UNIVERSIDAD DE COSTA RICA

SISTEMA DE ESTUDIOS DE PROGRADOS

REVISIÓN DEL CONTROL DEL PROCESO DS4:

GARANTIZAR LA CONTINUIDAD DEL SERVICIO DE LAS TIC's

Trabajo final de graduación sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas, para optar por el grado y título de Maestría Profesional en Auditoría en Tecnologías de Información.

ANA ELIGIA ORTEGA NAVARRO

Ciudad Universitaria Rodrigo Facio, Costa Rica

2015

Contenido

Tabla de gráficos

Dedicatoria

Gracias a esas personas importantes en mi vida, que siempre estuvieron listas para brindarme toda su ayuda, ahora me toca regresar un poquito de todo lo inmenso que me han otorgado. Con todo mi cariño este trabajo se lo dedico a ustedes:

Papá Nello

Mamá Esperanza

Y a mis Hermanas.

Agradecimiento

Primero y antes que nada, dar gracias a Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

Agradecer hoy y siempre a mi familia por el esfuerzo realizado por ellos. El apoyo en mis estudios. A mis padres y demás familiares que me brindan el apoyo, la alegría y me dan la fortaleza necesaria para seguir adelante.

Hoja de aprobación

Este trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar por el grado y título de Maestría Profesional en Auditoría de Tecnología de Información.

_____

[Doctor Sergio Espinoza Guido]

Profesor Guía

_____

[M. Sc. Xiomar Delgado]

Lector (Profesor de Posgrado)

_____

[Lic. Freddy Solano Vargas, MATI]

Lector de Empresa

_____

Dr. Aníbal Barquero Chacón

Director Programa de Posgrado en Administración y Dirección de Empresas

_____

[Ana Eligia Ortega Navarro]

Sustentante

CAPÍTULO I

1.1. Introducción

1.1.1. Delimitación del tema

El estudio a realizar es sobre el control del proceso de las Tecnologías de Información y Comunicaciones, en adelante (TIC), designado para Garantizar la Continuidad del Servicio (DS4)[1] del sistema principal de cuentas de ahorros, en adelante (AB), el cual se realizará en la oficina de la Auditoría de Sistemas y el área de Tecnología de Información de la Institución seleccionada.

1.1.2. La organización

ABC es una institución financiera, cuyos sus orígenes fueron en una casa bancaria de carácter regional, fundada para promover el desarrollo de la provincia mediante el impulso de la agricultura, tradicionalmente la actividad económica por excelencia en las fértiles tierras de la provincia.

Precisamente, a raíz de las dificultades económicas de la época, varios bancos capitalinos que tenían oficinas en la provincia decidieron retirarse, lo que afectó aún más a la economía local. Fue entonces cuando un grupo de ciudadanos toma la iniciativa de unir sus capitales para crear un banco dedicado, de manera exclusiva, a promover el desarrollo de la zona.

Nace así el 1° de junio de 1918 la Institución objeto de estudio del presente trabajo y abre sus puertas al público el 16 de setiembre del mismo año.

---

[1] Marco de Trabajo, Objetivos de Control, Directrices Gerenciales y Modelos de Madurez (COBIT 4.1.)

Las leyes bancarias de 1936, le permitieron adecuar su escritura social a la evolución del negocio bancario y ampliar sus actividades. El ABC es hoy una institución financiera consolidada, cuyo objetivo es mantener los niveles de eficiencia de la banca moderna y conservar el trato personalizado con sus clientes.

Misión

Somos su banco estatal de banca universal y de desarrollo, enfocado en la eficiencia, en el servicio al cliente y en una adecuada gestión del riesgo.

Visión

Seremos la corporación financiera que satisfaga las necesidades de sus clientes en banca universal y de desarrollo, a través de una gestión eficiente, prudente, transparente y rentable, con responsabilidad y en armonía con el ambiente.

Dentro de los productos que ofrece, se destacan los siguientes:

- Créditos Corporativos
- Tarjetas de Crédito Corporativas
- Seguros
- Cuentas Bancarias
- Inversiones a la Vista
- Comercio exterior
- Fideicomisos
- Cajas de Seguridad
- Servicios Electrónicos
- Convenios

1.1.3. Justificación

La empresa donde se va realizar el trabajo es una institución financiera consolidada, cuyo objetivo es mantener los niveles de eficiencia de la banca moderna y conservar el trato personalizado con clientes. Actualmente cuenta con más de 600 empleados y con 30 oficinas a nivel del todo el país.

Debido a lo indicado anteriormente, dicha institución necesita brindar la continuidad del servicio de TI, minimizado el impacto de las interrupciones que puedan afectar los servicios de TI y así los procesos claves del negocio.

Por tal motivo, es de interés para esta Auditoría que la práctica profesional sea enfocada en la evaluación del control interno del proceso DS4 Garantizar la Continuidad del Servicio y el Nivel de Madurez, el cual debe alcanzar un nivel de madurez 3 definido, según lo establecido en la normativa 14-09, emitida por la Superintendencia General de Entidades Financieras (SUGEF)

El objetivo de esta práctica profesional, es emitir un criterio al área de Tecnología de Información sobre el cumplimiento de los controles y el nivel de madurez alcanzado en el proceso DS4 Garantizar la Continuidad del Servicio, además de recomendar oportunidades de mejora y agregar valor, para garantizar de manera razonable la efectividad, eficiencia y disponibilidad del servicio del sistema principal (AB) y mantener la herramienta desarrollada para posteriores revisiones por parte de la Auditoría.

1.1.4. Finalidad del estudio

La Superintendencia General de Entidades Financieras (SUGEF) es un ente fiscalizador cuyo objetivo es velar por la estabilidad, la solidez y el funcionamiento eficiente del sistema financiero nacional, con estricto apego a las disposiciones legales y

reglamentarias y de conformidad con las normas, directrices y resoluciones que dicte la propia institución, todo en salvaguarda del interés de la colectividad.

Funciones de SUGEF[2]

- Velar por la estabilidad, la solidez y el funcionamiento eficiente del sistema financiero nacional.
- Fiscalizar las operaciones y actividades de las entidades bajo su control.
- Dictar las normas generales que sean necesarias para el establecimiento de prácticas bancarias sanas.
- Establecer categorías de intermediarios financieros en función del tipo, tamaño y grado de riesgo.
- Fiscalizar las operaciones de los entes autorizados por el Banco Central de Costa Rica a participar en el mercado cambiario.
- Dictar las normas generales y directrices que estime necesarias para promover la estabilidad, solvencia y transparencia de las operaciones de las entidades fiscalizadas.
- Presentar informes de sus actividades de supervisión y fiscalización al Consejo Nacional de Supervisión del Sistema Financiero.
- Cumplir con cualesquiera otras funciones y atributos que le correspondan, de acuerdo con las leyes, reglamentos y demás disposiciones atinentes.

Según sus funciones de fiscalización y supervisión, la SUGEF tiene la responsabilidad de dictar las normas generales que sean necesarias para el establecimiento de prácticas bancarias sanas, dentro de las instituciones que sean supervisadas por esta.

[2] Superintendencia de Entidades Financieras SUGEF, Objetivos y Funciones (www.sugef.fi.cr).

En lo referente al área de Tecnología de Información, dicha institución emitió el REGLAMENTO SOBRE LA GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN SUGEF 14-09, aprobado por el Consejo Nacional de Supervisión del Sistema Financiero, mediante Artículo 6, del acta de la sesión 773-2009, celebrada el 20 de febrero del 2009.

