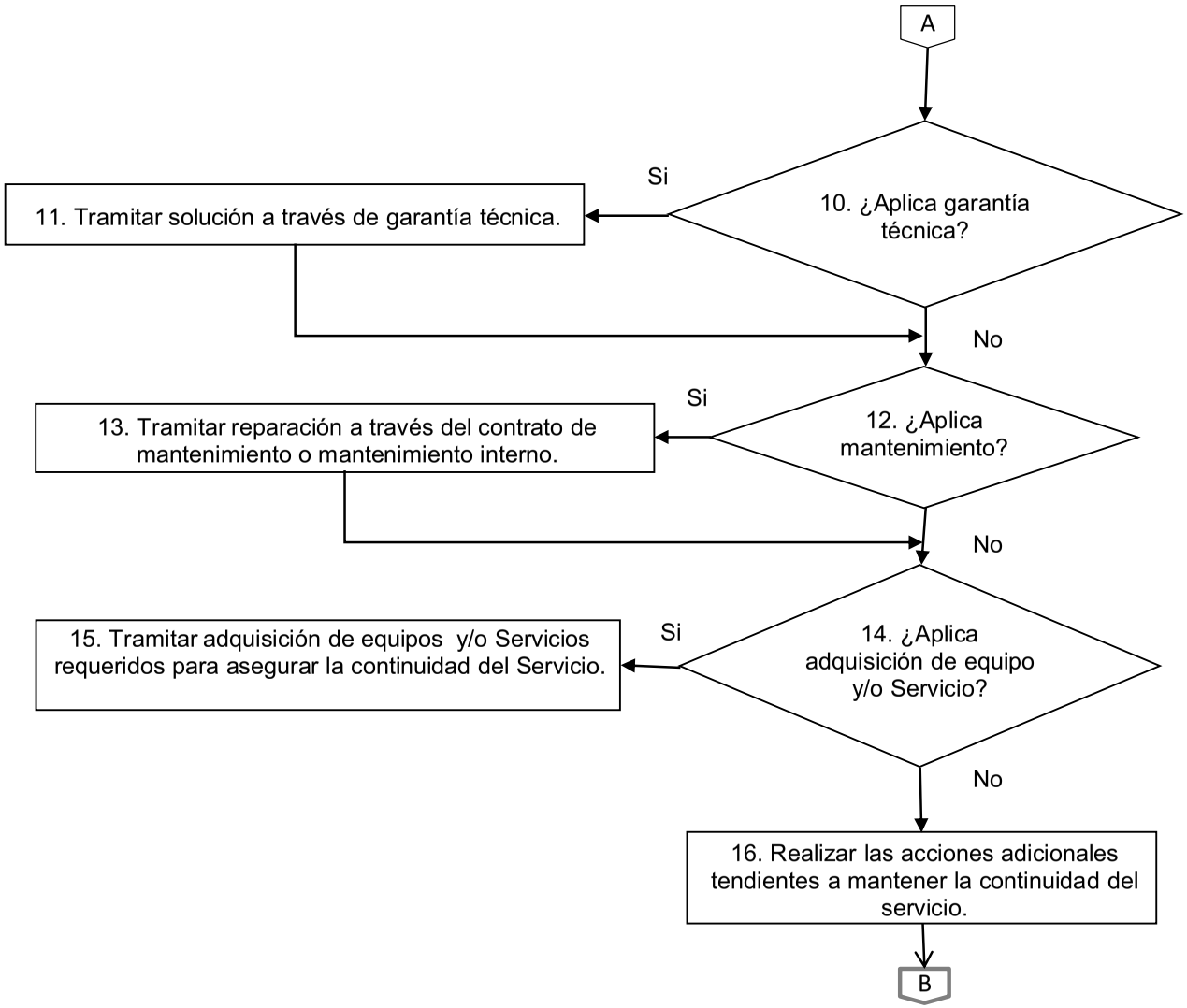
Doc.1.5.3.a.



SERVICIO CRITICO:"INSTALACIÓN/ REPARACIÓN DE ENERGÍA REGULADA Y RED DE DATOS"
Diagrama del procedimiento de Recuperación

Doc.1.5.3.b.




A
10. ¿Aplica garantía técnica?
Si
11. Tramitar solución a través de garantía técnica.
No
12. ¿Aplica mantenimiento?
Si
13. Tramitar reparación a través del contrato de mantenimiento o mantenimiento interno.
No
14. ¿Aplica adquisición de equipo y/o Servicio?
Si
15. Tramitar adquisición de equipos y/o Servicios requeridos para asegurar la continuidad del Servicio.
No
16. Realizar las acciones adicionales tendientes a mantener la continuidad del servicio.
B

SERVICIO CRITICO:"INSTALACIÓN/ REPARACIÓN DE ENERGÍA REGULADA Y RED DE DATOS"
Lista de Chequeo

Fecha y hora de inicio:2008-06-24 y 17h00 Fecha y hora de finalización:2008-06-25 y 13h00 **Doc.1.5.4**

No	Procedimientos y pasos	Parámetros a controlar, comparar y evaluar.		Cumplió			Observaciones
		Parámetro	Valor	Si	Par	No	
	Doc.1.5.2.a Diagrama del procedimiento de Respaldos y Restauración "Red de Energía."						
1	1. Solicitar respaldo de energía.						
2	2. Mantener en perfecto estado de funcionamiento los UPS.						
3	3. ¿Hay que cambiar el banco de baterías y/o el UPS.?						
4	Si .4. Realizar trámite de adquisición.						
5	No. 5. Mantener en perfecto estado de funcionamiento el generador de energía.						
6	6. ¿Pasó las pruebas periódicas.?						
7	No.7. Tramitar el mantenimiento correctivo.						
8	Si.6. ¿Se interrumpió la energía de red pública.?						
9	No.8. Continuar utilizando energía de UPS y/o generador.						
	Doc.1.5.2.b. Diagrama del procedimiento de Respaldos y Restauración "Red de Datos."						
10	1. Solicitar puntos de red de datos.						
11	2. Mantener en perfecto estado de funcionamiento todos los componentes del estructurado: Racks,Switches Centrales, de piso, hubs y puntos de red .						
12	3. Mantener vigentes los contratos de mantenimiento para todos los componentes de la red de datos: Switches Cisco 6500,...						
13	4. ¿Hay que iniciar el trámite para renovar contratos.?						
14	Si. 5. Tramitar renovación oportuna de los respectivos contratos.						
15	No.6. Monitorear permanentemente la disponibilidad de los componentes vitales de la red de datos.						
16	7. Asegurarse que se haya obtenido un respaldo de las configuraciones y saber la información que se requiere para solicitarlos.						
17	8. Probar los respaldos de las configuraciones						
18	9. ¿Los respaldos son válidos para restaurar las configuraciones.?						
19	No. Continuar con el paso 7.						
20	Si. 10. Continuar utilizando la red de datos original y/o de respaldo.						
	Doc.1.5.3.a.Diagrama del procedimiento de Recuperación "Red de Energía"						
21	1. Solicitar recuperación servicio de respaldo de energía.			si			
22	2, Monitorear la disponibilidad de la energía del respaldo.			si			
23	3. Aplicar Acuerdo de Nivel de servicios contratado para rehabilitar el UPS (Sistema de Alimentación Ininterrumpida) y/o generador.			si			
24	4. ¿Hay retraso.?						
25	Si. 5. Aplicar multas.						
26	No. 6. ¿Hay que iniciar trámite para renovar los contratos.?			si			
27	No. 7. Continuar utilizando el servicio de respaldo de energía.						
28	Si. 8. Tramitar renovación oportuna de los contratos respectivos.			si			
	Doc.1.5.3.b. Diagrama del procedimiento de Recuperación "Red de Datos."						

29	1. Solicitar la rehabilitación el servicio de Red de Datos.			si			
30	2. Retirar del sitio del almacenamiento el respaldo de equipos y sus configuraciones.			si			
31	3. Instalar cada equipo y recuperar la configuración respectiva.						
32	4. ¿Pasó las pruebas de funcionalidad.?			si			
33	No. Continuar con el paso 3.			si			
34	Si. 5. Devolver al sito de almacenamiento el respaldo de las configuración.			si			
35	6. ¿Reportó daño Sistema 1+1?			si			
36	Si. 7. Reemplazar Equipo para rehabilitar el Sistema 1+1.			si			
37	No. 8. ¿Servicio Restablecido?						
38	8. ¿Servicio Restablecido?			si			
39	Si. 9. Entrega/Recepción del servicio rehabilitado			si			
40	No. 10. ¿Aplica garantía Técnica?						
41	Si. 11. Tramitar solución a través de Garantía Técnica			si			
42	No. 12. ¿Aplica Mantenimiento?						
43	Si.13.Tramitar reparación a través del contrato de Mantenimiento. o Mantenimiento interno.			si			
44	No. 14. ¿Aplica adquisición de equipo y/o servicio?						
45	Si. 15. Tramitar adquisición de equipos y/o servicios requeridos para asegurar la continuidad del servicio			si			
46	No. 16. Realizar las acciones adicionales tendientes a mantener la continuidad del servicio.			si			
47	8. ¿Servicio Restablecido?			si			

Nivel de satisfacción del cliente : Total: Si Parcial: ☐ Insatisfecho: ☐

Por el Técnico encargado de rehabilitar el Servicio:

Firma: _____

Nombre: _____

No. Rol o Cédula de Ciudadanía: _____

Por el Responsable del Servicio:

_____

_____

_____

SERVICIO CRÍTICO "INSTALACIÓN / REPARACIÓN DE ENERGÍA REGULADA Y RED DE DATOS"

Fecha: 2008-06-24 **Acta de Entrega Recepción de Retorno a la Normalidad del Servicio Crítico de TI** **Doc.1.5.5**

Matriz, Filial o Distrito: PETROECUADOR y Unidad: Sistemas

En la ciudad de Quito se suscribe la presente Acta entre el Técnico que rehabilitó este Servicio y el Responsable del mismo, acta contenida en las siguientes cláusulas:

PRIMERA: OBJETIVO

Mantener la Continuidad del Servicio que apalanca a la Gestión Institucional y en caso de emergencia rehabilitarlo conforme a lo establecido en el Acuerdo de Nivel de Servicio.

SEGUNDA: ESCENARIOS DEL SERVICIO

2.1 Estado previo a la emergencia

Emergencia	Se perdía intermitentemente la comunicación con la Red LAN.
Diagnóstico	1. Daño del conector giba bit del patch panel del switch Cisco 6500.

2.2 Estado del Servicio durante la emergencia

Solución	1. Cambiar a otro pórtico giga bit en el mismo switch Cisco 6500. 2. Reparar o reemplazar el pórtico dañado.

2.3 Estado luego de la emergencia

Normalidad	Utilizar la Red LAN normalmente.

TERCERA: DERECHOS Y OBLIGACIONES

3.1 El Responsable del Servicio comprobó que el Servicio está 100% operativo.

3.2 El Técnico alertó al Responsable de este Servicio sobre las características de crecimiento, novedades que se han encontrado y conveniencia del mantenimiento preventivo.

3.3 El funcionario que debido a cualquier causa se separe de la Unidad de Sistemas, como paso previo a la obtención de su liquidación, procederá a capacitar y entregar a otros funcionarios los procedimientos de Continuidad de los Servicios y otros que estuvieron a su cargo.

CUARTA: ALCANCE

Lograr la Continuidad del Servicio que se encontraba en estado de emergencia, aplicando los procedimientos disponibles y/o otros que se requirieron para este fin.

QUINTA: ACEPTACION DE LOS FUNCIONARIOS, PARA QUE PETROECUADOR PUEDA EXIGIR Y DEMANDAR EL CUMPLIMIENTO DE SUS RESPONSABILIDADES

5.1 Aceptar y asumir todas las responsabilidades pertenecientes a la aplicación de procedimientos de Respaldo, Restauración, Recuperación y/ otros tendientes a rehabilitar la Continuidad de este Servicio, así como, de controles y actualización de la documentación respectiva, que también es útil para efectos de auditoría, lo cual incluye la incorporación de los cambios efectuados a la documentación existente y de nuevos procedimientos.

5.2 Aceptar que al suscribir esta acta, son administrativa, personal y pecuniariamente responsables tanto del estado en el cual retorna a la normalidad el Servicio recibido, como por la validez y la actualización de la documentación de los procedimientos aplicados en este caso.

Para constancia y fe de conformidad con lo actuado, suscriben la presente acta en original y tres copias de igual contenido y valor.

ENTREGUÉ CONFORME	**RECIBÍ CONFORME**
Firma y sello:	
Nombre:	
No. Rol. o Céd.Ciud.	

ANEXO 1.6

Gestión de Respaldos

Documentación mínima:

1.6.1 Un diagrama de bloque que incluya la Planificación y Ejecución

1.6.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

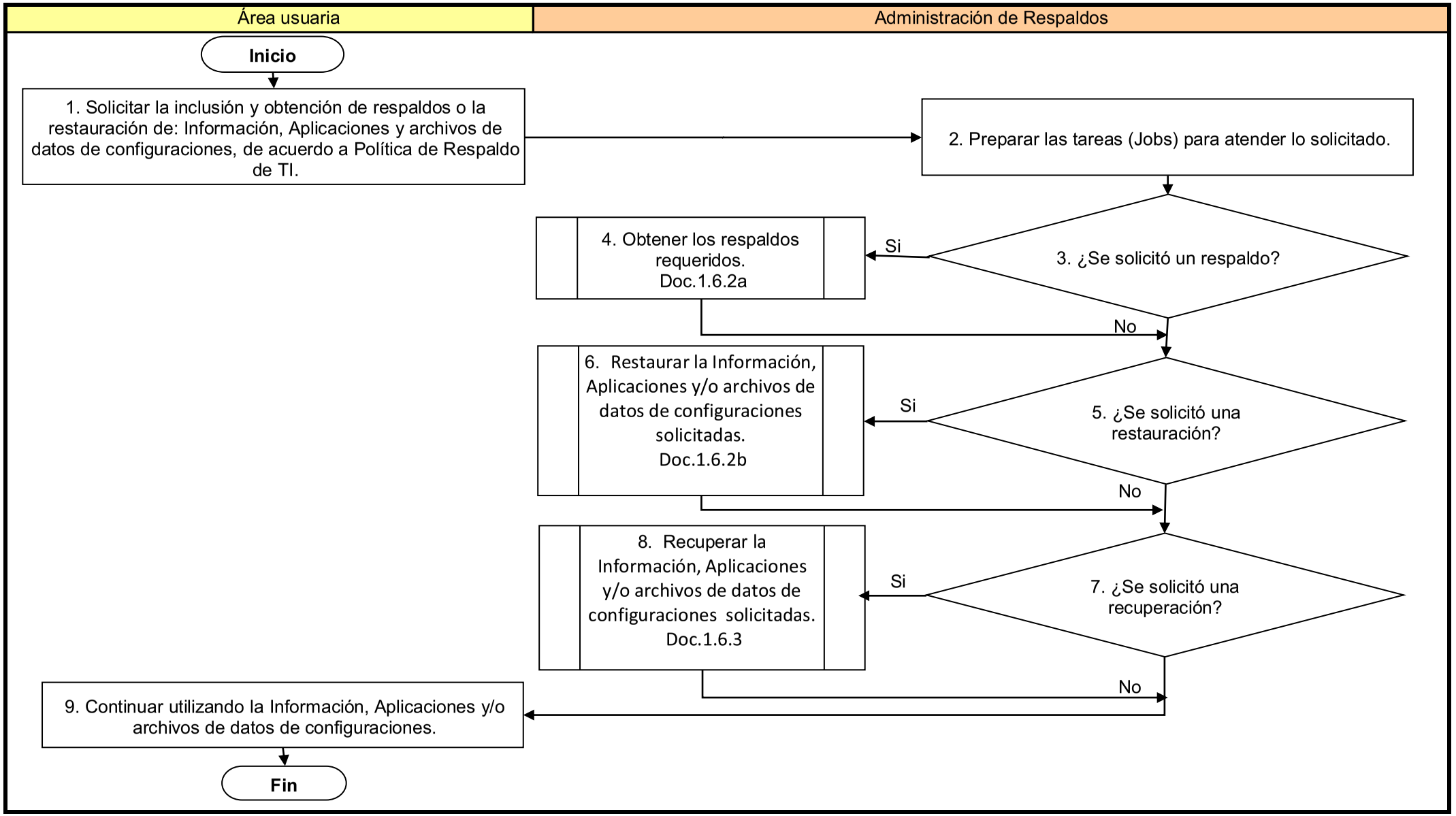
1.6.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

1.6.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

1.6.5 Acta de ER del retorno a la normalidad.

SERVICIO CRÍTICO DE TI:" GESTIÓN DE RESPALDOS."

