Banco Hipotecario de la Vivienda

Informe Final TI-OP-001-2016

AUDITORÍA SOBRE EL PLAN DE CONTINUIDAD DE LAS UNIDADES OPERATIVAS DEL BANCO

19/07/2016

INDICE

A. RESUMEN EJECUTIVO

En esta auditoria se examinó lo adecuado y completo del Plan de Continuidad de Negocio establecido por la Administración Activa para operar en ausencia de los principales recursos tecnológicos del Banco.

Dentro de los aspectos de mejora más relevantes que se localizaron en la revisión, fueron ciertas deficiencias de control sobre el documento existente del Plan de Continuidad, con la observación de que el mismo al momento de la auditoría estaba en proceso de desarrollo, por lo que los hallazgos indicados en el informe así como sus recomendaciones, pueden mejorar considerablemente los puntos de control deficientes.

Otra debilidad importante fue la relacionada con la no inclusión de las Entidades Autorizadas en ninguno de los procesos de desarrollo, aplicación y prueba de la continuidad de las operaciones que tengan relación con el Bono Familiar de Vivienda, esto en una posible ausencia de los principales insumos ofrecidos por el Departamento de Tecnologías de Información, siendo los más relevantes en este caso los sistemas de información o sus respectivas bases de datos.

Como parte adecuada del recurso humano involucrado directamente en la administración y el mantenimiento del Plan de Continuidad, se determinó que no se aplica un control que unifique las responsabilidades definidas en ese Plan contra las funciones del Manual de Puestos institucional, limitando un correcto seguimiento sobre el cumplimiento real de los puestos involucrados.

El Banco en la actualidad cuenta con una serie de servicios que son subcontratados a terceros tales como Seguridad, Limpieza, Mantenimientos de Aires Acondicionados, Planta Eléctrica, Unidades de Poder Ininterrumpido y otros detallados en el cuerpo del informe. De estos servicios se determinó que no han sido valorados para ser incluidos en el Plan de Continuidad, a pesar de que algunos podrían ser críticos para la operativa institucional.

Tomando en cuenta que el Plan de Continuidad tiene una relación directa con los insumos tecnológicos que en una eventualidad no podrían ser ofrecidos por el Departamento de Tecnologías de Información, se encontró como relevante que la jefatura del Departamento de TI no ha sido involucrada como parte de la Comisión de Continuidad de Negocio para el desarrollo del Plan, así como para la definición de su alcance y las diferentes estrategias y protocolos previstos.

Por último, se encontraron debilidades relacionadas con los insumos tecnológicos respaldados en el Centro de Procesamiento Alterno y sobre la normativa para su puesta en ejecución. Al igual que los temas anteriores, se pueden ver con más detalle en la sección de Resultados de este informe.

BANCO HIPOTECARIO DE LA VIVIENDA
AUDITORÍA INTERNA
Informe Final Nº TI-OP-001-2016
18 de Julio del 2016

AUDITORÍA SOBRE EL PLAN DE CONTINUIDAD DE LAS UNIDADES OPERATIVAS DEL BANCO

1. INTRODUCCIÓN

1.1 Justificación de la auditoría

Este estudio forma parte del Plan Anual de Trabajo de esta Auditoría Interna para el año 2016 y está fundamentado en el Artículo 31 de la Ley 7052 del Sistema Financiero Nacional para la Vivienda, en el Artículo 22 de la Ley 8292, Ley General de Control Interno, en los cuales se establece que la Auditoría Interna deberá velar y fiscalizar el uso adecuado de los recursos del BANHVI.

1.2 Objetivo

Evaluar lo adecuado y completo del Plan de Continuidad Institucional establecido por la Administración para operar en ausencia de los principales recursos tecnológicos del Banco.

1.3 Alcance

El estudio abarcó la normativa, información y procesos operativos vigentes al 30 de Abril del 2016 relacionados con los planes de continuidad definidos por la Administración Activa, exceptuando de este apartado el Plan de Continuidad de Tecnologías de Información, puesto que además de ser visiones distintas, son administrados por unidades diferentes.