Este reglamento tiene como objetivo la definición de los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información, que adopta entre otros, la metodología COBIT 4.0, que es dividida por procesos, en este caso el proceso Garantizar la Continuidad del Servicio (DS4).

De acuerdo con lo indicado en la norma, la institución en estudio realizó la implementación de los 17 procesos obligatorios, en cumplimiento de lo solicitado por el ente supervisor, actualmente la implementación de los procesos se encuentra en la etapa de ejecución.

1.1.5. Intereses profesionales

- Aplicar los conocimientos adquiridos en los cursos llevados en el programa de la maestría en Auditoría de Tecnología de Información.
- Adquirir mayor experiencia en la materia de Auditoría de Tecnologías de Información y Comunicación.
- Integrar los conocimientos transmitidos, por parte de los diferentes profesores de la maestría y personal de institución con conocimiento del tema.
- Adquirir mayor conocimiento sobre el proceso de Administración de la Continuidad del Servicio y de las nuevas tendencias referentes a esta materia.

1.1.6. Objetivos

Objetivo general

Evaluar el proceso Garantizar la Continuidad del Servicio (DS4), de acuerdo con la normativa aplicable por el ente supervisor (SUGEF) y normativa interna de la institución ABC, con el fin de emitir criterio sobre el cumplimiento de la aplicación de los controles y el nivel de madurez alcanzado.

Objetivos específicos

- Investigar con el dueño del proceso sobre las acciones que ha iniciado la Institución, como parte de la implementación del proceso, con el fin de obtener un conocimiento de la situación vigente y de los esfuerzos realizados para su implementación.
- Verificar los controles establecidos para el proceso de continuidad del servicio del sistema principal (AB), para determinar su cumplimiento y la reducción del riesgo asociado a este.
- Determinar el nivel de madurez en el que se encuentra el proceso Garantizar la Continuidad del Servicio (DS4) al sistema principal (AB), para ser comunicado al personal responsable de su implementación y que así se disminuyan de manera razonable los riesgos asociados al proceso.

1.1.7. Alcance

El trabajo se enfoca en la evaluación de los objetivos del control interno y el nivel de madurez definidos en el proceso para Garantizar la Continuidad del Servicio (DS4) del sistema principal (AB), establecidos en la Norma 14-09 emitida por la SUGEF, en el periodo comprendido entre julio y noviembre del 2014, de acuerdo con lo establecido por la Junta Directiva de la Institución ABC, para el debido cumplimiento e implementación de este proceso.

1.1.8. Limitaciones

En relación con la confidencialidad de la información, en cuanto a los resultados de análisis de las pruebas en la evaluación, sus riesgos y la documentación sensible según categorización de la institución, se debe mantener la confidencialidad y el acceso se limitará a la revisión en sitio para su verificación.

Es importante considerar como parte de la confidencialidad, que para efectos de este documento será protegido el nombre de la Institución y los datos que pueden incurrir en referencia de esta.

1.1.9. Marco teórico

La SUGEF en su normativa establece la implementación de los procesos establecidos en el COBIT 4.0; no obstante, de acuerdo con lo establecido por la institución donde se realiza el trabajo de revisión, aunque la SUGEF adoptara el COBIT 4.0, la entidad adoptó el COBIT 4.1 donde se establecen, entre otros, los siguientes objetivos de control.

Garantizar la Continuidad del Servicio

La necesidad de brindar continuidad en los servicios de TIC requiere desarrollar, mantener y probar planes de continuidad, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre dichos planes. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TIC, sobre funciones y procesos claves del negocio.

El objetivo general de garantizar la continuidad del servicio que satisface el requerimiento del negocio de TIC, es asegurar el mínimo impacto al negocio en caso de una interrupción de servicios de Tecnología.

Los objetivos de control de TI proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI. (IT Governance Institute ®, COBIT® 4.1, 2007)

Entre ellos:

- Son sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo
- Consisten en políticas, procedimientos, prácticas y estructuras organizacionales.
- Están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.

DS4.1 Marco de Trabajo de Continuidad de TIC

Desarrollar un marco de trabajo de continuidad de TIC para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida por la infraestructura y guiar el desarrollo de los planes de recuperación de desastres y de contingencias. El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TIC. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.

DS4.2 Planes de Continuidad de TIC

Desarrollar planes de continuidad de TIC con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TIC. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

DS4.3 Recursos Críticos de TIC

Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TIC, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.

DS4.4 Mantenimiento del Plan de Continuidad de TIC

Exhortar a la gerencia de TIC a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TIC se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.

DS4.5 Pruebas del Plan de Continuidad de TIC

Probar el plan de continuidad de TIC de forma regular para asegurar que los sistemas de TIC pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor.

DS4.6 Entrenamiento del Plan de Continuidad de TIC

Asegurarse de que todas las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.

DS4.7 Distribución del Plan de Continuidad de TIC

Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlos accesibles bajo cualquier escenario de desastre.

DS4.8 Recuperación y Reanudación de los Servicios de TIC

Planear las acciones a tomar durante el período en que TIC está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio

entienden los tiempos de recuperación de TIC y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio.

DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones

Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TIC críticos, necesarios para la recuperación de TIC y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el personal de TIC. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.

DS4.10 Revisión Post Reanudación

Una vez lograda una exitosa reanudación de las funciones de TIC después de un desastre, determinar si la gerencia de TIC ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

La Contraloría General de la República, en las Normas Técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), establece lo siguiente:

Continuidad de los servicios de TIC

La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.

> Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TIC según su criticidad. (*Contraloría General de la República, 2007)*

1.1.10. Procedimiento metodológico

El proceso para la aplicación de la planificación y el programa de Auditoría, según lo establecido en la institución donde se realizará el trabajo se hará de acuerdo con las siguientes etapas:

- Análisis preliminar
- Planificación del proyecto
- Ejecución del trabajo
- Informe con los hallazgos y sus recomendaciones

Análisis preliminar

El análisis preliminar consiste en las siguientes actividades:

- Determinar las fuentes de información referente al tema y al negocio.
- Identificar los lugares físicos o instalaciones a revisar.
- Comprensión del negocio.
- Comprensión del sistema principal (AB).

Planificación del proyecto

- Se debe de documentar la hoja de trabajo establecida por la unidad de AI.
- Realizar cuestionario de control interno y pruebas a realizar.
- Documentar el plan del estudio.

- Elaboración del informe de planificación.
- Elaborar programa de trabajo de acuerdo con cada una de las actividades, para ser realizadas en la etapa de ejecución.

Ejecución del trabajo

En esta etapa del proceso, se realizarán entrevistas con los dueños del proceso y se aplicarán las pruebas de cumplimiento y sustantivas si corresponden.

Informe con los hallazgos y sus recomendaciones

Luego de haber realizado el trabajo de ejecución, se elabora el informe, donde se detallen los resultados obtenidos y se comunica al personal de Tecnología de Información.

1.2. Contenido capitulario

El ordenamiento de los capítulos bajo el cual está organizado el presente trabajo se detalla a continuación:

Capítulo I

El capítulo I incluye el tema propuesto, la introducción, la delimitación del tema, la organización, la justificación del proyecto o trabajo, la finalidad del estudio, el objetivo general y los específicos, alcances, limitaciones y el procedimiento metodológico, así como el cronograma de las actividades.