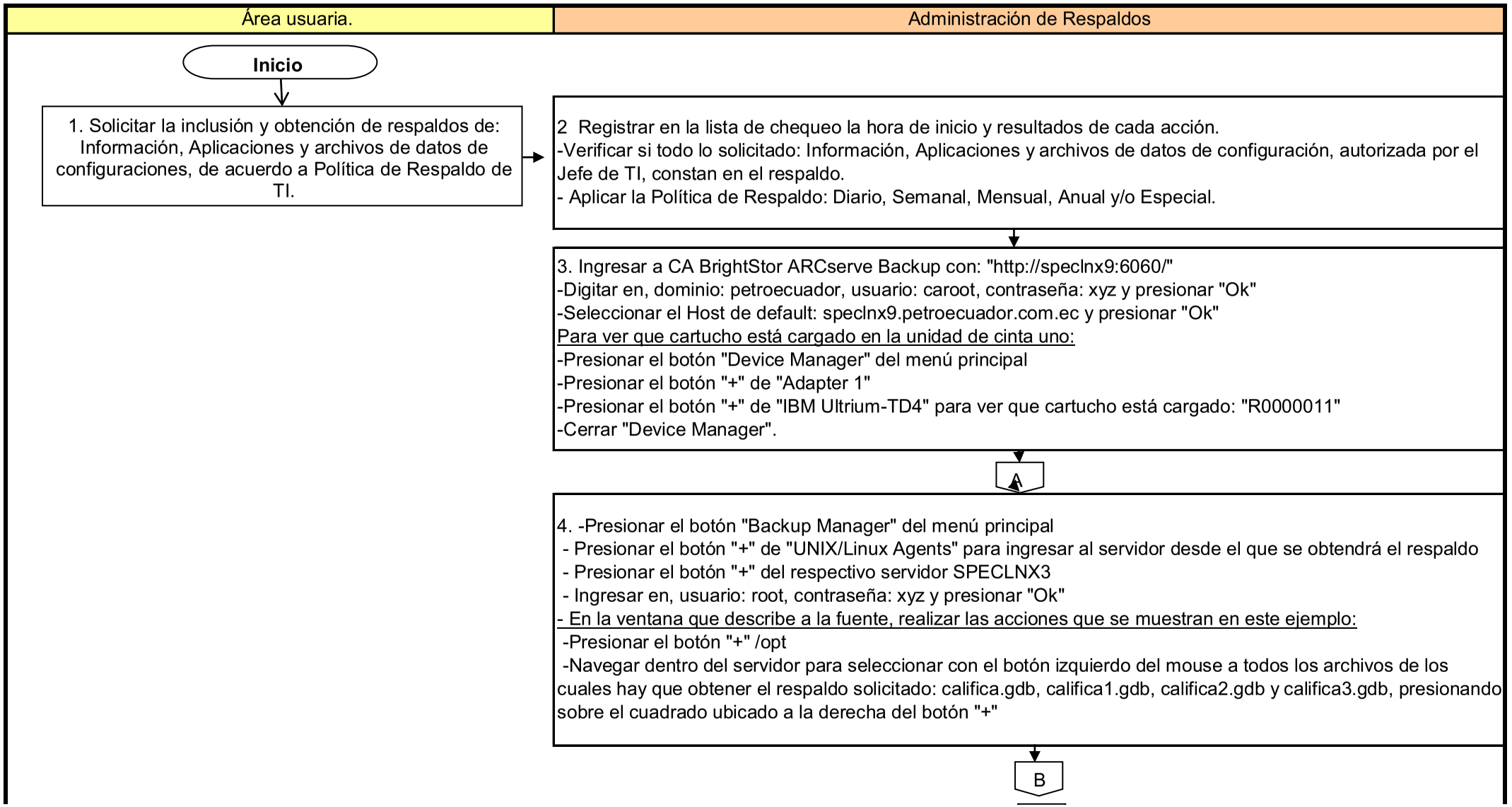
Diagrama de Bloque **Doc.1.6.1**

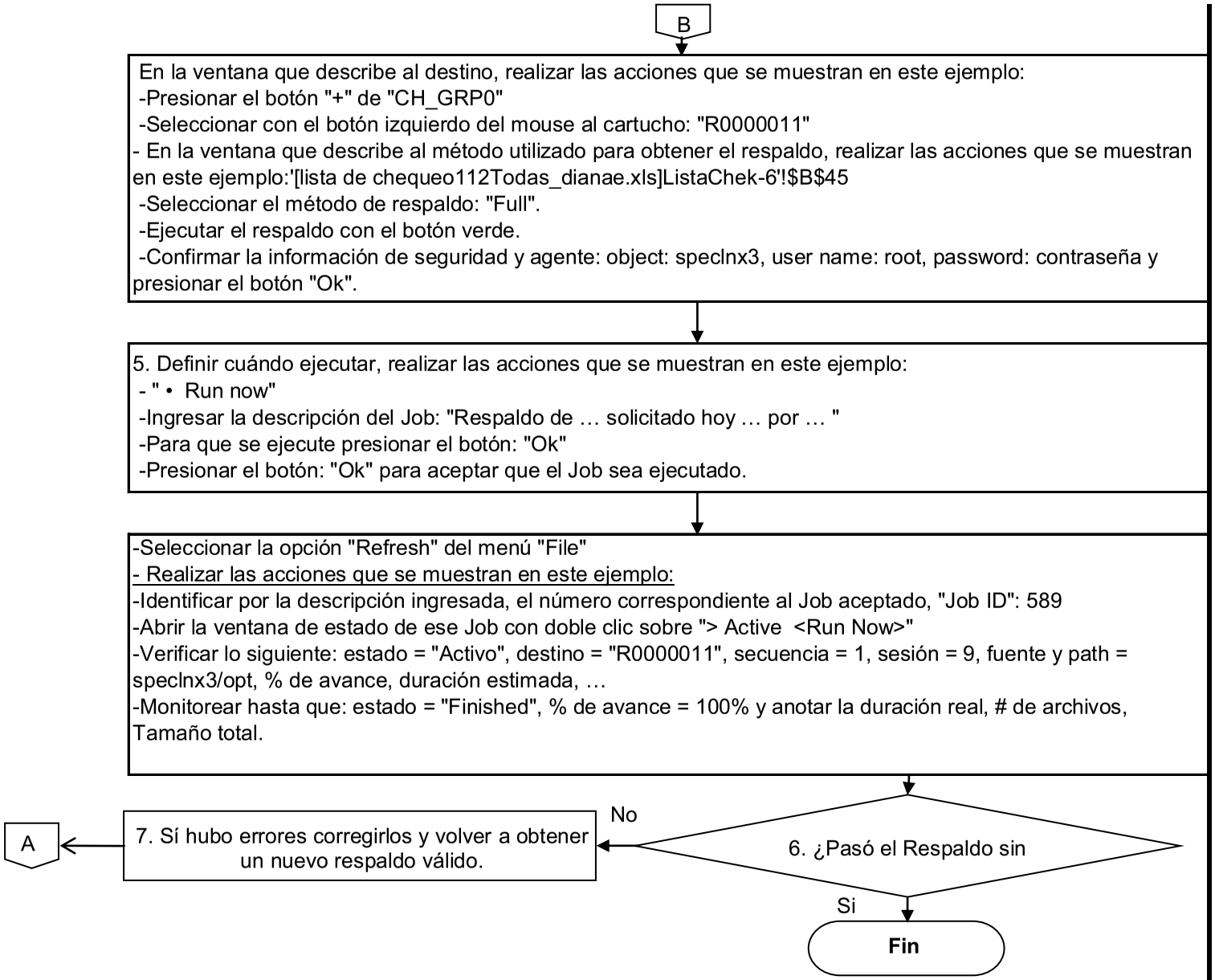


SERVICIO CRÍTICO DE TI:" GESTIÓN DE RESPALDOS."

Diagrama del procedimiento de Respaldos

Doc.1.6.2a




B
En la ventana que describe al destino, realizar las acciones que se muestran en este ejemplo:
-Presionar el botón "+" de "CH_GRP0"
-Seleccionar con el botón izquierdo del mouse al cartucho: "R0000011"
- En la ventana que describe al método utilizado para obtener el respaldo, realizar las acciones que se muestran en este ejemplo:'[lista de chequeo112Todas_dianae.xls]ListaChek-6'!B45
-Seleccionar el método de respaldo: "Full".
-Ejecutar el respaldo con el botón verde.
-Confirmar la información de seguridad y agente: object: speclnx3, user name: root, password: contraseña y presionar el botón "Ok".
5. Definir cuándo ejecutar, realizar las acciones que se muestran en este ejemplo:
- " • Run now"
-Ingresar la descripción del Job: "Respaldo de … solicitado hoy … por … "
-Para que se ejecute presionar el botón: "Ok"
-Presionar el botón: "Ok" para aceptar que el Job sea ejecutado.
-Seleccionar la opción "Refresh" del menú "File"
- Realizar las acciones que se muestran en este ejemplo:
-Identificar por la descripción ingresada, el número correspondiente al Job aceptado, "Job ID": 589
-Abrir la ventana de estado de ese Job con doble clic sobre "> Active <Run Now>"
-Verificar lo siguiente: estado = "Activo", destino = "R0000011", secuencia = 1, sesión = 9, fuente y path = speclnx3/opt, % de avance, duración estimada, …
-Monitorear hasta que: estado = "Finished", % de avance = 100% y anotar la duración real, # de archivos, Tamaño total.
6. ¿Pasó el Respaldo sin
No
7. Sí hubo errores corregirlos y volver a obtener un nuevo respaldo válido.
A
Si
Fin

SERVICIO CRÍTICO DE TI:" GESTIÓN DE RESPALDOS."

Diagrama del procedimiento de Restauración

Doc.1.6.2b

Área usuaria.	Administración de Respaldos

Inicio

1. Solicitar la Restauración de: Información, Aplicaciones y archivos de datos de configuración, conforme a su necesidad.

2. En la estación de Trabajo crear el directorio en el cual se restaurará lo solicitado desde un respaldo obtenido; como se muestra en este ejemplo:
-Ingresar como cliente de Linux, Servidor= "speclnx3", usuario= xyz, pórtico= "22", … y presionar el botón "Conectar", para ingresar la contraseña y Enter.
-Navegar hasta llegar al directorio requerido, ej: "cd /cluster1" y Enter.
-Crear el directorio con mkdir, ej: "mkdir restore2008-08-08".
-Salir del servidor con "Exit".

A

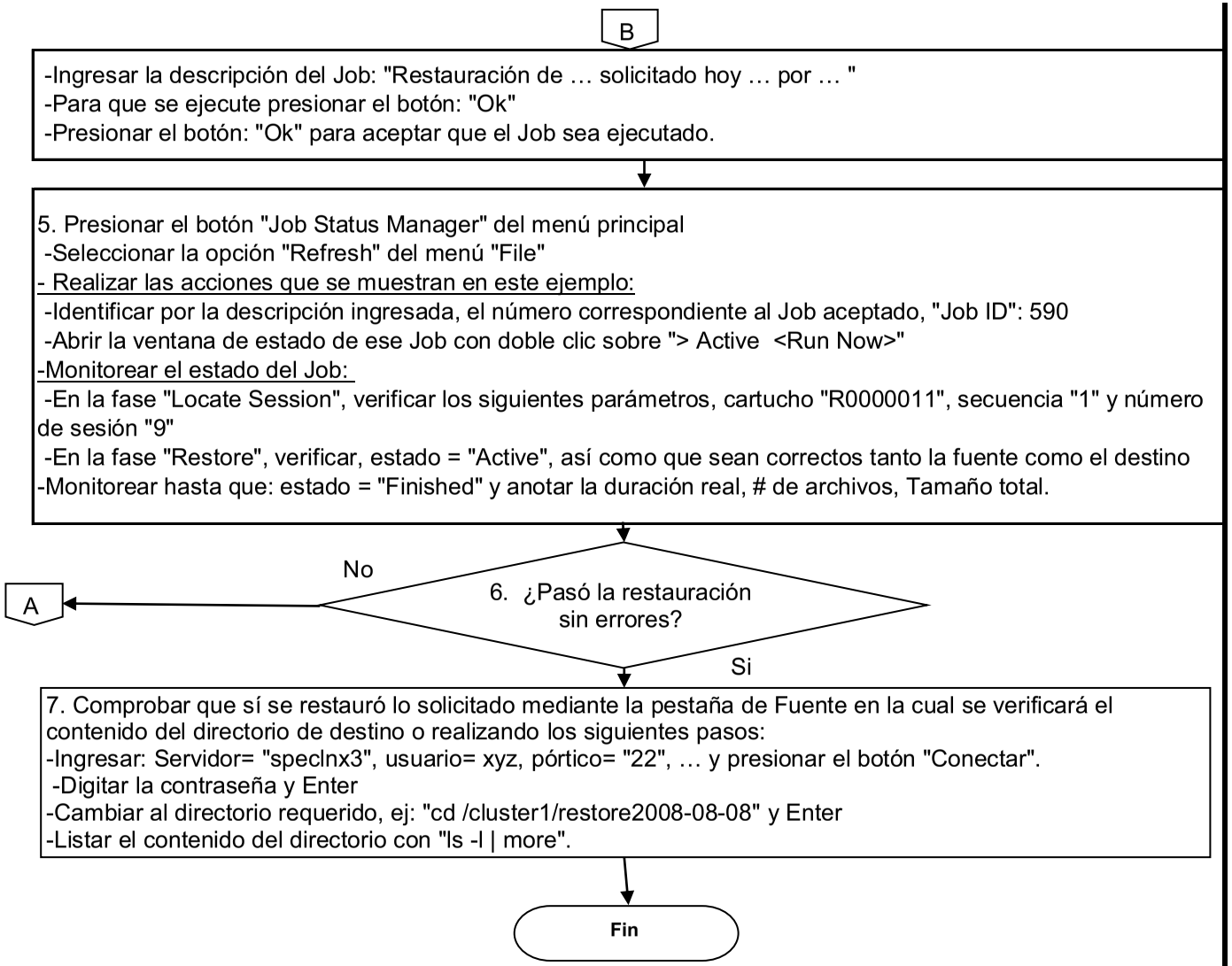
3. En el **CA BrightStor ARCserve Backup**, utilizar la información provista por el usuario y la disponible, referente a, cartucho y sesión, como se muestra en este ejemplo:
- Presionar el botón "Restore Manager" del menú principal
- Seleccionar el Grupo: "Restore By Session"

En la ventana que describe la Fuente desde la cual se restaurará lo solicitado:
-Presionar el botón "+" de "R0000011"
-Presionar el botón "+" de "Session 9 speclnx3: …"
-Navegar hasta marcar con el botón izquierdo del mouse a cada recuadro ubicado a la izquierda de cada uno de los archivos que el usuario solicitó restaurar

En la ventana que describe al Destino sobre el cual se restaurará lo solicitado:
-Presionar el botón "+" de "UNIX/Linux Agents"
-Presionar el botón "+" de "SPECLNX3"
-Ingresar al servidor con usuario = xyz, password = contraseña y presionar "Ok"
-Navegar hasta ubicarse sobre el directorio creado para el efecto: "restore2008-08-08"
-Marcar el directorio "restore2008-08-08" con el botón izquierdo del mouse

4. Ejecutar la restauración con el botón verde.
-Confirmar la información de seguridad y agente: object: speclnx3, user name: root, password: contraseña y presionar el botón "Ok"
-Definir cuándo ejecutar, realizar las acciones que se muestran en este ejemplo:
- " • Run now"