1.4 Metodología de Trabajo

Se aplicó la metodología establecida en el Manual para el ejercicio de la práctica de la Auditoría Interna, y el Procedimiento de Auditoría, emitido y aprobado en el 2012, por el Auditor Interno. Además, se aplicó el Manual de Normas Generales de Auditoría para el Sector Público emitido por la División de Fiscalización Operativa y Evaluativa. Otras normas y estándares utilizados fueron:

- ✓ la Norma de Gestión de Continuidad de Negocio INTE 01-01-18:2011 Parte I
- ✓ el Reglamento sobre Gestión del Riesgo Operativo, SUGEF 18-16

- ✓ las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información N-2-2007-CO-DFOE
- ✓ el Manual de Normas de control interno para el Sector Público N-2-2009-CO-DFOE
- ✓ la versión 4.0 del estándar COBIT

Además, se aplicaron técnicas de auditoría comúnmente aceptadas como entrevistas al personal clave involucrado directamente en su ejecución, revisión documental de la gestión administrativa y visitas de campo para la verificación del control interno.

Específicamente se ejecutaron entrevistas con el funcionario responsable del desarrollo del Plan de Continuidad de Negocio, así como con ciertos funcionarios del Departamento de TI claves dentro del proceso de continuidad tecnológica. Adicional se evaluó la existencia y razonabilidad de la documentación formal, referente a la continuidad de las operaciones del Banco.

Los resultados de las pruebas ejecutadas y demás documentos que respaldan el trabajo realizado, se mantienen como papeles de trabajo en el expediente electrónico de la Auditoria Interna. Las deficiencias detectadas, tanto en aspectos de control interno como operativas, de la presente revisión, se detallan en el aparte de Resultados.

Por último se aclara que en este informe ya se consideran las observaciones y comentarios correspondientes a las reuniones de cierre efectuadas con las áreas involucradas, así como lo indicado en el memorando UR-ME-041-2016 del 06 de Julio del 2016.

2. RESULTADOS DE LA EVALUACIÓN

2.1 Plan de Continuidad de Negocio

En la Auditoría se determinó la existencia de un Plan de Continuidad de Negocio, el cual cabe destacar que se encontraba en proceso de ejecución. No obstante y tomando en cuenta las posibles mejoras que se le puedan ir agregando al documento y a los procesos de continuidad previstos, seguidamente se detallan algunos aspectos localizados en la revisión que deben ser considerados por la Administración para próximas actualizaciones:

2.1.1 El documento que se está desarrollando incluye en su primera versión las áreas de gestión del FOSUVI, FONAVI; del área Administrativa abarca a Proveeduría (solamente contratación de bienes y servicios) y al sistema de Recursos Humanos. No obstante, se excluyeron los procesos automatizados (incluyendo tanto las aplicaciones como las herramientas de Microsoft Office utilizadas) referentes a la gestión de fideicomisos, así como los demás de la gestión administrativa y de apoyo, entre estos Tesorería y Custodia, Financiero Contable, Comunicaciones, Servicios Generales, Archivo Institucional, Bienes Inmuebles y los demás de Proveeduría.

2.1.2 No se incorpora en el plan las guías y criterios que detallen bajo qué circunstancias se deben activar cualquiera de las diferentes estrategias de contingencias definidas en el documento.

2.1.3 Como parte de los análisis de riesgos y sus respectivos protocolos a seguir en caso de que se materialicen, se encuentran establecidos los de Incendios, Sismos/Terremotos, Inundación, Huelga/Paro de labores, Toma de rehenes/Asalto violento, Disturbio o manifestación por parte de terceros, Epidemia y Suspensión prolongada de servicios públicos. Sin embargo, no existe en el documento ninguna referencia a las secciones específicas del Plan de Continuidad de Servicios de TI DTI-PL-DS4-006 2015, sobre el principal riesgo y hasta la fecha el más materializado en la institución, específicamente el relacionado con la falla en los servidores de datos o en el hardware y software que los sustentan, tales como las Unidades de Poder Ininterrumpido (UPS), aires acondicionados, equipos de comunicación (routers, switchs), bases de datos, actualizaciones de versiones, etc.