Capítulo II

En el capítulo II se detalla el resultado de un diagnóstico, de la situación actual del tema seleccionado.

Capítulo III

En el capítulo III se realiza un análisis de los resultados obtenidos, posterior a la evaluación realizada del tema seleccionado.

Capítulo IV

En el capítulo IV se detallan las conclusiones y recomendaciones, con base en los resultados que se desprendieron de la evaluación realizada del tema seleccionado.

Anexos

Se adjuntan los anexos del trabajo realizado.

1.3. Referencias

Contraloría General de la República de Costa Rica, (2007) Normas Técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).

IT Governance Institute ®, (2007) Marco de Trabajo, Objetivos de Control, Directrices Gerenciales, Modelos de Madurez, COBIT® 4.1.

Superintendencia de Entidades Financieras (SUGEF), (2009) Objetivos y Funciones; Reglamento sobre la Gestión de la Tecnología de Información SUGEF 14-09.

1.4. Cronograma

Cronograma del Proyecto final.			
Nombre de tarea	**Duración**	**Comienzo**	**Fin**
El análisis preliminar consiste en las siguientes actividades:	**10 días**	**lun 05/01/15**	**vie 16/01/15**
Determinar las fuentes de información referente al tema y al negocio.	2 días	lun 05/01/15	mar 06/01/15
Identificar los lugares físicos o instalaciones a revisar	2 días	mié 07/01/15	jue 08/01/15
Comprensión del negocio	2 días	vie 09/01/15	lun 12/01/15
Comprensión del sistema principal (AB)	4 días	mar 13/01/15	vie 16/01/15
Planificación del proyecto.	**10 días**	**lun 12/01/15**	**vie 23/01/15**
Se debe de documentar la hoja de trabajo establecida por la unidad de AI.	2 días	lun 12/01/15	mar 13/01/15
Realizar cuestionario de control interno y pruebas a realizar	2 días	mié 14/01/15	jue 15/01/15
Documentar el plan del estudio.	2 días	vie 16/01/15	lun 19/01/15
Elaboración del informe de planificación.	2 días	mar 20/01/15	mié 21/01/15
Elaborar programa de trabajo de acuerdo con cada una de las actividades, para ser realizadas en la etapa de ejecución.	2 días	jue 22/01/15	vie 23/01/15
Ejecución del trabajo.	25 días	lun 26/01/15	vie 27/02/15
Realización de entrevistas a los dueños del proceso y se aplicarán las pruebas de cumplimiento y sustantivas si corresponden.			

Informe de hallazgos y recomendaciones.	15 días	lun 02/03/15	vie 20/03/15
Elaboración del informe, donde se detallen los resultados obtenidos del trabajo realizado. (Conclusiones y recomendaciones).			

CAPÍTULO II

2.1. Situación actual

La intención de este capítulo es presentar la situación actual referente al tema propuesto desde un enfoque general, posteriormente la situación correspondiente a Costa Rica, seguido por la situación de la entidades financieras costarricenses y por último, en la institución donde se desarrolla el trabajo profesional, con el fin del que el lector no solo se entere de las tendencias en relación con el tema, sino de la importancia relativa que se requiere para conocimiento del mismo.

2.2. Situación actual global

Durante mucho tiempo el planteamiento de las empresas frente a los riesgos consistía en disponer del mejor proceso de gestión de riesgos posible. Sin embargo, con el transcurso del tiempo este enfoque de riesgos de acuerdo con la continuidad del negocio se observa insuficiente en la gran parte de las empresas a nivel global.

Esto se debe a que la preocupación de la condición del directivo de la empresa, así como la de sus propietarios o accionistas, no está en que un servidor haya fallado, que falte la energía eléctrica o incluso que haya un terremoto. El foco de la atención está en cómo afectan estos acontecimientos a su negocio y en cuánto tiempo éste volverá a funcionar. Si lo crítico es “si el negocio deja de funcionar”, resulta imprescindible para cualquier empresa disponer de:

- Un plan de continuidad de servicio

- Un departamento/infraestructura de TIC con el máximo nivel de resiliencia

Existen factores que afectan a la continuidad del negocio tales como:

- Dependencia creciente de la tecnología
- Interdependencia de los proveedores
- Un acto individual puede tener consecuencias a nivel mundial. La competencia no perdona interrupciones prolongadas o, simplemente, apreciables por los usuarios
- Cualquier obligación legal o regulación sectorial

La creciente complejidad de los riesgos significa:

- Cambios constantes y cada vez más complejos
- Mundo cada vez más interdependiente
- Redefinición de la economía mundial
- Cambios demográficos

2.3. Situación actual en Costa Rica

A nivel de país existen instituciones del Estado donde se emite normativa que regula el proceso de continuidad.

En 2007, la Contraloría General de la Republica, por medio del oficio N-2-2007-CO-DFOE emite las Normas Técnicas para la Gestión y Control de la Tecnología de Información, donde en el capítulo I Normas de aplicación general, inciso 1.4.7 Continuidad de los servicios de TI indica:

> La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.

> Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad. (Contraloría General de la República, 2007)

En el 2009, la Superintendencia General de Entidades Financieras (SUGEF) emite el Acuerdo SUGEF 14-09 Reglamento sobre la gestión de la Tecnología de Información, donde su objeto es la definición de los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información, basado en COBIT 4.0, que corresponde a las mejores prácticas emitidas por ISACA en 2005 y a realizar una implementación gradual del marco de gestión.

Debido a la normativa emitida por la SUGEF, esta realizaría una evaluación de la implementación dos años después de publicado el acuerdo, de lo cual surgieron los resultados a nivel país, de las instituciones que son fiscalizadas por este ente y que se muestran en el gráfico 1.

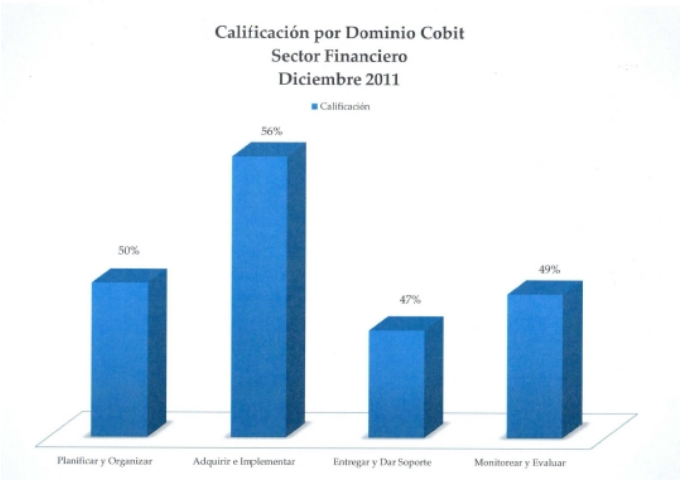

Gráfico 1: Calificación por Dominio COBIT del Sector Financiero.

Fuente: SUGEF (2011)

Los resultados de la Auditoría Externa de TIC en las entidades financieras, calificación por dominio COBIT Entregar y Dar Soporte, donde se encuentra incluido el proceso Garantizar la Continuidad del Servicio (DS4), obtiene una calificación de un 47% en las entidades financieras evaluadas. En el gráfico 2 se presentan los resultados de esos procesos, a diciembre del año 2011.