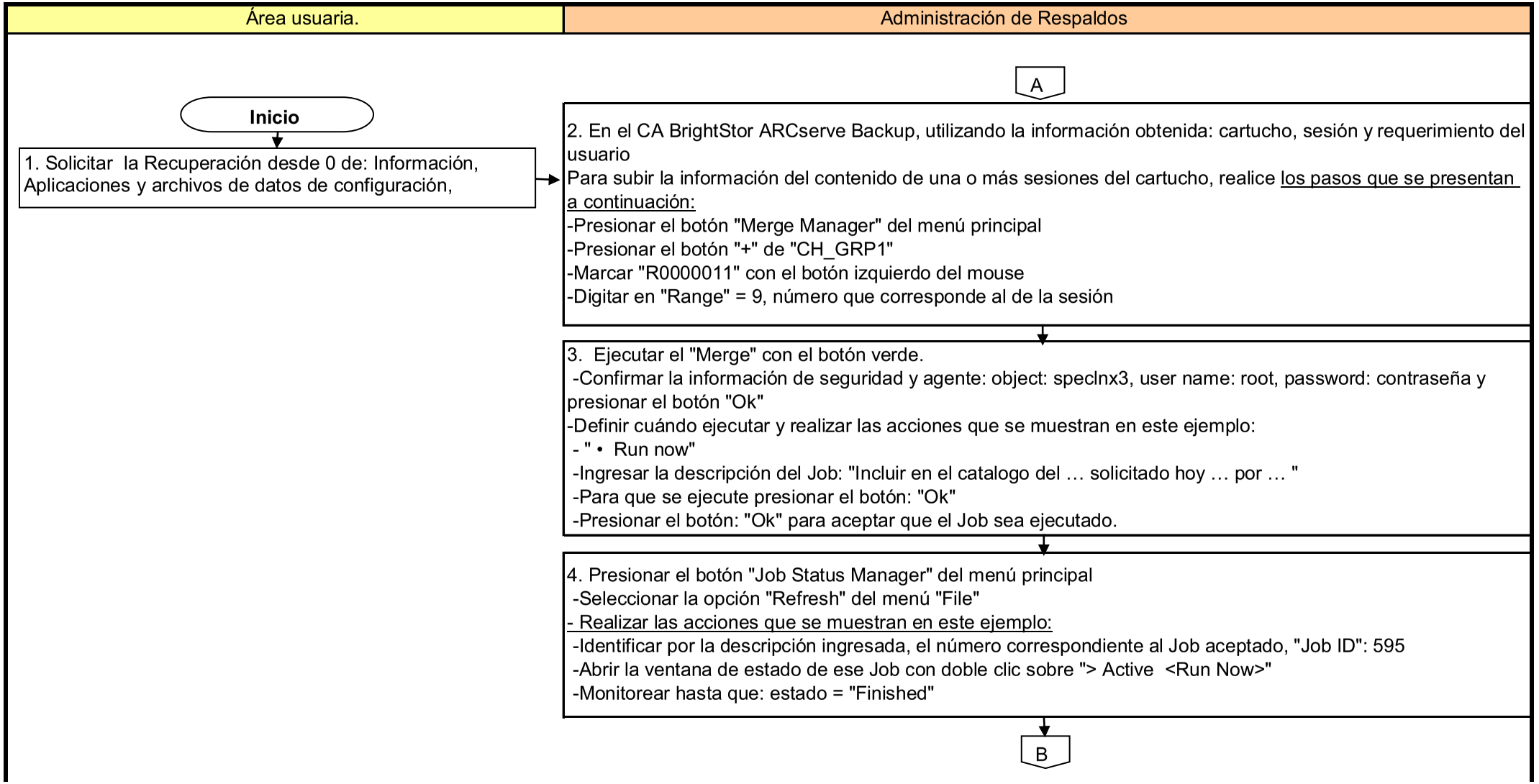
B

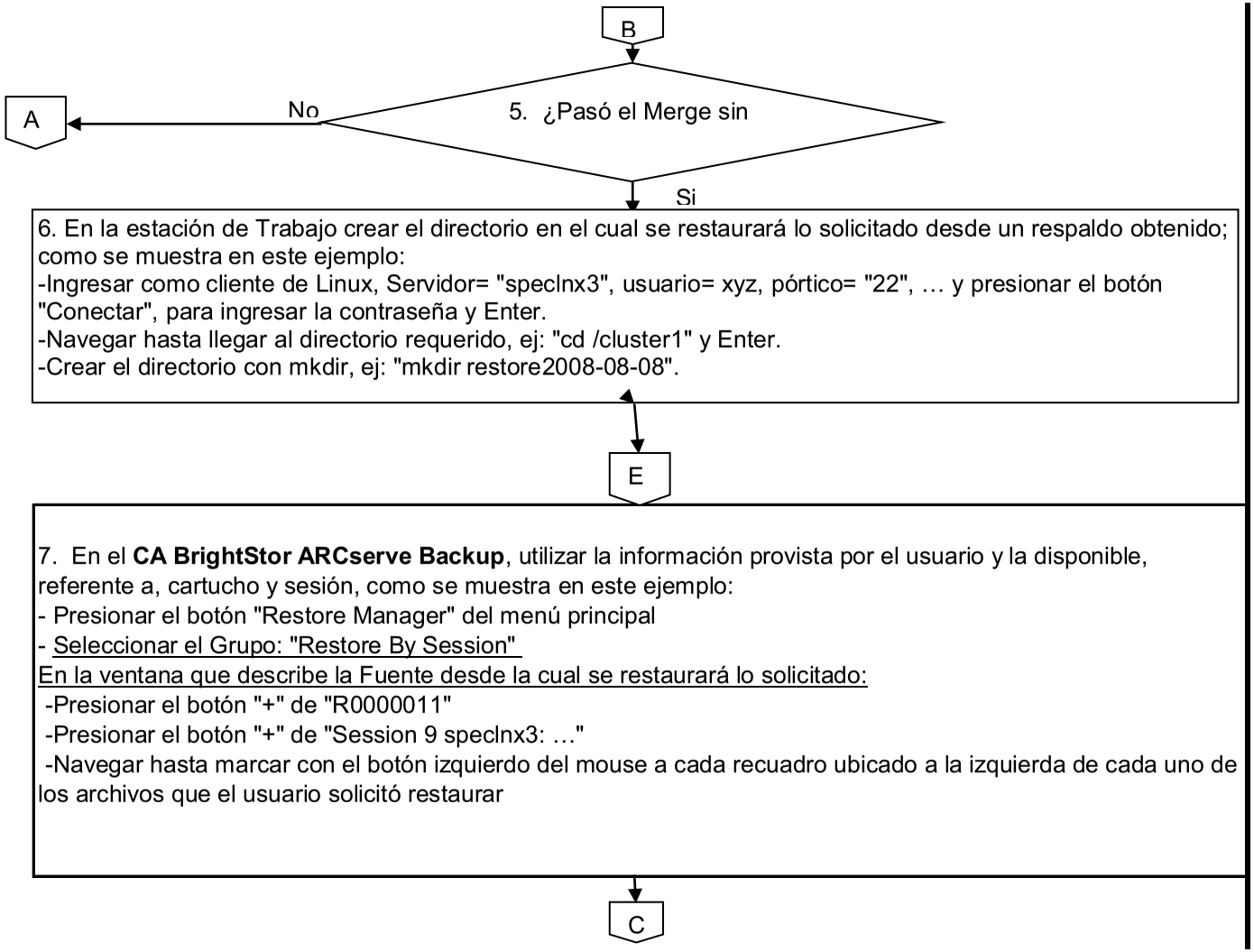

B
-Ingresar la descripción del Job: "Restauración de … solicitado hoy … por … "
-Para que se ejecute presionar el botón: "Ok"
-Presionar el botón: "Ok" para aceptar que el Job sea ejecutado.
5. Presionar el botón "Job Status Manager" del menú principal
-Seleccionar la opción "Refresh" del menú "File"
- Realizar las acciones que se muestran en este ejemplo:
-Identificar por la descripción ingresada, el número correspondiente al Job aceptado, "Job ID": 590
-Abrir la ventana de estado de ese Job con doble clic sobre "> Active <Run Now>"
-Monitorear el estado del Job:
-En la fase "Locate Session", verificar los siguientes parámetros, cartucho "R0000011", secuencia "1" y número de sesión "9"
-En la fase "Restore", verificar, estado = "Active", así como que sean correctos tanto la fuente como el destino
-Monitorear hasta que: estado = "Finished" y anotar la duración real, # de archivos, Tamaño total.
No
A
6. ¿Pasó la restauración sin errores?
Si
7. Comprobar que sí se restauró lo solicitado mediante la pestaña de Fuente en la cual se verificará el contenido del directorio de destino o realizando los siguientes pasos:
-Ingresar: Servidor= "speclnx3", usuario= xyz, pórtico= "22", … y presionar el botón "Conectar".
-Digitar la contraseña y Enter
-Cambiar al directorio requerido, ej: "cd /cluster1/restore2008-08-08" y Enter
-Listar el contenido del directorio con "ls -l | more".
Fin

SERVICIO CRÍTICO DE TI:" GESTIÓN DE RESPALDOS."

Diagrama del procedimiento de Recuperación

Doc.1.6.3




B
A
No
5. ¿Pasó el Merge sin
Si
6. En la estación de Trabajo crear el directorio en el cual se restaurará lo solicitado desde un respaldo obtenido; como se muestra en este ejemplo:
-Ingresar como cliente de Linux, Servidor= "speclnx3", usuario= xyz, pórtico= "22", … y presionar el botón "Conectar", para ingresar la contraseña y Enter.
-Navegar hasta llegar al directorio requerido, ej: "cd /cluster1" y Enter.
-Crear el directorio con mkdir, ej: "mkdir restore2008-08-08".
E
7. En el CA BrightStor ARCserve Backup, utilizar la información provista por el usuario y la disponible, referente a, cartucho y sesión, como se muestra en este ejemplo:
- Presionar el botón "Restore Manager" del menú principal
- Seleccionar el Grupo: "Restore By Session"
En la ventana que describe la Fuente desde la cual se restaurará lo solicitado:
-Presionar el botón "+" de "R0000011"
-Presionar el botón "+" de "Session 9 speclnx3: …"
-Navegar hasta marcar con el botón izquierdo del mouse a cada recuadro ubicado a la izquierda de cada uno de los archivos que el usuario solicitó restaurar
C

C

En la ventana que describe al Destino sobre el cual se restaurará lo solicitado:
-Presionar el botón "+" de "UNIX/Linux Agents"
-Presionar el botón "+" de "SPECLNX3"
-Ingresar al servidor con usuario = xyz, password = contraseña y presionar "Ok"
-Navegar hasta ubicarse sobre el directorio creado para el efecto: "restore2008-08-08"
-Marcar el directorio "restore2008-08-08" con el botón izquierdo del mouse
8. Ejecutar la restauración con el botón verde.
-Confirmar la información de seguridad y agente: object: speclnx3, user name: root, password: contraseña y presionar el botón "Ok"
-Definir cuándo ejecutar, realizar las acciones que se muestran en este ejemplo:
- " • Run now"

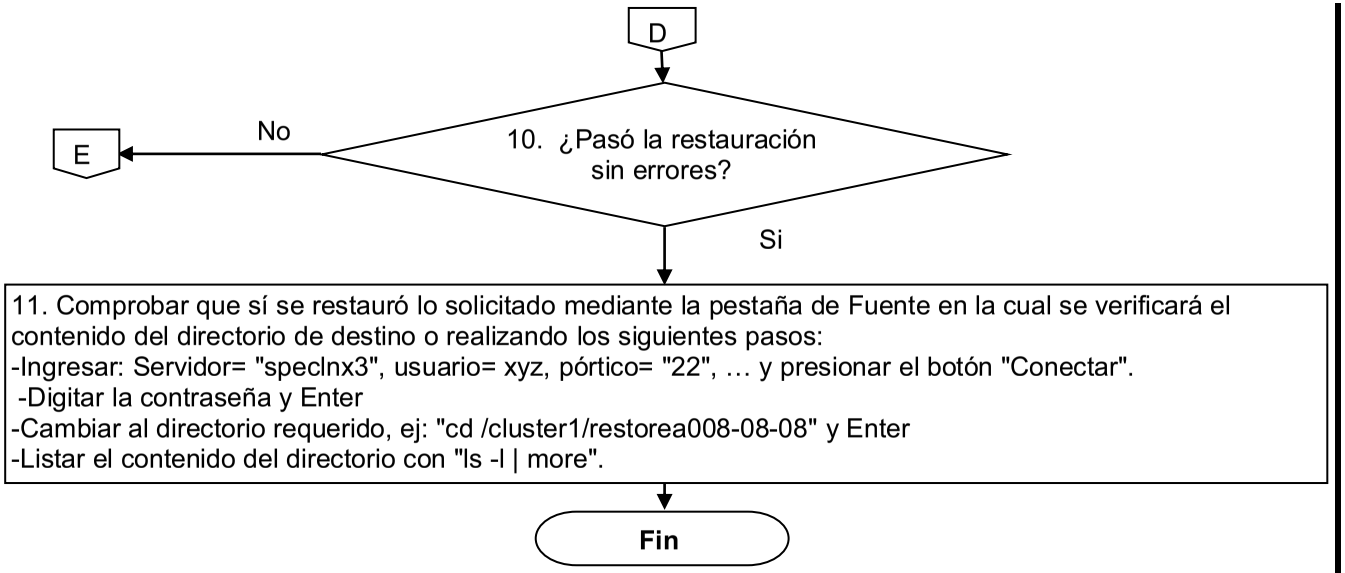
▼

-Ingresar la descripción del Job: "Restauración de … solicitado hoy … por … "
-Para que se ejecute presionar el botón: "Ok"
-Presionar el botón: "Ok" para aceptar que el Job sea ejecutado.

▼

9. Presionar el botón "Job Status Manager" del menú principal
-Seleccionar la opción "Refresh" del menú "File"
- Realizar las acciones que se muestran en este ejemplo:
-Identificar por la descripción ingresada, el número correspondiente al Job aceptado, "Job ID": 590
-Abrir la ventana de estado de ese Job con doble clic sobre "> Active <Run Now>"
-Monitorear el estado del Job:
-En la fase "Locate Session", verificar los siguientes parámetros, cartucho "R0000011", secuencia "1" y número de sesión "9"
-En la fase "Restore", verificar, estado = "Active", así como que sean correctos tanto la fuente como el destino
-Monitorear hasta que: estado = "Finished" y anotar la duración real, # de archivos, Tamaño total.

D


D
10. ¿Pasó la restauración sin errores?
No
E
Si
11. Comprobar que sí se restauró lo solicitado mediante la pestaña de Fuente en la cual se verificará el contenido del directorio de destino o realizando los siguientes pasos:
-Ingresar: Servidor= "speclnx3", usuario= xyz, pórtico= "22", … y presionar el botón "Conectar".
-Digitar la contraseña y Enter
-Cambiar al directorio requerido, ej: "cd /cluster1/restorea008-08-08" y Enter
-Listar el contenido del directorio con "ls -l | more".
Fin

SERVICIO CRÍTICO: "GESTIÓN DE RESPALDOS"
Lista de Chequeo

Fecha y hora de inicio:2008-06-24 y 17h00 Fecha y hora de finalización:2008-06-24 y 19h00 **Doc.1.6.4**

No	Procedimientos y pasos	Parámetros a controlar, comparar y evaluar.		Cumplió			Observaciones
		Parámetro	Valor	Si	Par	No	
	Doc.1.6.2a Diagrama del procedimiento de Respaldos						
1	1.Solicitar la inclusión y obtención de respaldos de: Información, Aplicaciones y archivos de datos de configuraciones, de acuerdo a la Política de Respaldo TI.						
2	2. Registrar en la lista de chequeo la hora de inicio y resultados de cada acción. Verificar si todo lo solicitado: Información, Aplicaciones y archivos de datos de configuración, autorizada por el Jefe de TI constan en el respaldo. Aplicar la Política de Respaldo: Diario, Semanal, Mensual, Anual y/o Especial.						
3	3. Ingresar a CA BrightStor ARCserve Backup con: "http://speclnx9:6060/" Digitar en, dominio: petroecuador, usuario: caroot, contraseña: xyz y presionar "Ok" Seleccionar el Host de default: speclnx9.petroecuador.com.ec y presionar "Ok" Para ver que cartucho está cargado en la unidad de cinta uno: Presionar el botón "Device Manager" del menú principal Presionar el botón "+" de "Adapter 1" Presionar el botón "+" de "IBM Ultrium- TD4" para ver que cartucho está cargado: " "R0000011". Cerrar "Device Manager".						
4	4.Presionar el botón "Backup Manager" del menú principal Presionar el botón "+" de "UNIX/Linux Agents" para ingresar al servidor desde el que se obtendrá el respaldo. Presionar el botón "+" del respectivo servidor SPECLNX3 Ingresar en, usuario: root, contraseña: xyz y presionar "Ok" En la ventana que describe a la fuente, realizar las acciones que se muestran en este ejemplo: Presionar el botón "+" /opt Navegar dentro del servidor para seleccionar con el botón izquierdo del mouse a todos los archivos de los cuales hay que obtener el respaldo solicitado: califica.gdb, califica1.gdb, califica2.gdb y califica3.gdb, presionando sobre el cuadrado ubicado a la derecha del botón "+" En la ventana que describe al destino, realizar las acciones que se muestran en este ejemplo: Presionar el botón "+" de "CH_GRP0" Seleccionar con el botón izquierdo del mouse al cartucho: "R0000011" En la ventana que describe al método utilizado para obtener el respaldo, realizar las acciones que se muestran en este ejemplo: Seleccionar el método de respaldo: "Full". Ejecutar el respaldo con el botón verde. Confirmar la información de seguridad y agente: object: speclnx3, user name: root, password: contraseña y presionar el botón "Ok". Definir cuándo ejecutar, realizar las acciones que se muestran en este ejemplo:						

	" • Run now" Ingresar la descripción del Job: "Respaldo de … solicitado hoy … por … " Para que se ejecute presionar el botón: "Ok" Presionar el botón: "Ok" para aceptar que el Job sea ejecutado.						
5	5. Presionar el botón "Job Status Manager" del menú principal Seleccionar la opción "Refresh" del menú "File" Realizar las acciones que se muestran en este ejemplo: Identificar por la descripción ingresada, el número correspondiente al Job aceptado, Job ID: 589 Abrir la ventana de estado de ese Job con doble clic sobre "> Active <Run Now>" Verificar lo siguiente: estado = "Activo", destino = "R0000011", secuencia = 1, sesión = 9, fuente y path = speclnx3/opt, % de avance, duración estimada, … Monitorear hasta que: estado = "Finished", % de avance = 100% y anotar la duración real, # de archivos, Tamaño total.						
6	6. ¿Pasó el Respaldo sin error?						
7	No.7.Si hubo errores corregirlos y volver a obtener un nuevo respaldo válido.						
8	Si. Fin.						
	Doc.1.6.2b Diagrama del procedimiento de Restauración						
9	1. Solicitar la Restauración de: Información, Aplicaciones y archivos de datos configuración, conforme a su necesidad.						
10	2. En la estación de Trabajo crear el directorio en el cual se restaurará lo solicitado desde un respaldo obtenido; como se muestra en este ejemplo: Ingresar como cliente de Linux, Servidor= "speclnx3", usuario= xyz, pórtico= "22", … y presionar el botón "Conectar", para ingresar la contraseña y Enter. Navegar hasta llegar al directorio requerido, ej: "cd /cluster1" y Enter. Crear el directorio con mkdir, ej: "mkdir restore2008-08-08". Salir del servidor con "Exit".						
11	3. En el CA BrightStor ARCserve Backup, utilizar la información provista por el usuario y la disponible, referente a, cartucho y sesión, como se muestra en este ejemplo: Presionar el botón "Restore Manager" del menú principal Seleccionar el Grupo: "Restore By Session" En la ventana que describe la Fuente desde la cual se restaurará lo solicitado: Presionar el botón "+" de "R0000011" Presionar el botón "+" de "Session 9 speclnx3: …" Navegar hasta marcar con el botón izquierdo del mouse a cada recuadro ubicado a la izquierda de cada uno de los archivos que el usuario solicitó restaurar En la ventana que describe al Destino sobre el cual se restaurará lo solicitado: Presionar el botón "+" de "UNIX/Linux Agents" Presionar el botón "+" de "SPECLNX3" Ingresar al servidor con usuario = xyz, password = contraseña y presionar "Ok" Navegar hasta ubicarse sobre el directorio creado para el efecto: "restore2008-08-08" Marcar el directorio "restore2008-08-08" con el botón izquierdo del mouse						

12	4. Ejecutar la restauración con el botón verde. Confirmar la información de seguridad y agente: object: speclnx3, user name: root, password: contraseña y presionar el botón "Ok" Definir cuándo ejecutar, realizar las acciones que se muestran en este ejemplo: " • Run now" Ingresar la descripción del Job: "Restauración de … solicitado hoy … por … " Para que se ejecute presionar el botón: "Ok" Presionar el botón: "Ok" para aceptar que el Job sea ejecutado. Listar el contenido del directorio con "ls -l | more" para verificar que sí se restauró						
13	5. Presionar el botón "Job Status Manager" del menú principal Seleccionar la opción "Refresh" del menú "File" Realizar las acciones que se muestran en este ejemplo: Identificar por la descripción ingresada, el número correspondiente al Job aceptado, "Job ID": 590 Abrir la ventana de estado de ese Job con doble clic sobre "> Active <Run Now>" Monitorear el estado del Job: En la fase "Locate Session", verificar los siguientes parámetros, cartucho R0000011, secuencia "1" y número de sesión "9" En la fase "Restore", verificar, estado = "Active", así como que sean correctos tanto la fuente como el destino Monitorear hasta que: estado = "Finished" y anotar la duración real, # de archivos, Tamaño total.						
14	6.¿Pasò la restauraciòn sin errores?						
15	No. Continuar con el paso 3.						
16	Si. 6. Comprobar que sí se restauró lo solicitado mediante la pestaña de Fuente en la cual se verificará el contenido del directorio de destino o realizando los siguientes pasos: Ingresar: Servidor= "speclnx3", usuario= xyz, pórtico= "22", … y presionar el botón "Conectar". Digitar la contraseña y Enter Cambiar al directorio requerido, ej: "cd /cluster1/restore2008-08-08" y Enter Listar el contenido del directorio con "ls -l | more".						
	Doc.1.6.3 Diagrama del procedimiento de Recuperación						
17	1. Solicitar la Recuperación desde 0 de: Información, Aplicaciones y archivos de datos de configuración, conforme a su necesidad.			si			
18	2. En el CA BrightStor ARCserve Backup, utilizando la información obtenida: cartucho, cartucho, sesión y requerimiento del usuario Para subir la información del contenido de una o más sesiones del cartucho, realice los pasos que se presentan a continuación: Presionar el botón "Merge Manager" del menú principal Presionar el botón "+" de "CH_GRP1" Marcar "R0000011" con el botón izquierdo del mouse Digitar en "Range" = 9, número que corresponde al de la sesión			si			
19	3. Ejecutar el "Merge" con el botón verde. Confirmar la información de seguridad y agente: object: speclnx3, user name: root, password: contraseña y presionar el botón "Ok".						