2.1.4 En el documento no se están incluyendo los tiempos mínimos de recuperación en caso de utilizar como estrategia de contingencia el uso de los espacios propios del Banco, los posibles acuerdos recíprocos con otras entidades, el subcontrato con terceros de espacios de trabajo o el uso del teletrabajo como primera opción contingente.

2.1.5 No se tienen identificado en el Plan los insumos suficientes para poner a operar cualquiera de las posibles estrategias de continuidad definidas, ya sea con el teletrabajo, el acceso mediante conexión remota al Centro de Procesamiento Alterno o la utilización de sala de trabajo en sitio externo. Al respecto tampoco se cuenta con la cadena de suministros necesarias para suplir dichos insumos en caso de ser requeridos durante la contingencia.

2.1.6 A pesar de que el documento sí detalla una serie de posibles riesgos previstos para ser atacados antes, durante y después de la contingencia; aún no han identificado los riesgos que por su costo/beneficio pueden ser asumidos por el Banco y no representarían un impacto considerable.

En los puntos 9.3.4 de la sección 9.3 sobre el contenido de los planes de continuidad, 7.3 relacionada con la identificación de actividades críticas, 7.5.1 y 7.5.4 de la sección 7.5 referente a la evaluación de amenazas a actividades críticas y 7.6.3 de apartado 7.6 concerniente a la determinación de alternativas; todos de la norma de Gestión de Continuidad de Negocio INTE 01-01-18:2011 Parte I, se detalla lo siguiente:

> *"**9.3.4 Activación de planes***
> *El método para activar los planes de manejo de incidentes, continuidad de negocio o recuperación del negocio debería estar claramente documentado. Este proceso debería permitir la activación de los planes o parte de éstos tan rápido como sea posible, luego de la ocurrencia de la interrupción del negocio.*
> *La organización debería establecer y documentar con claridad las guías y los criterios con respecto a cuales individuos tiene autoridad para activar los planes y bajo qué circunstancias…"*
>
> ***7.3 Identificación de actividades críticas***
> *La organización podrá categorizar sus actividades de acuerdo con su prioridad de recuperación. Aquellas actividades que se identifican durante el BIA como generadoras de grandes pérdidas, que tendrían los más altos impactos en el corto tiempo y que deberían recuperarse más rápidamente, son las que se conocen como "**actividades críticas**". Cada actividad crítica soporta uno o más productos o servicios claves.*
> *La organización podrá desear enfocar sus actividades de planificación en las actividades críticas, pero debería reconocer que otras actividades también necesitarán recuperarse dentro de sus períodos máximos tolerables de interrupción y también podrían requerir planes para llevarlas a cabo."*

> ***7.5.1*** *En el contexto de la GCN, el nivel de riesgo debería entenderse específicamente con respecto a las actividades críticas de la organización y el riesgo de interrupción de éstas. Las actividades críticas son sustentadas por recursos tales como personas, instalaciones, tecnología, información proveedores y partes interesadas. La organización debería entender las amenazas a esos recursos, las vulnerabilidades de cada recurso y el impacto que podría darse en caso de materializarse un incidente y causar la interrupción del negocio.*
>
> ***7.5.4*** *Las amenazas específicas podrán describirse como eventos o acciones que podrían, en algunos casos puntuales, causar un impacto a los recursos; por ejemplo amenazas como incendio, inundación, corte de suministro eléctrico, pérdida de vidas, ausentismo, virus informáticos, y falla del hardware.*
>
> ***7.6.3 Aceptación***
> *Se podrá aceptar un riesgo sin que sea necesario tomar acciones adicionales. Incluso si éste no es aceptable, la habilidad para hacer algo sobre otros riesgos podría estar limitada o el costo de tomar cualquier acción podrá ser desproporcionado con respecto al beneficio potencial obtenido. En estos casos la respuesta podrá ser tolerar la existencia del nivel de riesgo si la dirección estima que el riesgo es aceptable. En algunas circunstancias el impacto del riesgo podría superar el nivel de aceptación normal del riesgo, pero, debido a la baja posibilidad de ocurrencia y/o debido al costo económico que supone el control, la alta dirección podrá aceptar el riesgo.*
> *La aceptación podrá ser complementada por un plan para el manejo de impactos que surgirán si el riesgo se materializa."* Los subrayados son nuestros