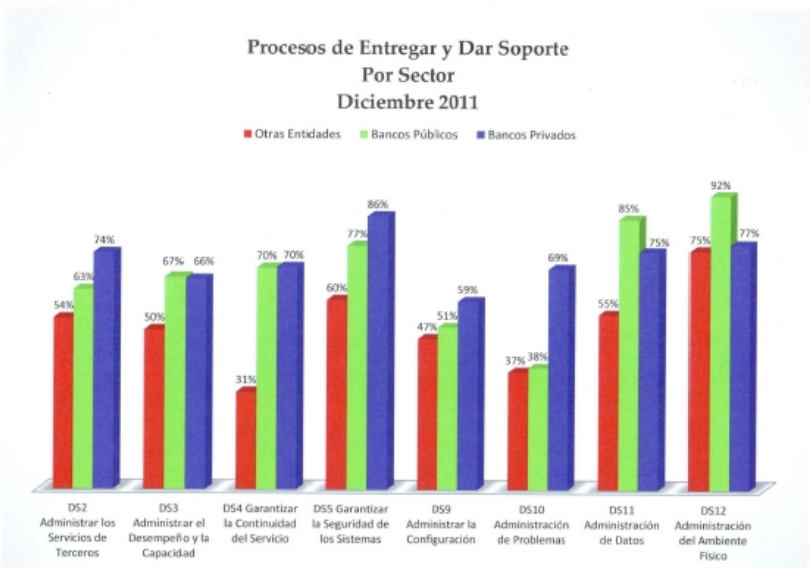

Gráfico 2: Calificación por proceso del Dominio Entregar y Dar Soporte del COBIT del Sector Financiero.

Fuente: SUGEF (2011)

2.4. Situación actual en la Institución

La institución donde se realiza el trabajo, es regulada por la Contraloría General de la Republica y Superintendencia General de Entidades Financieras (SUGEF). De acuerdo con las normas emitidas por ese último ente supervisor, la institución acordó implementar los 17 procesos obligatorios y posteriormente los 17 restantes de COBIT.

Luego ejecutar el plan de implementación, la SUGEF solicita que se realice una auditoría, para determinar la implementación de los procesos y su grado de madurez.

Aspectos que se consideraron para la evaluación por parte de la auditoría externa

1) Se deben de auditar los 17 procesos establecidos como obligatorios.
2) La institución debe considerar pertinente incluir procesos adicionales, puede realizarlos y comunicar el resultado obtenido.
3) Las pruebas deben de realizarse considerando los criterios de información y los recursos de TIC, definidos por el COBIT.

Procesos obligatorios a evaluar

Planear y Organizar.

PO1 Definir el plan estratégico de TIC.

PO3 Determinar la dirección tecnológica.

PO5 Administrar la inversión en TIC.

PO9 Evaluar y administrar riesgos de TIC.

PO10 Administrar proyectos.

Adquirir e Implementar

AI3 Adquirir y mantener la infraestructura tecnológica.

AI5 Adquirir recursos de TIC.

AI6 Administrar cambios.

Entregar y Dar Soporte

DS2 Administrar servicios de terceros.

DS3 Administrar desempeño y capacidad.

DS4 Garantizar la continuidad del servicio.

DS5 Garantizar la seguridad de los sistemas.

DS9 Administrar la configuración.

DS10 Administrar los problemas.

DS11 Administrar los datos.

DS12 Administrar el ambiente físico.

Monitorear y Evaluar

ME2 Monitorear y evaluar el control interno.

Luego de realización de la auditoría por parte de la auditoría externa, esta fue comunicada a la SUGEF. Con base en los resultados obtenidos, actualmente la institución se encuentra en un proceso de madurez de los 17 procesos obligatorios y la implementación de los 17 procesos restantes establecidos por el COBIT.

CAPÍTULO III

En este capítulo, se realizó un análisis preliminar del proceso de continuidad del negocio, para observar la situación global de la institución.

Al observar la situación de la entidad, se decidió ejecutar un plan de pruebas sustantivas para determinar el cumplimiento de la continuidad del sistema principal (AB).

3.1. Análisis preliminar del cumplimiento global sobre la continuidad a nivel de la institución.

N°	Garantizar la Continuidad del Servicio.-	Evaluaciones			Observaciones
		SI	NO	N/A	
	Marco de Referencia para la Continuidad de TI.				
1.	¿Se ha definido un marco de referencia para la continuidad de TI que apoye la gestión empresarial de la continuidad del negocio con un proceso consistente?	X			
	El objetivo de dicho marco es asistir en				
2.	1. La determinación de la resistencia a fallos y capacidad de recuperación requerida por la infraestructura.	X			
3.	2. Conducir el desarrollo de planes de recuperación de desastres y de contingencia de TI.	X			

N°	Garantizar la Continuidad del Servicio.-	Evaluaciones			Observaciones
	Dicho marco direcciona la estructura organizacional para la gestión de la continuidad cubriendo:				
4.	1. Roles, tareas y responsabilidades de los proveedores de servicio internos y externos, sus administradores y sus clientes.	**X**			
5.	2. Las reglas y las estructuras para documentar, probar y ejecutar los planes de recuperación de desastres y contingencia de TI.	**X**			
6.	El plan también considera aspectos tales como:				
7.	1. Identificación de recursos críticos.	**X**			
8.	2. Monitoreo y reporte de la disponibilidad de los recursos críticos.	**X**			
9.	3. Procesamiento alternativo.	**X**			
10.	4. Los principios de respaldo y recuperación.	**X**			
	Planes de Continuidad de TI				
11.	¿Existe un plan de continuidad de TI basado en el marco de referencia para la continuidad de TI?	**X**			
12.	¿Dicho plan está diseñado para reducir el impacto de una	**X**			

N°	Garantizar la Continuidad del Servicio.-	Evaluaciones			Observaciones
	interrupción importante en los principales procesos y funciones del negocio?				
13.	Para todos los servicios críticos de TI los planes de continuidad de TI direccionan requerimientos para:				
14.	1. Resistencia a fallos.	**X**			
15.	2. Procesamiento alternativo.	**X**			
16.	3. Capacidad de recuperación.	**X**			
17.	Los planes de continuidad de TI también cubren aspectos como:				
18.	1. Guías de uso.	**X**			
19.	2. Roles y responsabilidades.	**X**			
20.	3. Procedimientos.	**X**			
21.	4. Procesos de comunicación.	**X**			
22.	5. Enfoque de pruebas.	**X**			
	Recursos Críticos de TI				
	Para el establecimiento del plan de continuidad de TI respecto a los recursos de TI:				
23.	1. ¿Se encuentran identificados los ítems de mayor criticidad de manera que se construya resistencia a fallos y se establezcan prioridades en situaciones de recuperación?	**X**			

N°	Garantizar la Continuidad del Servicio.-	Evaluaciones			Observaciones
24.	2. ¿Se evitan las distracciones en recuperar ítems menos críticos?	**X**			
25.	3. ¿Se asegura la respuesta y recuperación en línea con las necesidades priorizadas del negocio?	**X**			
26.	4. ¿Se asegura que el costo se mantiene en un nivel aceptable?	**X**			
27.	5. ¿Se asegura el cumplimiento con requerimientos regulatorios y contractuales?	**X**			
28.	6. ¿Se considera la resistencia a fallos, los requerimientos de respuesta y recuperación para diferentes periodos (ejemplos de 1 a 4 horas, de 4 a 24 horas, más de 24 horas y los periodos críticos operacionales del negocio)?	**X**			
	Mantenimiento del Plan de Continuidad de TI				
	Existen y se ejecutan procedimientos para el control de cambios tales que:				
29.	1. Se asegura que el plan de continuidad de TI se mantiene actualizado.	**X**			
30.	2. Se asegura que el plan de continuidad refleje continuamente los requerimientos actuales del negocio.	**X**			
31.	¿Se comunican clara y oportunamente los cambios en los	**X**			