	Definir cuándo ejecutar y realizar las acciones que se muestran en este ejemplo: " • Run now" Ingresar la descripción del Job: "Incluir en el catalogo del … solicitado hoy … por …" Para que se ejecute presionar el botón: "Ok" Presionar el botón: "Ok" para aceptar que el Job sea ejecutado.			si			
20	4. Presionar el botón "Job Status Manager" del menú principal Seleccionar la opción "Refresh" del menú "File" Realizar las acciones que se muestran en este ejemplo: Identificar por la descripción ingresada, el número correspondiente al Job aceptado, "Job ID": 595 Abrir la ventana de estado de ese Job con doble clic sobre "> Active <Run Now>" Monitorear hasta que: estado = "Finished"			si			
21	5.¿Pasò el merge sin errores?			si			
22	No. Continuar con el paso 2.						
23	Si. 6. En la estación de Trabajo crear el directorio en el cual se restaurará lo solicitado desde un respaldo obtenido; como se muestra en este ejemplo: Ingresar como cliente de Linux, Servidor= "speclnx3", usuario= xyz, pórtico= "22", … y presionar el botón "Conectar", para ingresar la contraseña y Enter. Navegar hasta llegar al directorio requerido, ej: "cd /cluster1" y Enter. Crear el directorio con mkdir, ej: "mkdir restore2008-08-08". Salir del servidor con "Exit".			si			
24	7. En el CA BrightStor ARCserve Backup, utilizar la información provista por el usuario y la disponible, referente a, cartucho y sesión, como se muestra en este ejemplo: Presionar el botón "Restore Manager" del menú principal Seleccionar el Grupo: "Restore By Session" En la ventana que describe la Fuente desde la cual se restaurará lo solicitado: Presionar el botón "+" de "R0000011" Presionar el botón "+" de "Session 9 speclnx3: …" Navegar hasta marcar con el botón izquierdo del mouse a cada recuadro ubicado a la izquierda de cada uno de los archivos que el usuario solicitó restaurar			si			
25	8. En la ventana que describe al Destino sobre el cual se restaurará lo solicitado: Presionar el botón "+" de "UNIX/Linux Agents" Presionar el botón "+" de "SPECLNX3" Ingresar al servidor con usuario = xyz, password = contraseña y presionar "Ok" Navegar hasta ubicarse sobre el directorio creado para el efecto: "restore2008-08-08" Marcar el directorio "restore2008-08-08" con el botón izquierdo del mouse			si			
26	9. Ejecutar la restauración con el botón verde. Confirmar la información de seguridad y agente: object: speclnx3, user name: root, password: contraseña y presionar el botón "Ok" Definir cuándo ejecutar, realizar las acciones que se muestran en este ejemplo: " • Run now" Ingresar la descripción del Job: "Restauración de … solicitado hoy … por … " Para que se ejecute presionar el botón: "Ok" Presionar el botón: "Ok" para aceptar que el Job sea ejecutado.			si			

27	10. Presionar el botón "Job Status Manager" del menú principal Seleccionar la opción "Refresh" del menú "File" Realizar las acciones que se muestran en este ejemplo: Identificar por la descripción ingresada, el número correspondiente al Job aceptado, "Job ID": 590 Abrir la ventana de estado de ese Job con doble clic sobre "> Active <Run Now>" Monitorear el estado del Job: En la fase "Locate Session", verificar los siguientes parámetros, cartucho "R0000011", secuencia "1" y número de sesión "9" En la fase "Restore", verificar, estado = "Active", así como que sean correctos tanto la fuente como el destino Monitorear hasta que: estado = "Finished" y anotar la duración real, # de archivos, Tamaño total.			si			
28	11.¿pasò la restauraciòn sin errores?						
29	No. Continuar con el paso 7.						
30	Si.12. Comprobar que sí se restauró lo solicitado mediante la pestaña de Fuente en la cual se verificará el contenido del directorio de destino o realizando los siguientes pasos: Ingresar: Servidor= "speclnx3", usuario= xyz, pórtico= "22", … y presionar el botón "Conectar". Digitar la contraseña y Enter Cambiar al directorio requerido, ej.: "Cd /cluster1/restorea008-08-08" y Enter Listar el contenido del directorio con "ls -l | more".			si			

Nivel de satisfacción del cliente :	Total: Si	Parcial:	Insatisfecho:

Por el Técnico encargado de rehabilitar el Servicio:

Firma: _____
Nombre: _____
No. Rol o Cédula de Ciudadanía: _____

Por el Responsable del Servicio:

_____
_____
_____

SERVICIO CRÍTICO "GESTIÓN DE RESPALDOS"

Fecha: 2008-06-24 **Acta de Entrega Recepción de Retorno a la Normalidad del Servicio Crítico de TI** **Doc.1.6.5**

Matriz, Filial o Distrito: PETROECUADOR y Unidad: Sistemas

En la ciudad de Quito se suscribe la presente Acta entre el Técnico que rehabilitó este Servicio y el Responsable del mismo, acta contenida en las siguientes cláusulas:

PRIMERA: OBJETIVO

Mantener la Continuidad del Servicio que apalanca a la Gestión Institucional y en caso de emergencia rehabilitarlo conforme a lo establecido en el Acuerdo de Nivel de Servicio.

SEGUNDA: ESCENARIOS DEL SERVICIO

2.1 Estado previo a la emergencia

Emergencia	Se llenó el espacio del disco asignado a la base de datos de Respaldos y no se podía sacar más respaldos.
Diagnóstico	1. Asignar más espacio a la base de datos de respaldo e inicializarla para poder utilizarla nuevamente.

2.2 Estado del Servicio durante la emergencia

Solución	1. Liberar espacio de disco. 2. Asignar espacio a la Base de Datos. 3. Empezar a llenarla nuevamente.

2.3 Estado luego de la emergencia

Normalidad	Utilizar el Servicio de Respaldo y si se requiere recuperar archivos, primero debe cargarlos a la Base con la opción MERGE.

TERCERA: DERECHOS Y OBLIGACIONES

3.1 El Responsable del Servicio comprobó que el Servicio está 100% operativo.

3.2 El Técnico alertó al Responsable de este Servicio sobre las características de crecimiento, novedades que se han encontrado y conveniencia del mantenimiento preventivo.

3.3 El funcionario que debido a cualquier causa se separe de la Unidad de Sistemas, como paso previo a la obtención de su liquidación, procederá a capacitar y entregar a otros funcionarios los procedimientos de Continuidad de los Servicios y otros que estuvieron a su cargo.

CUARTA: ALCANCE

Lograr la Continuidad del Servicio que se encontraba en estado de emergencia, aplicando los procedimientos disponibles y/o otros que se requirieron para este fin.

QUINTA: ACEPTACION DE LOS FUNCIONARIOS, PARA QUE PETROECUADOR PUEDA EXIGIR Y DEMANDAR EL CUMPLIMIENTO DE SUS RESPONSABILIDADES

5.1 Aceptar y asumir todas las responsabilidades pertenecientes a la aplicación de procedimientos de Respaldo, Restauración, Recuperación y/ otros tendientes a rehabilitar la Continuidad de este Servicio, así como, de controles y actualización de la documentación respectiva, que también es útil para efectos de auditoría, lo cual incluye la incorporación de los cambios efectuados a la documentación existente y de nuevos procedimientos.

5.2 Aceptar que al suscribir esta acta, son administrativa, personal y pecuniariamente responsables tanto del estado en el cual retorna a la normalidad el Servicio recibido, como por la validez y la actualización de la documentación de los procedimientos aplicados en este caso.

Para constancia y fe de conformidad con lo actuado, suscriben la presente acta en original y tres copias de igual contenido y valor.

ENTREGUÉ CONFORME	**RECIBÍ CONFORME**
Firma y sello:	
Nombre:	
No. Rol. o Céd.Ciud.	

ANEXO 1.7

Interbase (Datos del RCP)

Documentación mínima:

1.7.1 Un diagrama de bloque que incluya la Planificación y Ejecución

1.7.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

1.7.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

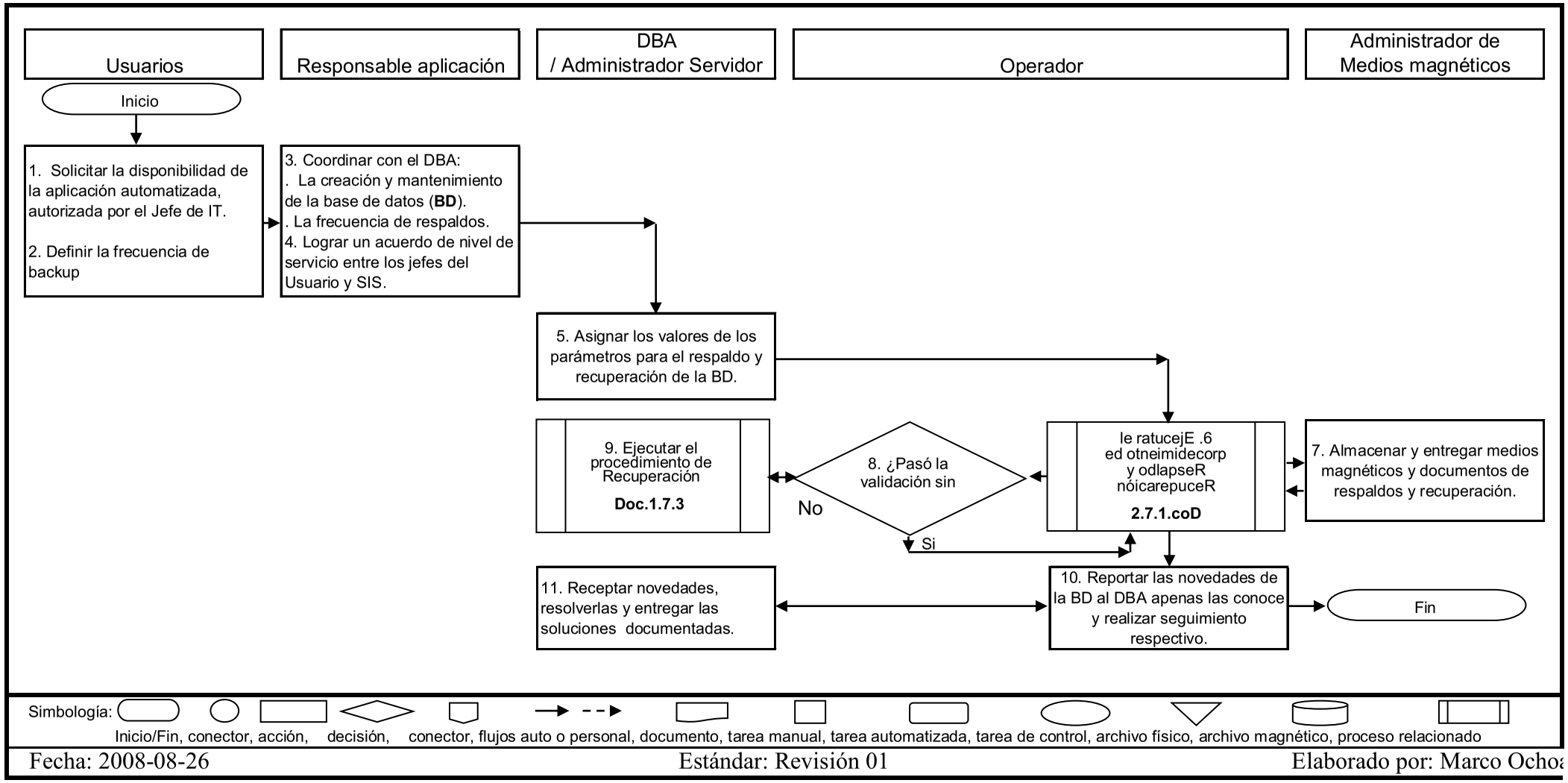
1.7.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

1.7.5 Acta de ER del retorno a la normalidad.

SERVICIO CRÍTICO "INTERBASE (DATOS RCP)"

Diagrama de Bloque

Doc.1.7.1



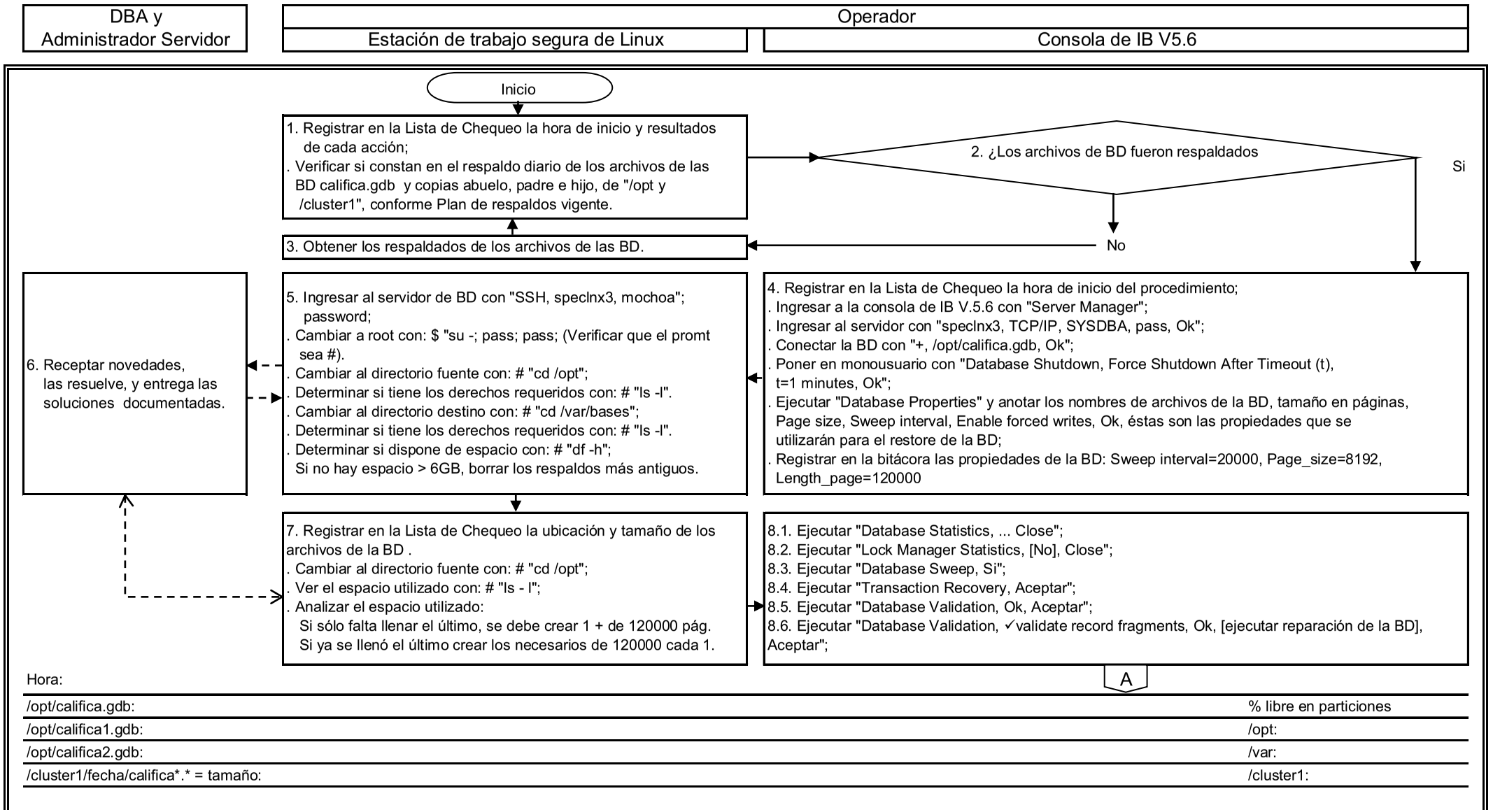
Fecha: 2008-08-26 Estándar: Revisión 01 Elaborado por: Marco Ochoa

SERVICIO CRÍTICO "INTERBASE (DATOS RCP)"

Diagrama del procedimiento de Respaldo y Restauración

Doc.1.7.2

Caso de estudio BD: "/opt/califica.gdb"



6. Receptar novedades, las resuelve, y entrega las soluciones documentadas.

A

No — 9. ¿Pasó la validación sin error?

Si

10. Por seguridad mantener tres respaldos válidos en línea (Abuelo, Padre e Hijo), dentro de /cluster1/*fecha*/ (califica*.* f1.gbk f2.gbk)
. Cambiar al directorio destino con: # "cd /cluster1"; # "mkdir *fecha*";
. Copiar con: # "cp /opt/califica*.* /cluster1/*fecha* ; # "cd *fecha*";
. Verificar copias y tamaños con: # "ls -l";

11. Ejecutar el respaldo en múltiple archivo con: # "cd /usr/local/interbase/bin";

Interbase: Desconectar la base de datos /opt/califica.gdb con "Database Disconnect" o "-"
Salir del server con. "-"; Salir del Interbase Manger con: Close;

"ps -aux | grep gds"; (Solo debe estar una conexion: "root ... grep gds";
eliminar las demás con # kill -9 numero-proceso-ej:22174;)
"./gbak -backup /opt/califica.gdb stdout | ./gsplit -split /var/bases/f1.gbk
1500m /var/bases/f2.gbk 1500m /var/bases/f3.gbk 1500m"; # "ls -l /var/bases";
Copiar tamaño de archivos:
f1.gbk:_____
f2.gbk:_____
f3.gbk:_____

Ejecutar el procedimiento de Recuperación **Doc.1.7.3**

No — 12. ¿Pasó el respaldo sin error?

Si

6. Receptar novedades, las resuelve, y entrega las soluciones documentadas.

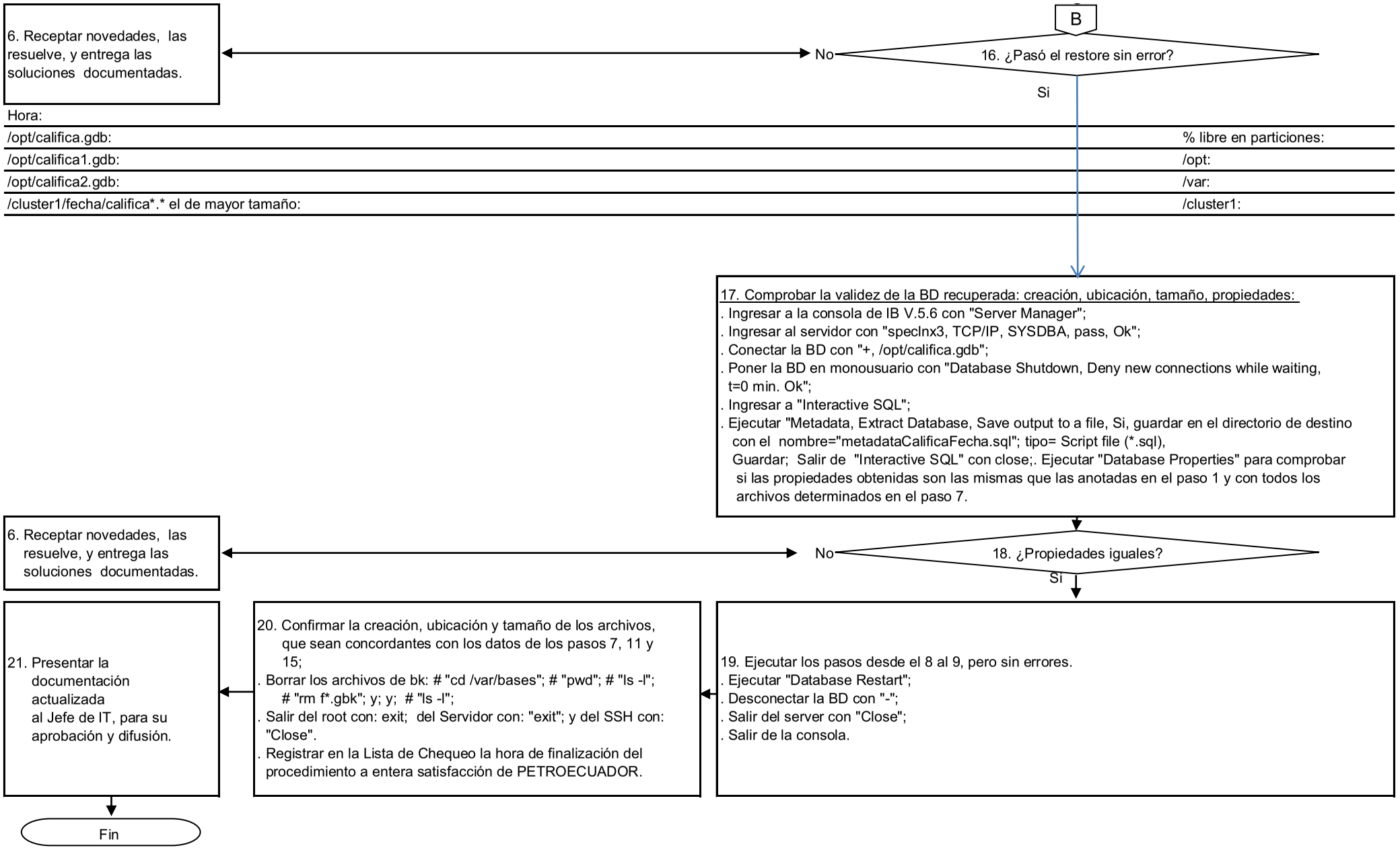
13. Por seguridad completar los tres respaldos válidos en línea:
. Cambiar al directorio de destino con: # "cd /cluster1/*fecha* ;
. Copiar con: # "cp /var/bases/f*.gbk /cluster1/*fecha* ;
. Verificar copias y tamaños con: # ls -l;

¡ Mucho cuidado !
Atención: Si se hubiera renombrado con el sufijo "old" a todos los archivos de la BD respaldada, Al conectar la BD calificaold.gdb, ésta direccionará a califica1y2.gdb mas no los califica1old.gdb y califica2old.gdb

14. Verificar en la Lista de Chequeo las propiedades con las que se restaura de la BD, que deben ser las mismas de la respaldada: Page_size: 120000 y Length_page: 8192.

15. Ejecutar el Restore con múltiples archivos de respaldo y de base de datos, que aseguren el 100% de la ejecución de dichas acciones, con:
"cd /usr/local/interbase/bin";
"ps -aux | grep gds"; (Solo debe estar una conexion: "root ... grep gds"; eliminar las demás con # kill -9 numero-proceso-ej:22174;)
"./gsplit -join /var/bases/f1.gbk /var/bases/f2.gbk /var/bases/f3.gbk | ./gbak -replace_database -page_size 8192 stdin /opt/califica.gdb 120000 /opt/califica1.gdb 120000 /opt/califica2.gdb 120000 /opt/califica3.gdb 120000";
. Verificar copias y tamaños con: # ls -l /opt;

B



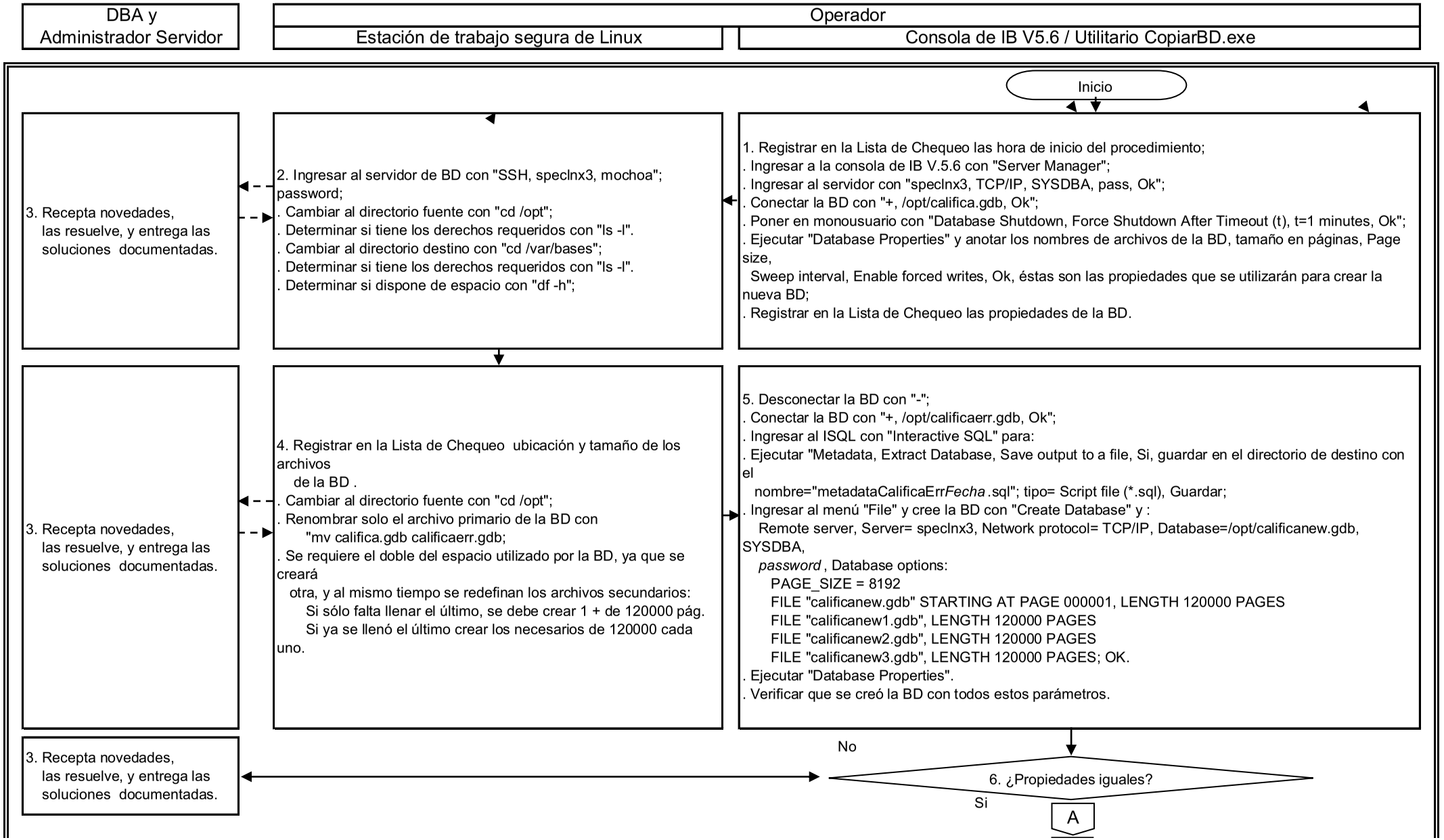
Fecha: 2008-08-26 Estándar: Revisión 03 Duración: 25 minutos

SERVICIO CRÍTICO "INTERBASE (DATOS RCP)"

Diagrama del procedimiento de Recuperación

Doc.1.7.3

Caso de estudio BD: "/opt/califica.gdb"



DBA y Administrador Servidor	Operador	
	Estación de trabajo segura de Linux	Consola de IB V5.6 / Utilitario CopiarBD.exe

A

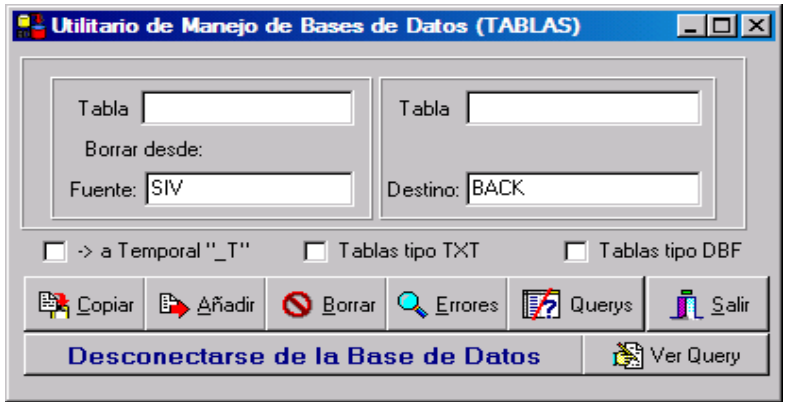
7. Cambiar en el script "metadataCalificaErr*Fecha* .sql" la sentencia "CREATE DATABASE ..." por:
"CONNECT 'specInx3:/opt/calificanew.gdb' USER 'SYSDBA' PASSWORD 'password'; "
. Crear los objetos de la BD en "/opt/calificanew.gdb' con: "Run an ISQL Script" con "metadataCalificaErr*Fecha* .sql" y Save output to a file, Si, guardar en directorio de destino con el nombre=metadataCalificaParte1*Fecha* .txt"; tipo= Results file (*txt), Guardar (parte2 , 3, ...);
. Verificar en el log que todo se haya ejecutado correctamente, si hay errores corregirlos y completar el proceso.
. Ejecutar "Metadata, Extract Database, Save output to a file, Si, guardar en directorio de destino con el nombre=metadataCalificaNew*Fecha* .sql"; tipo= Script file (*.sql), Guardar;
. Comparar entre las metadatas "metadataCalificaErr*Fecha* .sql" y "metadataCalificaNew*Fecha* .sql", para tener la certeza de que se crearon todos los objetos. Si faltan objetos, utilizar cada vez un nuevo escript para crearlos.

O en su lugar sacar un respaldo de "Backup Metadata Only" y el respectivo restore en Calificanew...gdb.

8. ¿Objetos iguales?

No

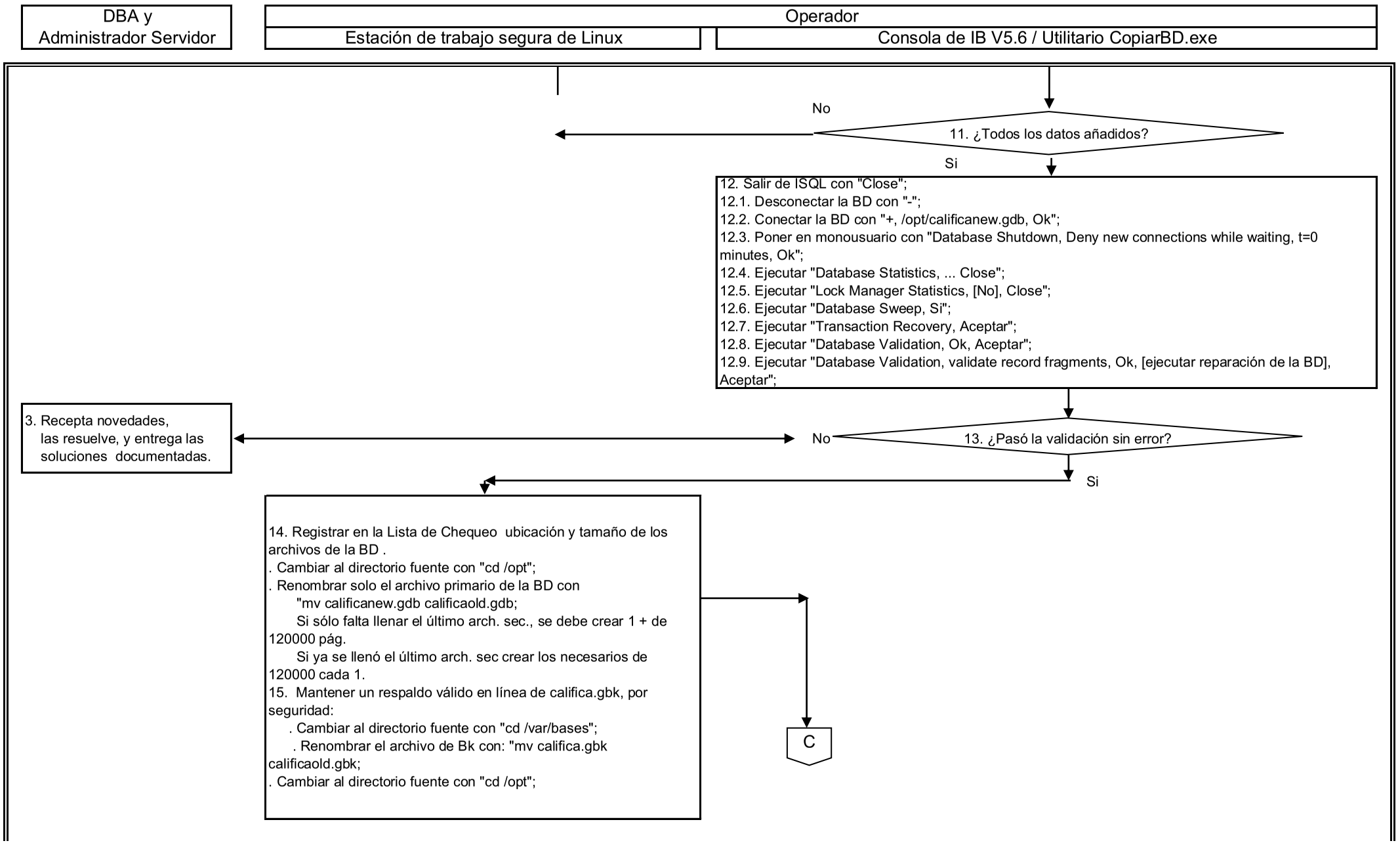
Si



Utilitario: CopiarBD.exe

9. Generar la Lista de todas las tablas con:
"Metadata, Show, Table, Ok";
"File, Save result to a file, en el directorio de destino, con el nombre=CalificaTablas*Fecha* , Guardar";
Editar "CalificaTablas*Fecha* " e imprimir;
Utilizar el "Borland Database Engine (BDE)" u otro para crear y probar los siguientes alias que son requeridos:
Fuente: "SIV" que apunte a la BD "calificaerr.gdb" (u otra BD anterior) y
Destino: "BACK" que apunte a la BD "calificanew.gdb";

10. Ejecutar "CopiarBD.exe" para pasar los datos de las tablas de la BD "calificaerr.gdb" a la "calificanew.gdb":
. Ingresar cada uno de los nombres de las tablas de "CalificaTablasFecha" en el campo denominado "Tabla", luego dar un click en el nombre de la tabla de destino; y otro click en el botón "Añadir". La primera vez pide que se conecte a cada una de las BD. Anotar en la misma lista junto al nombre de cada tabla el número de filas que se han añadido, luego adjuntarla a la Lista de Chequeo.


DBA y Administrador Servidor
Operador
Estación de trabajo segura de Linux
Consola de IB V5.6 / Utilitario CopiarBD.exe
No
11. ¿Todos los datos añadidos?
Si
12. Salir de ISQL con "Close";
12.1. Desconectar la BD con "-";
12.2. Conectar la BD con "+, /opt/calificanew.gdb, Ok";
12.3. Poner en monousuario con "Database Shutdown, Deny new connections while waiting, t=0 minutes, Ok";
12.4. Ejecutar "Database Statistics, ... Close";
12.5. Ejecutar "Lock Manager Statistics, [No], Close";
12.6. Ejecutar "Database Sweep, Si";
12.7. Ejecutar "Transaction Recovery, Aceptar";
12.8. Ejecutar "Database Validation, Ok, Aceptar";
12.9. Ejecutar "Database Validation, validate record fragments, Ok, [ejecutar reparación de la BD], Aceptar";
3. Recepta novedades, las resuelve, y entrega las soluciones documentadas.
No
13. ¿Pasó la validación sin error?
Si
14. Registrar en la Lista de Chequeo ubicación y tamaño de los archivos de la BD .
. Cambiar al directorio fuente con "cd /opt";
. Renombrar solo el archivo primario de la BD con
"mv calificanew.gdb calificaold.gdb;
Si sólo falta llenar el último arch. sec., se debe crear 1 + de 120000 pág.
Si ya se llenó el último arch. sec crear los necesarios de 120000 cada 1.
15. Mantener un respaldo válido en línea de califica.gbk, por seguridad:
. Cambiar al directorio fuente con "cd /var/bases";
. Renombrar el archivo de Bk con: "mv califica.gbk calificaold.gbk;
. Cambiar al directorio fuente con "cd /opt";
C

Caso de estudio BD: "/opt/califica.gdb"

DBA y Administrador Servidor	Operador	
	Estación de trabajo segura de Linux	Consola de IB V5.6 / Utilitario CopiarBD.exe

C

15. Ejecutar el respaldo en múltiple archivo con: # "cd /usr/local/interbase/bin";

Interbase: Desconectar la base de datos /opt/califica.gdb con "Database Disconnect" o "-"
Salir del server con. "-"; Salir del Interbase Manger con: Close;

"ps -aux | grep gds"; (Solo debe estar una conexion: "root ... grep gds";
eliminar las demás con # kill -9 numero-proceso-ej:22174;)
"./gbak -backup /opt/calificaold.gdb stdout | ./gsplit -split /var/bases/f1.gbk
1500m /var/bases/f2.gbk 1500m /var/bases/f3.gbk 1500m"; # "ls -l /var/bases";
Copiar tamaño de archivos:
f1.gbk:_____
f2.gbk:_____
f3.gbk:_____

16. ¿Pasó el respaldo sin error?

No

3. Recepta novedades, las resuelve, y entrega las soluciones documentadas.

Si

17. Para no perder el contenido de los archivos secundarios de la BD que residen en el directorio /opt , se debe renombrarlos, así:
"cd /opt";
"mv calificanew1.gdb califica1old.gdb;
"mv calificanew2.gdb califica2old.gdb; …
Atención: Así se tendrán con el sufijo "old" a todos los archivos de la BD respaldada, pero si conectara la BD calificaold.gdb, ésta direccionará a califica1,2 y 3.gdb mas no los calificanew1old, gdb y calificanew2old.gdb,
¡ Mucho cuidado !
. Registrar en la Lista de Chequeo las propiedades de la BD.

3. Recepta novedades, las resuelve, y entrega las soluciones documentadas.

D

DBA y Administrador Servidor	Operador	
	Estación de trabajo segura de Linux	Consola de IB V5.6 / Utilitario CopiarBD.exe

D

18. Ejecutar el Restore con múltiples archivos de respaldo y de base de datos, que aseguren el 100% de la ejecución de dichas acciones, con:
"cd /usr/local/interbase/bin";
"ps -aux | grep gds"; (Solo debe estar una conexion: "root ... grep gds"; eliminar las demás con # kill -9 numero-proceso-ej:22174;)
"./gsplit -join /var/bases/f1.gbk /var/bases/f2.gbk /var/bases/f3.gbk | ./gbak -replace_database -page_size 8192 stdin /opt/califica.gdb 120000 /opt/califica1.gdb 120000 /opt/califica2.gdb 120000 /opt/califica3.gdb 120000";
. Verificar copias y tamaños con: # ls -l /opt;

19. ¿Pasó el restore sin error?