N°	Garantizar la Continuidad del Servicio.-	Evaluaciones			Observaciones
	procedimientos y las responsabilidades del Plan de Continuidad de TI?				
	Pruebas del Plan de Continuidad				
32.	¿Se realizan pruebas al plan de continuidad de TI sobre una base regular?	**X**			
33.	¿Dichas pruebas aseguran que los sistemas de TI efectivamente se puedan recuperar, que las deficiencias son atendidas y que el plan sigue vigente?	**X**			
	Para realizar las pruebas se toma en cuenta:				
34.	1. Preparación adecuada.	**X**			
35.	2. La documentación necesaria.	**X**			
36.	3. Reporte de los resultados de las pruebas.	**X**			
37.	4. Implementación de planes de acción (según los resultados).	**X**			
	El alcance de las pruebas debe considerar:				
38.	1. Recuperación de aplicaciones individuales.	**X**			
39.	2. Escenarios de pruebas integradas.	**X**			
40.	3. Pruebas de punta a punta.	**X**			

N°	Garantizar la Continuidad del Servicio.-	Evaluaciones			Observaciones
41.	4. Pruebas integradas con el proveedor	**X**			
	Capacitación del Plan de Continuidad de TI				
42.	¿Se capacitan sobre una base periódica todas las partes involucradas en el Plan de Continuidad de TI?		**X**		A las capacitaciones no han sido de forma periódica.
43.	¿Dicha capacitación considera los procedimientos, roles y responsabilidades en caso de un incidente o desastre?		**X**		
44.	¿Se verifica y mejora la capacitación tomando en cuenta los resultados de las pruebas de contingencia?		**X**		
	Distribución del Plan de Continuidad de TI				
45.	¿Existe una estrategia administrada de distribución del plan de continuidad de TI?	**X**			
46.	¿Dicha estrategia asegura que los planes sean propia y seguramente distribuidos?	**X**			
47.	¿La estrategia también asegura que los planes se encuentren disponibles para las partes involucradas, autorizadas y apropiadas, en el momento y lugar que lo necesiten?	**X**			

N°	Garantizar la Continuidad del Servicio.-	Evaluaciones			Observaciones
48.	¿Los planes son accesibles bajo cualquier escenario de desastre?	**X**			
	Recuperación y Reanudación de los Servicios de TI				
49.	¿Se planean las acciones que se deben tomar para el periodo cuando TI se está recuperando y reanudando los servicios?	**X**			
50.	¿Dichas acciones incluyen la activación de sitios de respaldo, la iniciación del procesamiento alternativo, la comunicación con los clientes y las partes involucradas y procedimientos de reanudación?	**X**			
51.	¿El negocio entiende los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio?	**X**			
	Almacenamiento Externo de los Respaldos				
52.	¿Se almacena en un sitio externo los medios de respaldo críticos, la documentación y otros recursos de TI necesarios para los planes de recuperación de TI y de continuidad del negocio?	**X**			
53.	¿La necesidad de contenido de los respaldos se determina en colaboración con los dueños de	**X**			

N°	Garantizar la Continuidad del Servicio.-	Evaluaciones			Observaciones
	los procesos del negocio y el personal de TI?				
54.	¿La administración del sitio de almacenamiento externo debe apegarse a la política de clasificación de la información y de las prácticas de almacenamiento de la entidad?	**X**			
55.	¿Los contratos de almacenamiento externo se revisan periódicamente al menos una vez al año, tanto en contenido, como protección ambiental y seguridad?	**X**			
56.	¿Se asegura la compatibilidad del hardware y el software para restaurar los datos archivados?	**X**			
57.	¿Periódicamente se prueban y refrescan los datos archivados?	**X**			
	Revisión Post-Reanudación				
58.	¿La Gerencia de TI ha establecido procedimientos para que, después de una reanudación exitosa de la función de TI luego de un desastre, se valore lo adecuado del plan y se actualice según se necesite?	**X**			
	NIVEL DE MADUREZ				
	Inicial				
59.	¿La administración concentra la continuidad del servicio tanto en	**X**			

N°	Garantizar la Continuidad del Servicio.-	Evaluaciones			Observaciones
	los recursos de infraestructura como en los servicios de TI?				
60.	¿Lo usuarios no implementan soluciones temporales debido a interrupciones de los servicios?	**X**			
61.	¿La respuesta a las principales interrupciones de TI son proactivas y preparadas?	**X**			
62.	¿Las interrupciones planeadas se programan considerando tanto las necesidades de TI como los requerimientos del negocio?	**X**			
	Repetible pero intuitivo				
63.	¿Están definidas las responsabilidades en el servicio continuo?	**X**			
64.	¿Los enfoques para asegurar la continuidad están consolidados?	**X**			
65.	¿Existen reportes sobre la disponibilidad de los servicios?	**X**			
66.	¿Existe un plan de continuidad de TI documentado?	**X**			
67.	¿Existe un inventario confiable de los sistemas y componentes críticos?	**X**			
68.	¿Se han establecido prácticas para un servicio continuo?	**X**			
	Proceso definido				

N°	Garantizar la Continuidad del Servicio.-	Evaluaciones			Observaciones
69.	¿Las responsabilidades por la administración del servicio continuo, por el planeamiento y prueba del servicio continuo están claramente definidas?	**X**			
70.	¿El plan de continuidad de TI está documentado y se basa tanto en los sistemas críticos como en el impacto en el negocio?	**X**			En este caso en el grupo de sistemas críticos se encuentra el sistema en valuación del sistema (AB)
71.	¿Existe un reporte periódico sobre pruebas del servicio continuo?	**X**			
72.	¿Se siguen estándares y se recibe capacitación para hacer frente a los principales incidentes y desastres?		**X**		Si se cuenta con estándares, no obstante falta más capacitación.
73.	¿La Gerencia de T.I. comunica regularmente la necesidad de planear el aseguramiento de un servicio continuo?	**X**			
74.	¿Se aplican componentes de alta disponibilidad y sistemas redundantes?	**X**			
75.	¿Se mantiene un inventario de los sistemas y componentes críticos?	**X**			
	Administrado y Medible				
76.	¿Las responsabilidades y estándares para el servicio continuo se hacen cumplir?		**X**		A la fecha no se encuentra en este nivel de madurez.