No → 3. Recepta novedades, las resuelve, y entrega las soluciones documentadas.

Si

20. Desconectar la BD con "-";
. Conectar la BD con "+, /opt/califica.gdb";
. Poner la BD en monousuario con "Database Shutdown, Deny new connections while waiting, t=0 min. Ok";
. Ingresar a "Interactive SQL";
. Ejecutar "Metadata, Extract Database, Save output to a file, Si, guardar en "…\Procedim\IT_P#p_CodiFuen", nombre="metadataCalifica*Fecha*.sql"; tipo= Script file (*.sql), Guardar; Salir de "Interactive SQL" con close;.
. Ejecutar "Database Properties" para comprobar si las propiedades obtenidas son las mismas que las anotadas en el paso 1 y con todos los archivos determinados en el paso 4.

21. ¿Propiedades iguales?

No → 3. Recepta novedades, las resuelve, y entrega las soluciones documentadas.

Si

22. Ejecutar los pasos desde el 12.4 al 13, pero sin errores.
. Ejecutar "Database Restart";
. Desconectar la BD con "-";
. Salir del server con "Close";
. Salir de la consola.

23. Confirmar la creación, ubicación y tamaño de los archivos, que sean concordantes con los datos del paso 4;
. Salir del Servidor con "exit";
. Salir del SSH con "Close".
. Registrar en la Lista de Chequeo la hora de finalización del procedimiento a entera satisfacción de PETROECUADOR.

24. Presenta la documentación actualizada al Jefe de IT, para su aprobación y difusión.

Fin

SERVICIO CRÍTICO "INTERBASE (DATOS RCP)"
Lista de Chequeo

Fecha y hora de inicio:2008-06-03 y 18h00 Fecha y hora de finalización:2008-06-03 y 20h00 **Doc.1.7.4**

No	Procedimientos y pasos	Parámetros a controlar, comparar y evaluar. Parámetro	Valor	Cumplió Si	Par	No	Observaciones
	Doc.1.7.2 Procedimiento de Respaldo y Restauración						
1	1. Registrar en la Lista de Chequeo la hora de inicio y resultados de cada acción; . Verificar si constan en el respaldo diario de los archivos de las BD califica.gdb y copias abuelo, padre e hijo, de "/opt y /cluster1", conforme Plan de respaldos vigente.			Si			
2	2. ¿Los archivos de BD fueron respaldados ayer?			Si			
3	3. Obtener los respaldados de los archivos de las BD.						
4	4. Registrar en la Lista de Chequeo la hora de inicio del procedimiento; . Ingresar a la consola de IB V.5.6 con "Server Manager"; . Ingresar al servidor con "speclnx3, TCP/IP, SYSDBA, pass, Ok"; . Conectar la BD con "+, /opt/califica.gdb, Ok"; . Poner en monousuario con "Database Shutdown, Force Shutdown After Timeout (t), t=1 minutes, Ok"; . Ejecutar "Database Properties" y anotar los nombres de archivos de la BD, tamaño en páginas, Page size, Sweep interval, Enable forced writes, Ok, éstas son las propiedades que se utilizarán para el restore de la BD; . Registrar en la bitácora las propiedades de la BD: Sweep interval=20000, Page_size=8192, Length_page=120000	Sweep interval= Page_size= Length-page=	20000 8192 120000	Si			
5	5. Ingresar al servidor de BD con "SSH, speclnx3, mochoa"; password; . Cambiar a root con: $ "su -; pass; pass; (Verificar que el promt sea #). . Cambiar al directorio fuente con: # "cd /opt"; . Determinar si tiene los derechos requeridos con: # "ls -l". . Cambiar al directorio destino con: # "cd /var/bases"; . Determinar si tiene los derechos requeridos con: # "ls -l". . Determinar si dispone de espacio con: # "df -h"; Si no hay espacio > 6GB, borrar los respaldos más antiguos.			Si			
6	Si fuere el caso que se haya requerido soporte al DBA y/o Administrador del Servidor: Receptar novedades, las resuelve, y entrega las soluciones documentadas; continuar con le paso 5.						
7	7. Registrar en la Lista de Chequeo la ubicación y tamaño de los archivos de la BD . . Cambiar al directorio fuente con: # "cd /opt"; . Ver el espacio utilizado con: # "ls - l"; . Analizar el espacio utilizado: Si sólo falta llenar el último, se debe crear 1 + de 120000 pág. Si ya se llenó el último crear los necesarios de 120000 cada 1.						

8	8.1. Ejecutar "Database Statistics, ... Close"; 8.2. Ejecutar "Lock Manager Statistics, [No], Close"; 8.3. Ejecutar "Database Sweep, Si"; 8.4. Ejecutar "Transaction Recovery, Aceptar"; 8.5. Ejecutar "Database Validation, Ok, Aceptar"; 8.6. Ejecutar "Database Validation, üvalidate record fragments, Ok, [ejecutar reparación de la BD], Aceptar";	Hora: /opt/califica.gdb: /opt/califica1.gdb: /opt/califica2.gdb: /cluster1/fecha/califica*.* = tamaño: % libre en particiones /opt: /var: /cluster1:	18 horas 983048102 bytes 983048102 bytes 1709277184 bytes Bk de igual tamaño 3,7 GB 6,8 GB 24 GB	Si			
9	9. ¿Pasó la validación sin error?						
10	No. 6. Receptar novedades, las resuelve, y entrega las soluciones documentadas. Continuar con el paso 9.						
11	Si. 10. Por seguridad mantener tres respaldos válidos en línea (Abuelo, Padre e Hijo), dentro de /cluster1/fecha/ (califica*.* f1.gbk f2.gbk) . Cambiar al directorio destino con: # "cd /cluster1"; # "mkdir fecha"; . Copiar con: # "cp /opt/califica*.* /cluster1/fecha; # "cd fecha"; . Verificar copias y tamaños con: # "ls -l";	"cp /opt/califica*.* /clu	Igual tamaño	Si			
12	11. Ejecutar en: <u>Interbase:</u> Desconectar la base de datos /opt/califica.gdb con "Database Disconnect" o "-" Salir del server con. "-"; Salir del Interbase Manger con: Close; <u>Linux el respaldo en múltiple archivo con:</u> # "cd /usr/local/interbase/bin"; # "ps -aux | grep gds"; (Solo debe estar una conexion: "root ... grep gds"; eliminar las demás con # kill -9 numero-proceso-ej:22174;) # "./gbak -backup /opt/califica.gdb stdout | ./gsplit -split /var/bases/f1.gbk 1500m /var/bases/f2.gbk 1500m /var/bases/f3.gbk 1500m"; # "ls -l /var/bases"; Copiar tamaño de archivos:	f1.gbk= f2.gbk= f3.gbk=	1572864000 bytes 1572864000 bytes 258244908 bytes				
13	12. ¿Pasó el respaldo sin error?						
14	No. Pedir soporte al DBA y/o Administrador del Servidor. Receptar novedades, las resuelve, y entrega las soluciones documentadas. Continuar con le paso 12.						
15	Si. 13. Por seguridad completar los tres respaldos válidos en línea: . Cambiar al directorio de destino con: # "cd /cluster1/fecha; . Copiar con: # "cp /var/bases/f*.gbk /cluster1/fecha; . Verificar copias y tamaños con: # ls -l; ¡ Mucho cuidado ! Atención: Si se hubiera renombrado con el sufijo "old" a todos los archivos de la BD respaldada, Al conectar la BD calificaold.gdb, ésta direccionará a califica1y2.gdb mas no los califica1old.gdb y califica2old.gdb						
16	14. Verificar en la Lista de Chequeo las propiedades con las que se restaura de la BD, que deben ser las mismas de la respaldada: Page_size: 120000 y Length_page: 8192.	Page_size: Length_page:	120000 8192	Si			

17	15. Ejecutar el Restore con múltiples archivos de respaldo y de base de datos, que aseguren el 100% de la ejecución de dichas acciones, con: # "cd /usr/local/interbase/bin"; # "ps -aux | grep gds"; (Solo debe estar una conexion: "root ... grep gds"; eliminar las demás con # kill -9 numero-proceso-ej:22174;) # "./gsplit -join /var/bases/f1.gbk /var/bases/f2.gbk /var/bases/f3.gbk | ./gbak -replace_database -page_size 8192 stdin /opt/califica.gdb 120000 /opt/califica1.gdb 120000 /opt/califica2.gdb 120000 /opt/califica3.gdb 120000"; . Verificar copias y tamaños con: # ls -l /opt;						
18	16. ¿Pasó el restore sin error?						
19	No. Pedir soporte al DBA y/o Administrador del Servidor. Receptar novedades, las resuelve, y entrega las soluciones documentadas. Continuar con le paso 16.						
20	17. Comprobar la validez de la BD recuperada: creación, ubicación, tamaño, propiedades: . Ingresar a la consola de IB V.5.6 con "Server Manager"; . Ingresar al servidor con "speclnx3, TCP/IP, SYSDBA, pass, Ok"; . Conectar la BD con "+, /opt/califica.gdb"; . Poner la BD en monousuario con "Database Shutdown, Deny new connections while waiting, t=0 min. Ok"; . Ingresar a "Interactive SQL"; . Ejecutar "Metadata, Extract Database, Save output to a file, Si, guardar en el directorio de destino con el nombre="metadataCalificaFecha.sql"; tipo= Script file (*.sql), Guardar; Salir de "Interactive SQL" con close;. Ejecutar "Database Properties" para comprobar si las propiedades obtenidas son las mismas que las anotadas en el paso 1 y con todos los archivos determinados en el paso 7.	Hora: /opt/califica.gdb: /opt/califica1.gdb: /opt/califica2.gdb: /opt/califica3.gdb: /cluster1/fecha/califica*.* = tamaño: % libre en particiones /opt: /var: /cluster1:	18H22 983048102 bytes 983048102 bytes 983048102 bytes 657072128 bytes Bk de igual tamaño 2,8 GB 3,4 GB 12 GB				
21	18. ¿Propiedades iguales?						
22	No. Pedir soporte al DBA y/o Administrador del Servidor. Receptar novedades, las resuelve, y entrega las soluciones documentadas. Continuar con le paso 18.						
23	19. Ejecutar los pasos desde el 8 al 9, pero sin errores. . Ejecutar "Database Restart"; . Desconectar la BD con "-"; . Salir del server con "Close"; . Salir de la consola.						
24	20. Confirmar la creación, ubicación y tamaño de los archivos, que sean concordantes con los datos de los pasos 7, 11 y 15; . Borrar los archivos de bk: # "cd /var/bases"; # "pwd"; # "ls -l"; # "rm f*.gbk"; y; y; # "ls -l"; . Salir del root con: exit; del Servidor con: "exit"; y del SSH con: "Close". . Registrar en la Lista de Chequeo la hora de finalización del procedimiento a entera satisfacción de PETROECUADOR.						

25	21. Presentar la documentación actualizada al Jefe de IT, para su aprobación y difusión.						
26	Fin del Procedimiento.						
	Doc.1.7.3 Procedimiento Recuperación						
27	1. Registrar en la Lista de Chequeo las hora de inicio del procedimiento; . Ingresar a la consola de IB V.5.6 con "Server Manager"; . Ingresar al servidor con "speclnx3, TCP/IP, SYSDBA, pass, Ok"; . Conectar la BD con "+, /opt/califica.gdb, Ok"; . Poner en monousuario con "Database Shutdown, Force Shutdown After Timeout (t), t=1 minutes, Ok"; . Ejecutar "Database Properties" y anotar los nombres de archivos de la BD, tamaño en páginas, Page size, Sweep interval, Enable forced writes, Ok, éstas son las propiedades que se utilizarán para crear la nueva BD; . Registrar en la Lista de Chequeo las propiedades de la BD.						
28	2. Ingresar al servidor de BD con "SSH, speclnx3, mochoa"; password; . Cambiar al directorio fuente con "cd /opt"; . Determinar si tiene los derechos requeridos con "ls -l". . Cambiar al directorio destino con "cd /var/bases"; . Determinar si tiene los derechos requeridos con "ls -l". . Determinar si dispone de espacio con "df -h";						
29	3. Si fuere el caso que se haya requerido soporte al DBA y/o Administrador del Servidor: Receptar novedades, las resuelve, y entrega las soluciones documentadas; continuar con le paso 2.						
30	4. Registrar en la Lista de Chequeo ubicación y tamaño de los archivos de la BD . . Cambiar al directorio fuente con "cd /opt"; . Renombrar solo el archivo primario de la BD con "mv califica.gdb calificaerr.gdb; . Se requiere el doble del espacio utilizado por la BD, ya que se creará otra, y al mismo tiempo se redefinan los archivos secundarios: Si sólo falta llenar el último, se debe crear 1 + de 120000 pág. Si ya se llenó el último crear los necesarios de 120000 cada uno.						

31	5. Desconectar la BD con "-"; . Conectar la BD con "+, /opt/calificaerr.gdb, Ok"; . Ingresar al ISQL con "Interactive SQL" para: . Ejecutar "Metadata, Extract Database, Save output to a file, Si, guardar en el directorio de destino con el nombre="metadataCalificaErrFecha.sql"; tipo= Script file (*.sql), Guardar; . Ingresar al menú "File" y cree la BD con "Create Database" y : Remote server, Server= specInx3, Network protocol= TCP/IP, Database=/opt/calificanew.gdb, SYSDBA, password, Database options: PAGE_SIZE = 8192 FILE "calificanew.gdb" STARTING AT PAGE 000001, LENGTH 120000 PAGES FILE "calificanew1.gdb", LENGTH 120000 PAGES FILE "calificanew2.gdb", LENGTH 120000 PAGES FILE "calificanew3.gdb", LENGTH 120000 PAGES; OK. . Ejecutar "Database Properties". . Verificar que se creó la BD con todos estos parámetros.						
32	6. ¿Propiedades iguales?						
33	No. Pedir soporte al DBA y/o Administrador del Servidor. Receptar novedades, las resuelve, y entrega las soluciones documentadas. Continuar con le paso 6.						
34	7. Cambiar en el script "metadataCalificaErrFecha.sql" la sentencia "CREATE DATABASE ..." por: "CONNECT 'specInx3:/opt/calificanew.gdb' USER 'SYSDBA' PASSWORD 'password'; " . Crear los objetos de la BD en "/opt/calificanew.gdb' con: "Run an ISQL Script" con "metadataCalificaErrFecha.sql" y Save output to a file, Si, guardar en directorio de destino con el nombre=metadataCalificaParte1Fecha.txt"; tipo= Results file (*txt), Guardar (parte2 , 3, ...); . Verificar en el log que todo se haya ejecutado correctamente, si hay errores corregirlos y completar el proceso. . Ejecutar "Metadata, Extract Database, Save output to a file, Si, guardar en directorio de destino con el nombre=metadataCalificaNewFecha.sql"; tipo= Script file (*.sql), Guardar; . Comparar entre las metadatas "metadataCalificaErrFecha.sql" y "metadataCalificaNewFecha.sql", para tener la certeza de que se crearon todos los objetos. Si faltan objetos, utilizar cada vez un nuevo escript para crearlos. O en su lugar sacar un respaldo de "Backup Metadata Only" y el respectivo restore en Calificanew...gdb.						
35	8. ¿Objetos iguales?						
36	No. Ejecutar el paso 7 hasta que se hayan creado todos los objetos.						

37	9. Generar la Lista de todas las tablas con: "Metadata, Show, Table, Ok"; "File, Save result to a file, en el directorio de destino, con el nombre=CalificaTablasFecha, Guardar"; Editar "CalificaTablasFecha" e imprimir; Utilizar el "Borland Database Engine (BDE)" u otro para crear y probar los siguientes alias que son requeridos: Fuente: "SIV" que apunte a la BD "calificaerr.gdb" (u otra BD anterior) y Destino: "BACK" que apunte a la BD "calificanew.gdb";						
38	10. Ejecutar "CopiarBD.exe" para pasar los datos de las tablas de la BD "calificaerr.gdb" a la "calificanew.gdb": . Ingresar cada uno de los nombres de las tablas de "CalificaTablasFecha" en el campo denominado "Tabla", luego dar un click en el nombre de la tabla de destino; y otro click en el botón "Añadir". La primera vez pide que se conecte a cada una de las BD. Anotar en la misma lista junto al nombre de cada tabla el número de filas que se han añadido, luego adjuntarla a la Lista de Chequeo.						
39	11. ¿Todos los datos añadidos?						
40	No. Ejecutar el paso 10 hasta que se hayan pasado todos los datos de todas las tablas.						
41	12. Salir de ISQL con "Close"; 12.1. Desconectar la BD con "-"; 12.2. Conectar la BD con "+, /opt/calificanew.gdb, Ok"; 12.3. Poner en monousuario con "Database Shutdown, Deny new connections while waiting, t=0 minutes, Ok"; 12.4. Ejecutar "Database Statistics, ... Close"; 12.5. Ejecutar "Lock Manager Statistics, [No], Close"; 12.6. Ejecutar "Database Sweep, Si"; 12.7. Ejecutar "Transaction Recovery, Aceptar"; 12.8. Ejecutar "Database Validation, Ok, Aceptar"; 12.9. Ejecutar "Database Validation, validate record fragments, Ok, [ejecutar reparación de la BD], Aceptar";						
42	13. ¿Pasó la validación sin error?						
43	No. Pedir soporte al DBA y/o Administrador del Servidor. Receptar novedades, las resuelve, y entrega las soluciones documentadas. Continuar con le paso 13.						
44	14. Registrar en la Lista de Chequeo ubicación y tamaño de los archivos de la BD . . Cambiar al directorio fuente con "cd /opt"; . Renombrar solo el archivo primario de la BD con "mv calificanew.gdb calificaold.gdb; Si sólo falta llenar el último arch. sec., se debe crear 1 + de 120000 pág. Si ya se llenó el último arch. sec crear los necesarios de 120000 cada 1. 15. Mantener un respaldo válido en línea de califica.gbk, por seguridad: . Cambiar al directorio fuente con "cd /var/bases"; . Renombrar el archivo de Bk con: "mv califica.gbk calificaold.gbk; . Cambiar al directorio fuente con "cd /opt";						

45	15. Ejecutar el respaldo en múltiple archivo con: # "cd /usr/local/interbase/bin"; Interbase: Desconectar la base de datos /opt/califica.gdb con "Database Disconnect" o "-" Salir del server con. "-"; Salir del Interbase Manger con: Close; # "ps -aux | grep gds"; (Solo debe estar una conexion: "root ... grep gds"; eliminar las demás con # kill -9 numero-proceso-ej:22174;) # "./gbak -backup /opt/calificaold.gdb stdout | ./gsplit -split /var/bases/f1.gbk 1500m /var/bases/f2.gbk 1500m /var/bases/f3.gbk 1500m"; # "ls -l /var/bases"; Copiar tamaño de archivos:						
46	16. ¿Pasó el respaldo sin error?						
47	No. Pedir soporte al DBA y/o Administrador del Servidor. Receptar novedades, las resuelve, y entrega las soluciones documentadas. Continuar con le paso 16.						
48	17. Para no perder el contenido de los archivos secundarios de la BD que residen en el directorio /opt , se debe renombrarlos, así: "cd /opt"; "mv calificanew1.gdb califica1old.gdb; "mv calificanew2.gdb califica2old.gdb; … Atención: Así se tendrán con el sufijo "old" a todos los archivos de la BD respaldada, pero si conectara la BD calificaold.gdb, ésta direccionará a califica1,2 y 3.gdb mas no los calificanew1old, gdb y calificanew2old.gdb, ¡ Mucho cuidado ! . Registrar en la Lista de Chequeo las propiedades de la BD.						
49	18. Ejecutar el Restore con múltiples archivos de respaldo y de base de datos, que aseguren el 100% de la ejecución de dichas acciones, con: # "cd /usr/local/interbase/bin"; # "ps -aux | grep gds"; (Solo debe estar una conexion: "root ... grep gds"; eliminar las demás con # kill -9 numero-proceso-ej:22174;) # "./gsplit -join /var/bases/f1.gbk /var/bases/f2.gbk /var/bases/f3.gbk | ./gbak -replace_database -page_size 8192 stdin /opt/califica.gdb 120000 /opt/califica1.gdb 120000 /opt/califica2.gdb 120000 /opt/califica3.gdb 120000"; . Verificar copias y tamaños con: # ls -l /opt;						
50	19. ¿Pasó el restore sin error?						
51	No. Pedir soporte al DBA y/o Administrador del Servidor. Receptar novedades, las resuelve, y entrega las soluciones documentadas. Continuar con le paso 19.						

52	20. Desconectar la BD con "-"; . Conectar la BD con "+, /opt/califica.gdb"; . Poner la BD en monousuario con "Database Shutdown, Deny new connections while waiting, t=0 min. Ok"; . Ingresar a "Interactive SQL"; . Ejecutar "Metadata, Extract Database, Save output to a file, Si, guardar en "…\Procedim\IT_P#p_CodiFuen", nombre="metadataCalificaFecha.sql"; tipo= Script file (*.sql), Guardar; Salir de "Interactive SQL" con close;. . Ejecutar "Database Properties" para comprobar si las propiedades obtenidas son las mismas que las anotadas en el paso 1 y con todos los archivos determinados en el paso 4.						
53	21. ¿Propiedades iguales?						
54	No. Pedir soporte al DBA y/o Administrador del Servidor. Receptar novedades, las resuelve, y entrega las soluciones documentadas. Continuar con le paso 21.						
55	22. Ejecutar los pasos desde el 12.4 al 13, pero sin errores. . Ejecutar "Database Restart"; . Desconectar la BD con "-"; . Salir del server con "Close"; . Salir de la consola.						
56	23. Confirmar la creación, ubicación y tamaño de los archivos, que sean concordantes con los datos del paso 4; . Salir del Servidor con "exit"; . Salir del SSH con "Close". . Registrar en la Lista de Chequeo la hora de finalización del procedimiento a entera satisfacción de PETROECUADOR.						
57	24. Presenta la documentación actualizada al Jefe de IT, para su aprobación y difusión.						
58	Fin						

Nivel de satisfacción del cliente :	Total:	Si	Parcial:		Insatisfecho:	

Por el Técnico encargado de rehabilitar el Servicio:

Por el Responsable del Servicio:

Firma: _____ _____

Nombre: _____ _____

No. Rol o Cédula de Ciudadanía: _____ _____

SERVICIO CRÍTICO "INTERBASE (DATOS RCP)"

Fecha: 2008-06-03 **Acta de Entrega Recepción de Retorno a la Normalidad del Servicio Crítico de TI** **Doc.1.7.5**

Matriz, Filial o Distrito: PETROECUADOR y Unidad: Sistemas

En la ciudad de Quito se suscribe la presente Acta entre el Técnico que rehabilitó este Servicio y el Responsable del mismo, acta contenida en las siguientes cláusulas:

PRIMERA: OBJETIVO

Mantener la Continuidad del Servicio que apalanca a la Gestión Institucional y en caso de emergencia rehabilitarlo conforme a lo establecido en el Acuerdo de Nivel de Servicio.

SEGUNDA: ESCENARIOS DEL SERVICIO

2.1 Estado previo a la emergencia

Emergencia	Base de Datos de Interbase “Califica” de múltiple archivo, que por el crecimiento acelerado de la cantidad de datos, su tiempo de respuesta se ha degradado y en promedio superaba los 3 segundos.
Diagnóstico	1. El tamaño de sus archivos excedió el umbral establecido del 75% 2. Dio error al ejecutar “Validate record fragments”.

2.2 Estado del Servicio durante la emergencia

Solución	Abrir la Base de Datos en modo mono usuario. Ejecutar sin errores el procedimiento de Respaldo . Ejecutar sin errores el procedimiento de recuperación de la Base de Datos con un archivo adicional. Ejecutar sin errores la “Validate record fragments”.

2.3 Estado luego de la emergencia

Normalidad	Abrir la base de datos en modo multiusuario, sin pérdida de datos.

TERCERA: DERECHOS Y OBLIGACIONES

3.1 El Responsable del Servicio comprobó que el Servicio está 100% operativo.

3.2 El Técnico alertó al Responsable de este Servicio sobre las características de crecimiento, novedades que se han encontrado y conveniencia del mantenimiento preventivo.

3.3 El funcionario que debido a cualquier causa se separe de la Unidad de Sistemas, como paso previo a la obtención de su liquidación, procederá a capacitar y entregar a otros funcionarios los procedimientos de Continuidad de los Servicios y otros que estuvieron a su cargo.

CUARTA: ALCANCE

Lograr la Continuidad del Servicio que se encontraba en estado de emergencia, aplicando los procedimientos disponibles y/o otros que se requirieron para este fin.

QUINTA: ACEPTACION DE LOS FUNCIONARIOS, PARA QUE PETROECUADOR PUEDA EXIGIR Y DEMANDAR EL CUMPLIMIENTO DE SUS RESPONSABILIDADES

5.1 Aceptar y asumir todas las responsabilidades pertenecientes a la aplicación de procedimientos de Respaldo, Restauración, Recuperación y/ otros tendientes a rehabilitar la Continuidad de este Servicio, así como, de controles y actualización de la documentación respectiva, que también es útil para efectos de auditoría, lo cual incluye la incorporación de los cambios efectuados a la documentación existente y de nuevos procedimientos.

5.2 Aceptar que al suscribir esta acta, son administrativa, personal y pecuniariamente responsables tanto del estado en el cual retorna a la normalidad el Servicio recibido, como por la validez y la actualización de la documentación de los procedimientos aplicados en este caso.

Para constancia y fe de conformidad con lo actuado, suscriben la presente acta en original y tres copias de igual contenido y valor.

ENTREGUÉ CONFORME	**RECIBÍ CONFORME**
Firma y sello:	
Nombre:	
No. Rol. o Céd.Ciud.	

ANEXO 1.8

Internet/Intranet

Documentación mínima:

1.8.1 Un diagrama de bloque que incluya la Planificación y Ejecución

1.8.2 Un diagrama del procedimiento de Respaldo y Restauración con todo lo necesario para recuperar desde 0

1.8.3 Un diagrama del procedimiento de Recuperación desde 0, a partir de los recursos disponibles

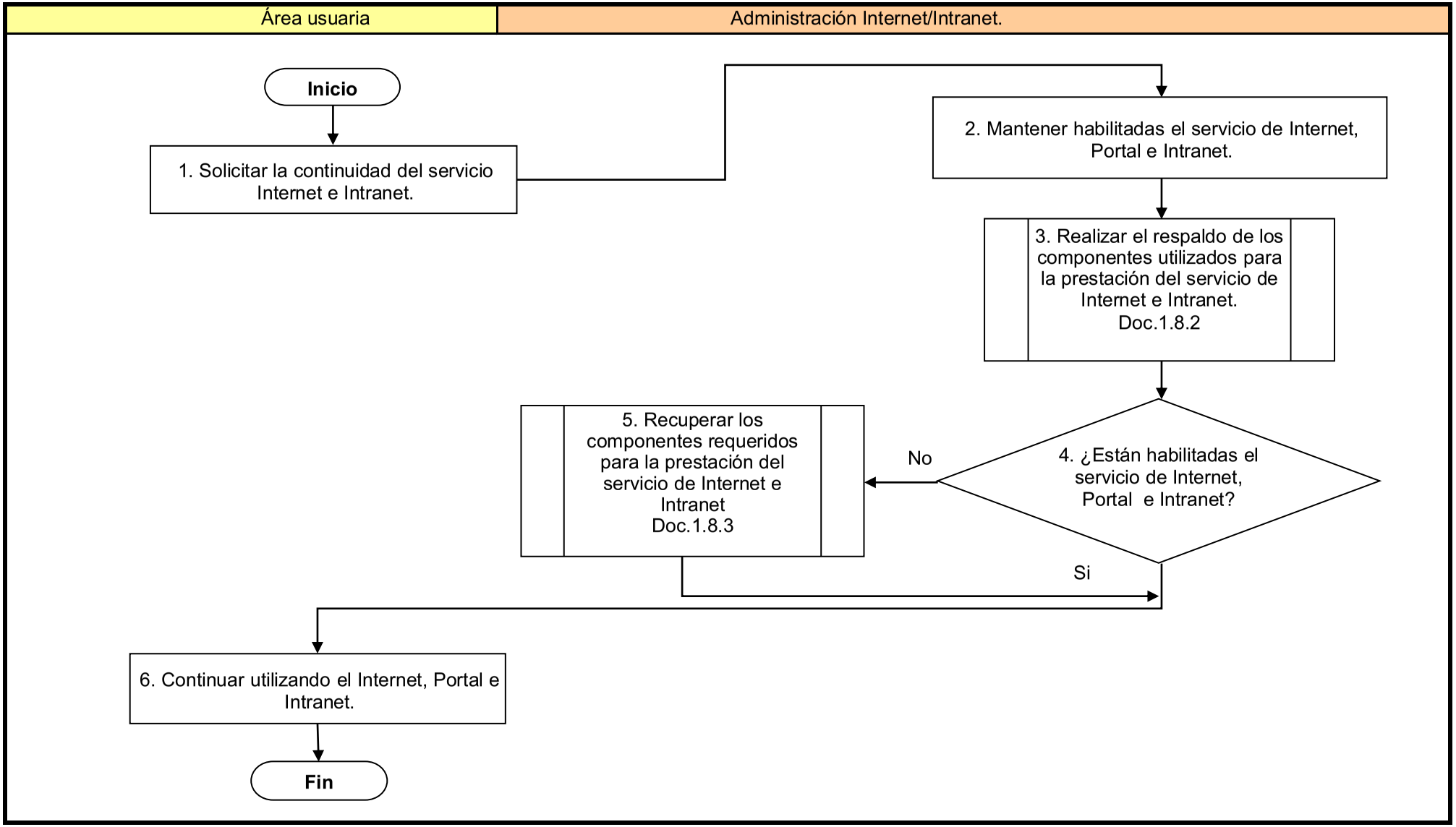
1.8.4 Lista de chequeo que incluye a los dos procedimientos anteriores.

1.8.5 Acta de ER del retorno a la normalidad.

SERVICIO CRITICO:"INTERNET / INTRANET"

Diagrama de Bloque

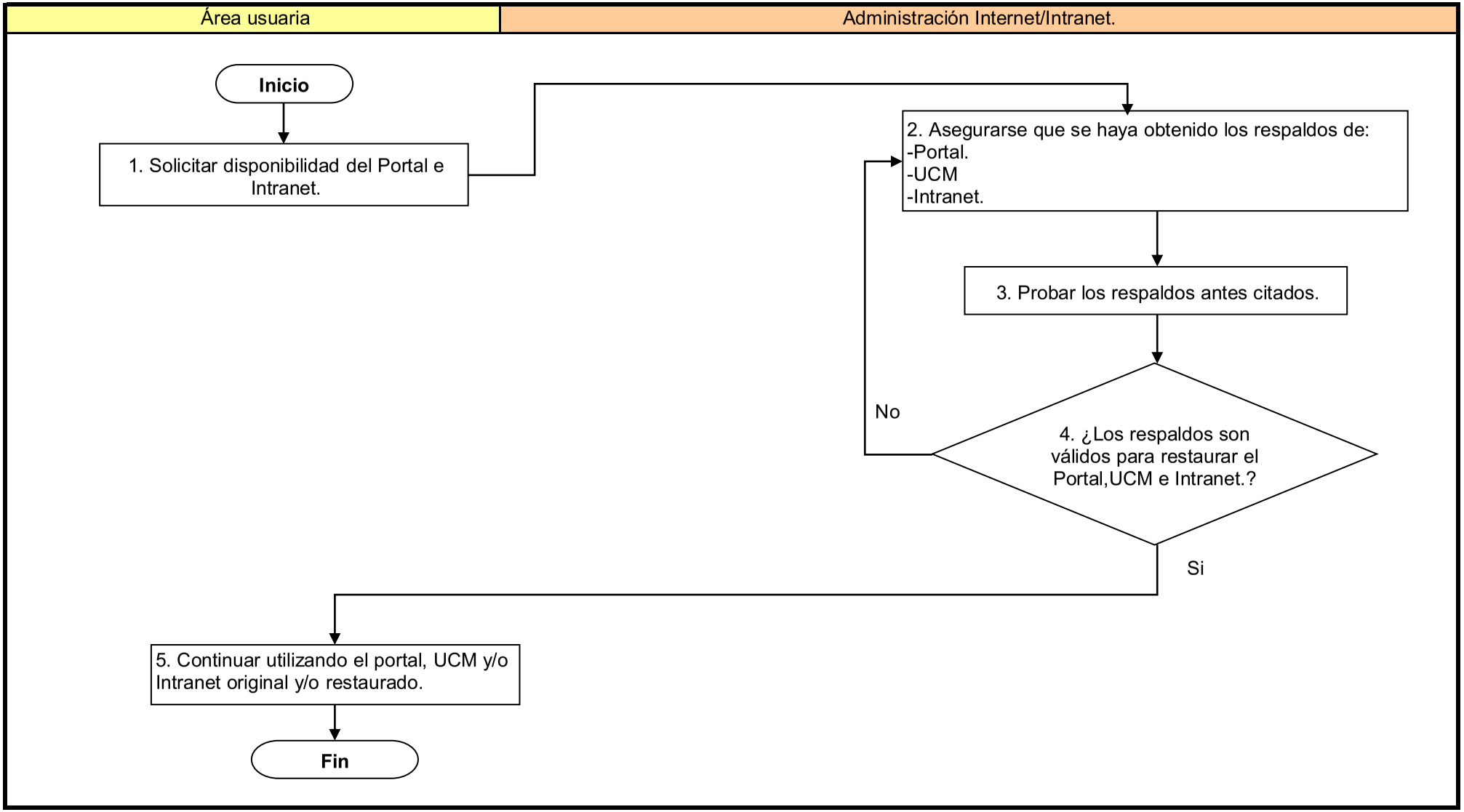
Doc.1.8.1



SERVICIO CRITICO:"INTERNET / INTRANET"

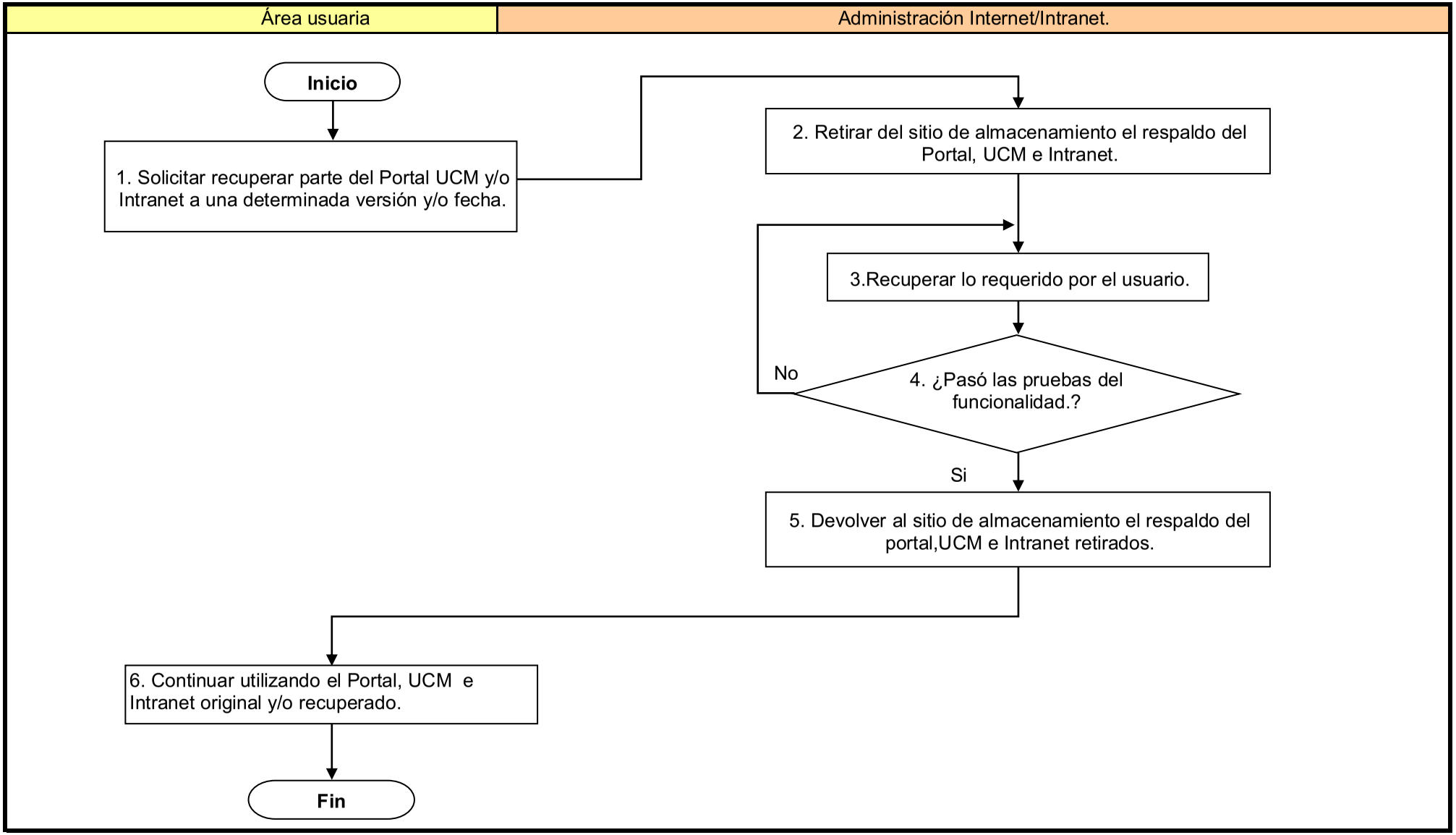
Diagrama del procedimiento de Respaldos y Restauración

Doc.1.8.2



SERVICIO CRITICO:"INTERNET / INTRANET"
Diagrama del procedimiento de Recuperación.