N°	Garantizar la Continuidad del Servicio.-	Evaluaciones			Observaciones
77.	¿La responsabilidad de mantener el plan de servicio continuo se encuentra asignada?		**X**		
	La actividades de mantenimiento se basan en:				
78.	1. Resultados de pruebas del servicio continuo.		**X**		
79.	2. Buenas prácticas internas.		**X**		
80.	3. Cambios en el ambiente de TI y del negocio.		**X**		
81.	¿Se obtiene, analiza y reporta información estructurada acerca del servicio continuo y se actúa de acuerdo a esta?		**X**		
82.	¿Se provee capacitación formal y obligatoria sobre los procesos de servicio continuo?		**X**		
83.	¿Se han implementado de manera regular mejores prácticas de disponibilidad de sistemas?		**X**		
84.	¿Las prácticas de disponibilidad y el planeamiento de servicio continuo se influencian mutuamente?		**X**		
85.	¿Se clasifican los incidentes de discontinuidad y la ruta de escalamiento es bien conocida por todos los involucrados?		**X**		
86.	¿Se han definido y aceptado indicadores clave de desempeño (KPIs) así como indicadores clave		**X**		

N°	Garantizar la Continuidad del Servicio.-	Evaluaciones			Observaciones
	de meta (KGIs) para el servicio continuo?				
	Optimizado				
87.	¿Los procesos de servicio continuo se encuentran integrados y toman en cuenta benchmarking y las mejores prácticas externas?		**X**		A la fecha no se encuentra en este nivel de madurez.
88.	¿El plan de continuidad de TI se integra con el plan de continuidad del negocio y se actualiza periódicamente?		**X**		
89.	¿Los requerimientos para asegurar el servicio continuo se encuentran respaldados por los proveedores?		**X**		
90.	¿Se realizan pruebas globales al plan de continuidad de TI, y los resultados son tomados para actualizar el plan?		**X**		
91.	¿Se realiza mejora continua del proceso a través de la recolección y análisis de datos?		**X**		
92.	¿Las prácticas de disponibilidad y planeamiento del servicio continuo se encuentran completamente alineados?		**X**		
93.	¿La Gerencia de T.I. se asegura que no puedan ocurrir desastres o incidentes importantes debido a puntos únicos de falla?		**X**		

N°	Garantizar la Continuidad del Servicio.-	Evaluaciones			Observaciones
94.	¿Las prácticas de escalamiento son entendidas y se hacen cumplir?		**X**		
95.	¿El logro de los KGIs y KPIs del servicio continuo se mide de manera sistemática?		**X**		
96.	¿La Gerencia de T.I. realiza ajustes al planeamiento del servicio continuo en respuesta a los resultados de los KGIs y KPIs?		**X**		

3.2. Procedimiento de pruebas que fueron aplicadas, para determinar la continuidad del sistema en revisión (AB).

Se realizaron las pruebas detalladas en el programa, la documentación de la evidencia se encuentra el anexo 1.

N°	Procedimientos por aplicar	Ref. RT	Observaciones
1.	Asegúrese que TI cuenta con un registro de mantenimiento del servidor principal del sistema en estudio.	Prueba N. 1	Satisfactoria.
2.	Verificar si el plan considera la priorización de las aplicaciones, con respecto a los tiempos de recuperación y retorno	Prueba N. 2	Satisfactoria.
3.	Investigue si se contaba y se cuenta con monitoreo del servidor donde se encuentra instalado el sistema.	Prueba N. 3	No satisfactoria.
4.	Verificar y validar si se realizan pruebas al plan de continuidad del sistema, en forma	Prueba N. 4	No satisfactoria.

N°	Procedimientos por aplicar	Ref. RT	Observaciones
	regular para asegurar que el sistema pueda recuperarse en forma efectiva.		
5.	Asegúrese de la existencia de documentación y reporte de resultados de las pruebas y planes de acción según esos resultados.	Prueba N. 5	No satisfactoria.
6.	Verificar y validar si en las pruebas de recuperación consideran - Aplicación individual - Escenarios de pruebas integrales - Pruebas de punta a punta - Pruebas integradas con el proveedor	Prueba N. 6	Satisfactoria.
7.	Revise si las pruebas contemplan los elementos críticos y simulan las condiciones de operación más parecida a las normas de operación normal del sistema en revisión.	Prueba N. 7	Satisfactoria.
8.	Entrenamiento: Verificar la formación (entrenamiento) y el conocimiento de los usuarios y el personal de los servicios de información en cuanto a funciones, tareas, roles y responsabilidades dentro del plan.	Prueba N. 8	No satisfactoria.
9.	Recuperación y reanudación de los servicios de TI, donde se incluye el sistema en revisión: Asegurarse que el plan de acción contempla: -La activación de sitios de respaldo. -Inicio de procesamiento alternativo -La comunicación a clientes -La elaboración de los procedimientos de reanudación.	Prueba N. 9	Satisfactoria.

N°	Procedimientos por aplicar	Ref. RT	Observaciones
10.	Revise si los encargados del sistema verifica que los acuerdos con sitios externos son evaluados periódicamente al menos una vez al año, respecto al contenido, la protección ambiental y la seguridad.	Prueba N. 10	Satisfactoria.

CAPÍTULO IV

Conclusiones y Recomendaciones

Conclusiones

- La institución adoptó la implementación de los 34 procesos solicitados por la SUGEF, según acuerdo 14-09, dentro de los cuales se incluye el proceso DS4 Garantizar la Continuidad de los Servicios, en este en particular el sistema en revisión (AB).

- A nivel institucional, existe un Plan de Continuidad del Negocio debidamente documentado y aprobado por el órgano competente.

- Se determinó la implementación del proceso DS4 en el sistema (AB), con los controles establecidos para disminuir el riesgo y su impacto al negocio.

- Se concluye a satisfacción, ya que existe un plan definido, donde se establece la priorización de la aplicación (AB), con respecto al tiempo establecido para su recuperación.

- De acuerdo con la revisión realizada, se determinó que se efectuaron las pruebas, en las cuales se contemplaron elementos críticos y la simulación de funcionalidad similar al sistema en operación, no obstante falta que dichas pruebas sean periódicas.

- Se concluye que el plan de acción contempla las actividades en el proceso de recuperación y reanudación del servicio, considerando aspectos como la activación de sitios de respaldo, inicio de procesamiento alternativo, comunicación a clientes y elaboración de procedimientos de reanudación.

- A pesar de que existe documentación de la implementación del Plan, se debe realizar mayor capacitación al personal para crear conocimiento en cuanto a sus tareas y responsabilidades.

- En cuanto al nivel de madurez, de acuerdo con la revisión se determinó que se encuentra en un nivel 3 definido, ya que la responsabilidad sobre la administración de la continuidad del servicio es clara, las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas, el plan de continuidad de TI está documentado y basado en la criticidad de los sistemas y el impacto al negocio. No obstante se han realizado pruebas, estas no son periódicas.

Recomendaciones

- Implementar en los planes, el monitoreo y reporte de disponibilidad del proceso en revisión, para aplicar acciones preventivas o anticipadas a la ocurrencia de un evento en el sistema (AB), para garantizar el mínimo impacto en el negocio, con base en las pruebas realizadas.

- Elaborar la respectiva programación de pruebas periódicas para los planes de continuidad del sistema (AB) y establecer el tipo de prueba a ejecutar, para

asegurarse la disponibilidad del sistema y reducir el impacto en el servicio y por ende en el negocio.

- Implementar que las pruebas del plan de contingencia donde se incluye el sistema (AB), se ejecuten en su totalidad y sean constantes.

- Con base en los resultados obtenidos de las pruebas efectuadas al plan de continuidad (sistema AB), capacitar al personal para crear conocimiento en cuanto a sus tareas y responsabilidades dentro del proceso de continuidad para la ejecución del plan establecido para este sistema.

Anexo 1

Las pruebas que se aplicaron, para determinar el cumplimiento del proceso de continuidad en el sistema (AB).

Prueba #1

REGISTRO DE TRABAJO

ESTUDIO: Evaluación para Garantizar la Continuidad del Servicio (DS4) del sistema (AB).

ASUNTO: Revisión del Sistemas (AB)

PROCEDIMIENTO RELACIONADO: 1. Asegúrese que se cuenta con un registro de mantenimiento del servidor principal del sistema en estudio.