Doc.1.8.3



SERVICIO CRITICO:"INTERNET / INTRANET"
Lista de Chequeo

Fecha y hora de inicio:2008-08-12 y 8h00 Fecha y hora de finalización:2008-08-15 y 12h00 **Doc.1.8.4**

No.	Procedimientos y Pasos:	Parámetros a controlar, comparar y evaluar.		Cumplió			Observaciones:
		Parámetro	Valor	Si	Par	No	
	Doc.1.8.2. Diagrama del procedimiento de Respaldos y Restauración						
1	1. Solicitar disponibilidad del Portal e Intranet.						
2	2. Asegurarse que se haya obtenido los respaldos de: Portal, UCM, Intranet.						
3	3. Probar los respaldos y/o restauración antes citados.						
4	4. ¿Los respaldos son válidos para restaurar el Portal,UCM e Intranet?						
5	No. Continuar con el paso 2.						
6	Si. 5. Continuar utilizando el Portal, UCM y/o Intranet original y/o restaurado.						
	Doc.1.8.3. Diagrama del procedimiento de Recuperación.						
7	1. Solicitar recuperar parte del portal UCM y/o intranet a una determinada versión y/o fecha.			si			
8	2. Retirar del sitio de almacenamiento el respaldo del portal, UCM e Intranet.			si			
9	3.Recuperar lo requerido por el usuario.			si			
10	4. ¿Pasó las pruebas del funcionalidad?			si			
11	No. Continuar con el paso 3.						
12	Si. 5. Devolver al sitio de almacenamiento el respaldo del Portal,UCM e Intranet retirados.			si			
13	6. Continuar utilizando el Portal, UCM e Intranet original y/o recuperado.			si			

Nivel de satisfacción del cliente : Total: Si Parcial: ☐ Insatisfecho: ☐

Por el Técnico encargado de rehabilitar el Servicio:

Firma: _____
Nombre: _____
No. Rol o Cédula de Ciudadanía: _____

Por el Responsable del Servicio:

_____
_____
_____

SERVICIO CRÍTICO "INTERNET / INTRANET"

Fecha: 2008-08-12 **Acta de Entrega Recepción de Retorno a la Normalidad del Servicio Crítico de TI** **Doc.1.8.5**

Matriz, Filial o Distrito: PETROECUADOR y Unidad: Sistemas

En la ciudad de Quito se suscribe la presente Acta entre el Técnico que rehabilitó este Servicio y el Responsable del mismo, acta contenida en las siguientes cláusulas:

PRIMERA: OBJETIVO

Mantener la Continuidad del Servicio que apalanca a la Gestión Institucional y en caso de emergencia rehabilitarlo conforme a lo establecido en el Acuerdo de Nivel de Servicio.

SEGUNDA: ESCENARIOS DEL SERVICIO

2.1 Estado previo a la emergencia

Emergencia	Se daño el disco del servidor del Universal Content Management (UCM) en el cual funcionaba el Sistema de Administración de Contenido (SAC) en la Intranet, por lo que se lo formateó.
Diagnóstico	1. Realizar la reinstalación del UCM. 2. Realizar la restauración de los componentes del SAC.

2.2 Estado del Servicio durante la emergencia

Solución	1. Recuperar la base de datos Oracle a partir del respaldo obtenido mediante el agente de Oracle y el RMAN. 2. Completar las tareas de recuperación de la Base de Datos para dejarla 100% operativa. 3. Recuperar el SAC que opera dentro de la Intranet.

2.3 Estado luego de la emergencia

Normalidad	Utilizar el SAC en la Intranet sin pérdida de datos y en forma normal.

TERCERA: DERECHOS Y OBLIGACIONES

3.1 El Responsable del Servicio comprobó que el Servicio está 100% operativo.

3.2 El Técnico alertó al Responsable de este Servicio sobre las características de crecimiento, novedades que se han encontrado y conveniencia del mantenimiento preventivo.

3.3 El funcionario que debido a cualquier causa se separe de la Unidad de Sistemas, como paso previo a la obtención de su liquidación, procederá a capacitar y entregar a otros funcionarios los procedimientos de Continuidad de los Servicios y otros que estuvieron a su cargo.

CUARTA: ALCANCE

Lograr la Continuidad del Servicio que se encontraba en estado de emergencia, aplicando los procedimientos disponibles y/o otros que se requirieron para este fin.

QUINTA: ACEPTACION DE LOS FUNCIONARIOS, PARA QUE PETROECUADOR PUEDA EXIGIR Y DEMANDAR EL CUMPLIMIENTO DE SUS RESPONSABILIDADES

5.1 Aceptar y asumir todas las responsabilidades pertenecientes a la aplicación de procedimientos de Respaldo, Restauración, Recuperación y/ otros tendientes a rehabilitar la Continuidad de este Servicio, así como, de controles y actualización de la documentación respectiva, que también es útil para efectos de auditoría, lo cual incluye la incorporación de los cambios efectuados a la documentación existente y de nuevos procedimientos.

5.2 Aceptar que al suscribir esta acta, son administrativa, personal y pecuniariamente responsables tanto del estado en el cual retorna a la normalidad el Servicio recibido, como por la validez y la actualización de la documentación de los procedimientos aplicados en este caso.

Para constancia y fe de conformidad con lo actuado, suscriben la presente acta en original y tres copias de igual contenido y valor.

ENTREGUÉ CONFORME	**RECIBÍ CONFORME**
Firma y sello:	
Nombre:	
No.Rol. o Céd.Ciud.	

GLOSARIO

El Marco Conceptual está conformado por los siguientes conceptos operativos de las variables y otros términos básicos utilizados en la investigación:

Adquirir e Implementar (ACQUIRE AND IMPLEMENT AI): Para llevar a cabo la estrategia de IT, las soluciones de IT deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Almacenamiento Alterno Off-site: Es el almacenamiento externo a la entidad, de los recursos indispensables para mantener la continuidad de los servicios de IT, tales como archivos grabados en medios magnéticos con fines de respaldo y recuperación, etc.

Análisis de riesgos: Es la identificación y evaluación de las debilidades y amenazas relacionados con la continuidad de la Prestación de Servicios de IT, considerando la probabilidad y frecuencia de ocurrencia, su impacto, urgencia y prioridad de restablecer el Servicio.

Aplicaciones: Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.

Aplicaciones: Son software que cuenta con su respectiva documentación de procedimientos manuales, semimanuales o automatizados de operación, seguimiento y control.

Application Management: Administrar las Aplicaciones.

Availability Management: Gestión de la disponibilidad.

Blanco: Vacío, podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

Business Continuty Mgt: Gestión de la continuidad de la Institución.

Capacity Management: Gestión de la capacidad.

Caso de estudio COBIT e ITIL: Es un tema estratégico de Gestión de TI en una Entidad más que tecnológico.

Centro de procesamiento de datos: Es el área física donde se ubica a los computadores que reciben, procesan y almacenan la información.

Change Management: Gestión de cambio.

COBIT: Control **Ob**jectives for **I**nformation and Related **T**echnology.

Cold-Site: Es un sitio de respaldo que cuenta con la infraestructura indispensable para restaurar desde allí la continuidad del servicio de IT.

Computer Installations and Acceptance: Gestión de instalación y aceptación de computadoras.

Confiabilidad: Es el Criterio de Información que mide si es o no apropiada y útil para la gestión y toma de decisiones de IT y la entidad.

Confidencialidad: Es el Criterio de Información que determina si es o no sensible contra divulgación no autorizada.

Configuration Management: Gestión de la configuración.

Control Interno: Son las políticas, procedimientos, prácticas y estructuras organizativas diseñadas para proveer aseguramiento razonable de que se alcanzarán los objetivos de la entidad y que los eventos no deseados serán prevenidos, detectados y corregidos. Se traducen en objetivos y procedimientos de control.

Controles Compensatorios o Preventivos: Son parte del control interno y sirven para reducir el riesgo causado por la existencia de una debilidad o amenaza.

Controles Correctivos: Son controles que están diseñados para corregir cualesquier desvío para retornar a la normalidad.

Controles de Entrada: Son técnicas y procedimientos que se usan para verificar, validar y editar datos para asegurar que sólo se ingresen a la computadora datos correctos.

Criterios o requerimientos de Información: Son la Efectividad, Eficiencia, Confidencialidad, Disponibilidad, Cumplimiento y Confiabilidad, que también son categorías superpuestas extraídas de los requerimientos de Calidad, Fiduciarios y Seguridad de la información.

Cumplimiento: Es el Criterio de Información que observa siempre el cumplimiento de leyes, regulaciones, normativa vigente, derechos y obligaciones.

Dato: Es el Recurso de IT que se transforma en información y conocimiento de interés para la entidad. **Datos:** Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

Disponibilidad: Es el Criterio de Información que con la debida seguridad otorga accesibilidad oportuna a los recursos y capacidades de los procesos. Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

Dominios: Son la Planeación y Organización; Adquisición e Implementación; Entrega y Soporte; y Monitoreo, los mismos que corresponden a la agrupación natural de los procesos de IT de cualquier entidad.

Efectividad: Es el Criterio de Información que responde por la oportunidad, relevancia, pertinencia, exactitud, consistencia, integridad y utilidad de la misma, para los procesos de IT y entidad.

Eficiencia: Es el Criterio de Información que se encarga de la productividad en la generación de la misma, mediante el empleo óptimo de los recursos.

Entidad: Es sinónimo de negocio, empresa, Institución, organización u otra persona jurídica, que podría adoptar estándares y buenas prácticas.

Entregar y dar Soporte (DELIVER AND SUPPORT (DS): En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. *Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.* Es el dominio de COBIT que define la Prestación de Servicios de IT, Capacitación y Procesos de Soporte.

Estrategia o estratégico: Es un lineamiento regulable mediante el cual se toman decisiones óptimas en cada momento.

Factores Críticos de Éxito (Critical Success Factors): Son las directrices más importantes que deben ser consideradas para lograr el éxito de los procesos de

IT, tales como la obtención, mantenimiento y nivelación de capacidades y habilidades del Recurso Humano, etc.

Financial Management: Gestión financiera.

Gestión de la Capacidad (Capacity Management): Es el Proceso de ITIL que permite que la entidad cuente con la infraestructura y capacidad necesarias para prestar los Servicios de IT conforme a lo acordado en el corto, mediano y largo plazos. Incluye el análisis de la oferta y demanda de dichos Servicios.

Gestión de la Continuidad (IT Service Continuity Management): Es el Proceso de ITIL que responde por el análisis y administración de riesgos para prevenir, mitigar y recuperarse de una interrupción en los procesos críticos de IT y la entidad, así como de definir, probar y ejecutar el Plan de Continuidad de los Servicios de IT, que también es conocido como Plan de contingencias y recuperación de desastres. El impacto de los riesgos se medirá en función de la pérdida de oportunidades y/o ganancias para la entidad.

Gestión de la Disponibilidad (Availability Management): Es el Proceso de ITIL encargado del diseño e implantación de la infraestructura de IT que soporte adecuadamente los Acuerdos de Niveles de Servicios programados y vigentes.

Gestión de la Prestación de los Servicios (Services Delivery): Es el dominio táctico de ITIL que incluye los procesos estratégicos de IT, la Gestión de la Capacidad, Gestión Financiera, Gestión de la Disponibilidad, Gestión de los Niveles de Servicio y Gestión de la Continuidad de los Servicios de IT, y se encarga de la calidad, relación costo – beneficio y rentabilidad de los Servicios de IT. Se une estrechamente con el ciclo de planificación anual de la entidad

Gestión de los Acuerdos de Niveles de Servicios (Service Level Management SLA y SLM): Es el Proceso de ITIL que permite brindar servicios de calidad que satisfagan las necesidades de los usuarios y clientes, para lo cual se suscribirán acuerdos con los proveedores, usuarios y clientes en los que se establezcan las condiciones, derechos y obligaciones de las partes. Logrando así alinear y balancear los servicios de IT con los objetivos de la entidad. Incluye un catálogo de servicios, la negociación, seguimiento y revisión de acuerdos.

Gestión de los Servicios de IT: Es el Dominio de ITIL que contribuye a mejorar la calidad de los demás Procesos de IT y a su alineación con los objetivos de la entidad.

Gestión Financiera (Financial Management): Es el Proceso de ITIL que se encarga de clarificar el verdadero costo de los Servicios de IT como un centro con rentabilidad, considerando presupuestos, contabilidad, distribución y recuperación de costos.

Governability: Se traduce como Gobernabilidad, y se refiere a la capacidad de gobernar

Governance: Se traduce como Forma de Gobierno o simplemente como Gobierno

Grado de Madurez: Es el valor real que le corresponde a cada proceso, sobre la base de su propio desarrollo dentro de un modelo que utiliza un rango de 0 a 5, siendo el 5 el grado de mayor madurez del proceso. Mide cuántos Objetivos de Control se están cumpliendo, respecto de todos los objetivos existentes. Sirve para determinar la brecha entre la situación actual y el grado de madurez al cual se desea llegar en el período planeado.

Hot-Site: Es un sitio alterno totalmente equipado y operativo, listo para ser usado en caso de una interrupción en la continuidad de la operación de IT, para que desde allí se continúe prestando los Servicios de IT a la entidad.

ICT Infrastructure Management: Administrar la Infraestructura.

Incident Management: Gestión de servicios e incidentes.

Indicadores de Desempeño (KPI): Son medidas de COBIT para valorar el desempeño de los Procesos y sobre esa base establecer la estrategia de mejora continua de los mismos.

Indicadores de Resultado (KGI): Son medidas de COBIT para evaluar los resultados alcanzados por los Procesos, con un enfoque hacia las Perspectivas del Cliente y Financiera del Cuadro de Mando Integral (Balanced Scorecard BSC).

Instalaciones de Tecnología: Es un Recurso de IT constituido por todos los componentes de infraestructura física y tecnológica, tales como hardware y software básico; sistemas operativos; sistemas de administración de bases de datos; redes; telecomunicaciones; multimedia; etc., que son indispensables para la prestación de los Servicios de IT.

Integridad: Es el Criterio de Información que responde por la exactitud, totalidad y validez de la misma, para IT y entidad. Se refiere a la precisión y suficiencia de la

información, así como a su validez de acuerdo con los valores y expectativas del negocio.

IT o TI: Comunicaciones, Tecnologías de la Información y Automatización.

ITIL: IT Infrastructure Library.

Management of Local Processors: Gestión de los servidores (procesadores) locales.

Monitorear y Evaluar (MONITOR AND EVALUATE ME): Es el dominio de COBIT que se encarga de realizar el seguimiento de los KPIs y KGIs de cada proceso, para posibilitar el mejoramiento continuo de los mismos y reaccionar dinámicamente con estrategias y planes de acción que corrijan las desviaciones que se detecten.

Network Services Management: Gestión de servicios de red.

Objetivo de Control: Es el resultado pre establecido para cada control, que se aplicará a cada Dominio, Proceso o Actividad de IT, a fin de que siempre estén alineados a los objetivos de la entidad.

Operations Management: Gestión de operaciones.

Partnerships and Outsourcing: Gestión de asociaciones y tercerización.

Personal: Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

Planear y Organizar (PLAN AND ORGANISE PO): Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Planificación y Organización: Es el dominio de COBIT que define la alineación estratégica y táctica de los objetivos de IT con los de la entidad.

Planning to Implement Service Management: Planificar para implementar la administración de los Servicios

Practice through Radical Change: Gestión de cambio radical.

Primario: Es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.

Problem Management: Gestión de problemas.

Procedimiento de Implementación: Es conjunto de pasos que se plantean para realizar con éxito la implementación de los procesos de Gestión de Prestación de Servicios de las Tecnologías de la Información (TI), basados en el estándar COBIT y buenas prácticas ITIL.

Recurso Humano: Es el Recurso de IT que hace posible la transformación de la materia prima en los Servicios de IT, a través del talento humano, habilidad, conciencia, productividad, etc.

Recursos de TI: Son los Datos, Aplicaciones**,** Tecnología, Instalaciones y Recurso Humano, que tienen que ser debidamente administrados para alcanzar los objetivos de IT y entidad.

Release Management: Gestión de liberación de versiones.

Respaldo: Son objetos válidos y probados, debidamente almacenadas en un sitio alterno, tales como archivos, equipos, datos, procedimientos, etc., que están disponibles para utilizarse en el restablecimiento de la Prestación de los Servicios de IT, cuando se presente una interrupción prolongada en las operaciones de IT.

Secundario: Es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.

Security Management: Gestión de las seguridades.

Service Continuity Mgt: Gestión de la continuidad de los servicios de IT.

Service Delivery: Prestación del servicio.

Service Level Management: Gestión de niveles de servicio.

Service Management: Administración de los servicios.

Service Support: Servicios de apoyo y soporte.

Software Lifecycle Support: Gestión de soporte al ciclo de vida del software.

Surviving Changes: Gestión de sobrevivencia a cambios.

Systems Management: Gestión de sistemas.

Tecnología: La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.

Testing an IT Service for operational use: Gestión de prueba de servicios de TI antes de utilizarlo.

The Business Perspective: La Perspectiva de la Institución.

Transformation of Business: Gestión de transformación de la Institución.

ESCUELA POLITECNICA NACIONAL
FACULTAD DE INGENIERÍA DE SISTEMAS

CARRERA DE MAESTRÍA EN GESTIÓN DE LAS COMUNICACIONES Y TECNOLOGÍAS DE LA INFORMACIÓN

ORDEN DE EMPASTADO

De acuerdo con lo estipulado en el Artículo 83 del Reglamento del Sistema de Estudios de las Carreras de Formación Profesional y de Postgrados, aprobado por el Consejo Politécnico en sesión del 16 de agosto de 2011 y una vez verificado el cumplimiento del formato de presentación establecido, se autoriza la impresión y encuadernación final de la Tesis de Grado presentado por los Ingenieros:

OCHOA MORENO MARCO ANTONIO

Fecha de autorización: **Quito, D.M., 07 de junio de 2012.**

Ing. MSc. Carlos Montenegro
DECANO
FACULTAD DE INGENIERÍA DE SISTEMAS