Detalle:

De acuerdo con la revisión realizada, se observa documentación de las bitácoras, en la que se registra el mantenimiento principal de los servidores, donde se encuentra instalado el sistema en revisión.

Conclusión:

Según lo observado y de acuerdo con la documentación existente, se concluye que dichos registros se encuentran a satisfacción, con los controles que fueron establecidos.

Hecho por: Ana Eligia Ortega Navarro.

Fecha: 29 de enero del 2015

Prueba #2

REGISTRO DE TRABAJO

ESTUDIO: Evaluación para Garantizar la Continuidad del Servicio (DS4) del sistema (AB).

ASUNTO: Revisión del Sistemas (AB)

PROCEDIMIENTO RELACIONADO: 2. Verificar si el plan considera la priorización de las aplicaciones, con respecto a los tiempos de recuperación y retorno.

Detalle:

En el Plan de Continuidad de Tecnología de Información, existen puntos donde se establece la priorización de recuperación, lo indicado es cómo se espera recuperar la infraestructura física y el sistema de información de acuerdo con la priorización con los RTO (Objetivo de Tiempo de Recuperación) de cada sistema.

Cabe señalar que el sistema en revisión es uno de los sistemas con mayor priorización de acuerdo con el objetivo de tiempo de recuperación establecido por la institución.

Conclusión:

Se concluye a satisfacción, ya que existe un plan definido, donde se establece la priorización de las aplicaciones, con respecto al tiempo establecido para su recuperación, según lo definido por la institución.

Hecho por: Ana Eligia Ortega Navarro.

Fecha: 26 de febrero del 2015

Prueba # 3

REGISTRO DE TRABAJO

ESTUDIO: Evaluación para Garantizar la Continuidad del Servicio (DS4) del sistema (AB).

ASUNTO: Revisión del Sistemas (AB)

PROCEDIMIENTO RELACIONADO: 3. Investigue si se contaba y se cuenta con monitoreo del servidor donde se encuentra instado el sistema.

Detalle:

Dentro del Plan de Continuidad de Tecnología de Información, no se encuentra implementado el monitoreo y reporte de disponibilidad de los procesos.

El plan de contingencia general de Tecnología de Información, contiene en la metodología de evaluación de riesgo, los procesos críticos o prioritarios en cuanto a la contingencia se refiere; no obstante, el monitoreo y el reporte de disponibilidad no se identifican en el plan.

De acuerdo con lo establecido en COBIT 4.1.

DS4.2 Planes de Continuidad de TI: Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

Por lo tanto, se debe desarrollar un marco de trabajo de continuidad de Tecnología de Información, para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización.

El plan debe también considerar puntos tales como la identificación de recursos, el monitoreo y reporte de la disponibilidad de los recursos, el procesamiento alternativo y los principios de respaldo y recuperación.

El no tener controlados los procesos críticos, ocasionaría que los planes de contingencia no sean efectivos y eficientes a la hora de ponerlos en marcha para minimizar el impacto ocurrido en determinado evento.

La situación anterior puede conllevar al riesgo de no garantizar la continuidad del negocio en un tiempo razonable, después de ocurrido un evento, lo cual ocasionaría pérdida de imagen, de información y pérdidas económicas.

Recomendación:

Implementar en los planes de Tecnología de Información, el monitoreo y reporte de disponibilidad del proceso en revisión, para aplicar acciones preventivas o anticipadas a la ocurrencia de un evento en el sistema (AB), para garantizar el mínimo impacto en el negocio.

Hecho por: Ana Eligia Ortega Navarro.

Fecha: 29 de febrero del 2015

Prueba # 4

REGISTRO DE TRABAJO

ESTUDIO: Evaluación para Garantizar la Continuidad del Servicio (DS4) del sistema (AB).

ASUNTO: Revisión del Sistemas (AB)

PROCEDIMIENTO RELACIONADO: 4. Verificar y validar si se realizan pruebas al plan de continuidad del sistema (AB), en forma regular para asegurar que el sistema pueda recuperarse en forma efectiva.

Detalle:

Las directrices generales del proceso Garantizar la Continuidad del Servicio, normadas por la institución, establecen diferentes tipos de pruebas a los planes de continuidad:

1- Pruebas de escritorio
2- Pruebas individuales
3- Pruebas por componentes
4- Pruebas integradas
5- Pruebas de punta a punta y
6- Pruebas con los proveedores

Según se observó, actualmente se está finalizando la ejecución de la primera etapa, pruebas de escritorio. Existe un documento donde se muestran las fechas en que se han realizado pruebas de escritorio al sistema en revisión; no obstante, a la fecha no se contaba con la programación de pruebas para el siguiente periodo y además el tipo de prueba que se aplicará al sistema (AB).

De acuerdo con lo establecido en COBIT 4.1

DS4.5 Pruebas del Plan de Continuidad de TI. Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor.

Además, no se evidenció la definición de un plazo máximo establecido, en el cual se deba tener preparado el plan de pruebas aplicable para el siguiente periodo.

No contar con un plan actualizado de pruebas aplicable a la infraestructura crítica de la institución, incrementa el riesgo de la continuidad del servicio, al no conocer la forma en que se desarrollará el plan de contingencia definido y si el mismo asegura que el sistema en revisión pueda recuperarse en forma efectiva.

Recomendaciones:

Elaborar la respectiva programación de pruebas para los planes de continuidad del sistema (AB) y establecer el tipo de prueba a ejecutar, para asegurarse la disponibilidad del sistema y reducir el impacto al negocio.

Hecho por: Ana Eligia Ortega Navarro.

Fecha: 25 de febrero del 2015

Prueba # 5

REGISTRO DE TRABAJO

ESTUDIO: Evaluación para Garantizar la Continuidad del Servicio (DS4) del sistema (AB).

ASUNTO: Revisión del Sistemas (AB)

PROCEDIMIENTO RELACIONADO: 5. Asegúrese de la existencia de documentación y reporte de resultados de las pruebas y planes de acción según esos resultados.

Detalle:

Según la verificación realizada, no se efectúa la totalidad de las pruebas del plan de continuidad de TI en forma regular, tampoco son atendidas en su totalidad las deficiencias para que el plan permanezca aplicable y además, no se cuenta con un plan de acción basado en los resultados de las pruebas.

Es de gran valor realizar pruebas del Plan de Continuidad de Tecnología de Información de forma regular, para asegurar que los sistemas pueden ser recuperados de manera efectiva, que las deficiencias sean atendidas y que el plan permanezca aplicable. Por lo tanto, se requiere una preparación cuidadosa, debidamente documentada basada en el reporte de los resultados de las pruebas, de acuerdo con los resultados, la implementación de los planes de acción a seguir.

De acuerdo a lo establecido en COBIT 4.1

DS4.5 *Pruebas del Plan de Continuidad de TI. Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una*

preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor.

El objetivo principal de aplicarlo es evaluar si los planes son capaces de proporcionar el nivel deseado de soporte de los principales procesos en caso de posibles fallas y además permite validar si un plan puede llevarse a cabo dentro de un período de tiempo dado, proporcionando la oportunidad de hacer los ajustes necesarios al plan y al ambiente dentro del cual el plan es probado.

Dentro de los aspectos a considerar en el plan de pruebas están los tipos, las fases, los pasos y documentación y análisis de los resultados.

Además, se debe documentar detalladamente cada fase de las pruebas, observaciones, problemas y soluciones, esto para realizar un análisis de fortalezas y debilidades del plan.

La situación descrita conlleva el riesgo de no contar con un plan de continuidad de TI debidamente probado, ocasionando pérdida de confiabilidad en la disponibilidad y efectividad de los servicios y del proceso en este caso al sistema en revisión (AB).

Recomendación:

Implementar que las pruebas del plan de contingencia donde se incluye el sistema (AB), se ejecuten en su totalidad y se defina el alcance requerido.

Hecho por: Ana Eligia Ortega Navarro.

Fecha: 23 de febrero del 2015

Prueba # 6

REGISTRO DE TRABAJO

ESTUDIO: Evaluación para Garantizar la Continuidad del Servicio (DS4) del sistema (AB).

ASUNTO: Revisión del Sistemas (AB)

PROCEDIMIENTO RELACIONADO: 6. Verificar y validar si en las pruebas de recuperación consideran:

- Aplicación individual
- Escenarios de pruebas integrales
- Pruebas de punta a punta
- Pruebas integradas con el proveedor

Detalle:

Según las Directrices Generales del Proceso Garantizar la Continuidad del Servicio, se establece en los puntos correspondientes, que al menos una vez al año se probará el plan de continuidad. Así como que las pruebas se ejecutarán de acuerdo al nivel de madurez que la organización lo requiera para el sistema en evaluación (AB) y que estas pruebas considerarán pruebas de escritorio, individuales, por componente, integradas, de punta a punta y con los proveedores.

Conclusión:

En el Informe de pruebas de continuidad de TI, en algunas pruebas realizadas, se consideró al proveedor, tal como en pruebas a los sistemas, como parte del proceso de pruebas de escritorio.

Hecho por: Ana Eligia Ortega Navarro.

Fecha: 23 de febrero del 2015

Prueba # 7

REGISTRO DE TRABAJO

ESTUDIO: Evaluación para Garantizar la Continuidad del Servicio (DS4) del sistema (AB).

ASUNTO: Revisión del Sistemas (AB)

PROCEDIMIENTO RELACIONADO: 7. Revise si las pruebas contemplan los elementos críticos y simulan las condiciones de operación más parecidas a las normas de operación normal del sistema en revisión.

Detalle:

Según el Plan de Continuidad de Tecnología de Información, se establecen los componentes de la infraestructura crítica y también se estableció la Infraestructura crítica de TI; en el Informe de pruebas de continuidad de Tecnología de Información, se indican los resultados sobre las pruebas de escritorio de esa infraestructura con instructivos para cada componente crítico y similar a la operación del sistema en revisión de este trabajo.

Conclusión:

De acuerdo con la revisión realizada, se determinó que se realizaron las pruebas, en las cuales se contemplaron elementos críticos y la simulación de funcionalidad similar al sistema en operación.

Hecho por: Ana Eligia Ortega Navarro.

Fecha: 23 de febrero del 2015

Prueba # 8

REGISTRO DE TRABAJO

ESTUDIO: Evaluación para Garantizar la Continuidad del Servicio (DS4) del sistema (AB).

ASUNTO: Revisión del Sistemas (AB)

PROCEDIMIENTO RELACIONADO: 8. Entrenamiento: verificar la formación (entrenamiento) y el conocimiento de los usuarios y el personal de los servicios de información en cuanto a funciones, tareas, roles y responsabilidades dentro del plan.

Detalle:

Según se determinó en la revisión realizada y con verificación por parte del jefe del área de Tecnología de Información, las capacitaciones y entrenamiento al personal, sobre las acciones contingentes, actualmente no se están llevando a cabo.

El área de Tecnología de Información debe asegurarse de que todas las partes involucradas en el plan de contingencia, reciban sesiones de habilitación de forma regular respecto a los procesos, sus roles y responsabilidades en caso de incidente o desastre. Además debe de verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas realizadas al plan de contingencia donde se encuentra la aplicación en revisión.

De acuerdo con lo establecido en COBIT 4.1

DS4.6 Entrenamiento del Plan de Continuidad de TI. Asegurarse de que todas las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.

La administración de la continuidad debe asegurar que todas las personas involucradas, cuenten con la capacidad de respuesta oportuna a seguir, en caso de una interrupción de los servicios.

La situación descrita conlleva el riesgo de que si el personal, no se encuentra capacitado, para recuperar las actividades del negocio en tiempo mínimo, podría ocasionar pérdidas económicas y de imagen.

Recomendación:

Con base en los resultados obtenidos de las pruebas efectuadas al Plan de Continuidad de la Tecnología de Información (sistema AB), capacitar al personal para crear conocimiento en cuanto a sus tareas y responsabilidades dentro del Plan.

Hecho por: Ana Eligia Ortega Navarro.

Fecha: 23 de febrero del 2015

Prueba # 9

REGISTRO DE TRABAJO

ESTUDIO: Evaluación para Garantizar la Continuidad del Servicio (DS4) del sistema (AB).

ASUNTO: Revisión del Sistemas (AB)

PROCEDIMIENTO RELACIONADO: 9. Recuperación y reanudación de los servicios de TI:

Asegurarse que el plan de acción contempla:
-La activación de sitios de respaldo.
-Inicio de procesamiento alternativo
-La comunicación a clientes
-La elaboración de los procedimientos de reanudación.

Detalle:

De acuerdo con la verificación realizada en el plan de acción, con el que cuenta la institución, se encuentra el sistema (AB), donde entre los puntos a contemplar para asegurarse la efectividad del Plan de acción, se observó:

- La activación de sitios de respaldo.
-Inicio de procesamiento alternativo
-La comunicación a clientes
-La elaboración de los procedimientos de reanudación.

Esto aspectos además están contemplados el Plan de pruebas que fue desarrollado, tal y como lo tiene establecido COBIT 4.1.

Conclusión:

Se concluye que el plan de acción contempla las actividades en el proceso de recuperación

y reanudación del servicio, considerando aspectos como la activación de sitios de respaldo, inicio de procesamiento alternativo, comunicación a clientes y elaboración de procedimientos de reanudación.

Hecho por: Ana Eligia Ortega Navarro.

Fecha: 23 de febrero del 2015

Prueba # 10

REGISTRO DE TRABAJO

ESTUDIO: Evaluación para Garantizar la Continuidad del Servicio (DS4) del sistema (AB).

ASUNTO: Revisión del Sistemas (AB)

PROCEDIMIENTO RELACIONADO: 10. Revise si los encargados del sistema verifican que los acuerdos con sitios externos son evaluados periódicamente al menos una vez al año, respecto al contenido, la protección ambiental y la seguridad.

Detalle:

La institución donde se realizó la evaluación del sistema (AB), cuenta con un almacenamiento en un sitio externo, donde permite almacenar los códigos fuentes y bases de datos, donde se incluye este sistema.

Para el almacenamiento externo de información se utiliza la librería robótica. Además, se identificó evidencia que permite establecer que los sitios externos son evaluados periódicamente respecto al contenido, protección ambiental y seguridad, así como la documentación (dentro del DS4) que regule la realización de estas funciones.

Es importante mencionar que se cuenta con un contrato de acuerdos de servicio (SLA).

Conclusión:

Se concluye que existen acuerdos de servicios para el almacenamiento externo y que estos son revisados una vez al año de acuerdo con lo estipulado en el contrato.

Hecho por: Ana Eligia Ortega Navarro.

Fecha: 23 de febrero del 2015