En el artículo 12 del Reglamento sobre Gestión del Riesgo Operativo, SUGEF 18-16, relativo a la continuidad del Negocio detalla:

> *"**Artículo 12. Continuidad del Negocio***
> *Como parte de una adecuada gestión del riesgo operativo, la entidad debe implementar y mantener un sistema que le permita la continuidad del negocio, con el propósito de brindar respuestas efectivas, para que la operatividad de la entidad continúe de una manera razonable, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en sus operaciones.*
> *El sistema para la continuidad del negocio debe ser congruente con el perfil de riesgo, el tamaño, la complejidad y el volumen de las operaciones de la entidad..."*

Sobre la continuidad de los servicios de TI, en el punto 1.4.7 de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información N-2-2007-CO-DFOE, se indica lo siguiente:

> *"1.4.7 Continuidad de los servicios de TI*
> *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."*

Las diferentes situaciones descritas en los puntos anteriores, se presentan debido a que es la primera vez que se está desarrollando desde la perspectiva de la Administración activa (excluyendo al área de Tecnologías de Información), un documento que trate de cubrir todos los posibles riesgos y controles asociados con la ausencia de los principales recursos tecnológicos del Banco y que por defecto deberían estar inmersos en un Plan de Continuidad de Negocio. A esta situación se le suma que para la elaboración del plan, no se obtuvo ninguna asesoría externa especialista en este tipo de herramientas.

Como principal riesgo de que el Plan de Continuidad de Negocio no incluya todos los aspectos de control indicados, es que al momento de presentarse una contingencia real no se tengan previstas todas sus implicaciones y peor aún, como responder de la mejor forma para volver los servicios a la normalidad, limitando la operativa de la unidad afectada y por defecto del Banco.

2.2 Inclusión de las Entidades Autorizadas en el Plan de Continuidad

De acuerdo a lo recabado del estudio, como parte del desarrollo del Plan de Continuidad institucional las Entidades Autorizadas (EAs) no fueron tomadas en cuenta a para la identificación y definición de necesidades para afrontar una contingencia donde se impida o limite su acceso a los recursos informáticos del Banco, principalmente al Sistema de Vivienda. Tampoco están incluidas en los cronogramas como sujetos para probar las estrategias definidas. En todo el documento solo se mencionan a las EAs como sujetos interesados y como proveedores claves, sin ahondar en detalles como los indicados anteriormente.

En los puntos 1.5, 4.1 y 5.1 del Manual de Normas de control interno para el Sector Público N-2-2009-CO-DFOE, se indica:

> *"**1.5 Responsabilidad de los funcionarios sobre el SCI***
> *De conformidad con las responsabilidades que competen a cada puesto de trabajo, los funcionarios de la institución deben, de*

manera oportuna, efectiva y con observancia a las regulaciones aplicables, realizar las acciones pertinentes y atender los requerimientos para el debido diseño, implantación, operación, y fortalecimiento de los distintos componentes funcionales del SCI."

4.1 Actividades de control
El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SCI y el logro de los objetivos institucionales. Dichas actividades deben ser dinámicas, a fin de introducirles las mejoras que procedan en virtud de los requisitos que deben cumplir para garantizar razonablemente su efectividad.
El ámbito de aplicación de tales actividades de control debe estar referido a todos los niveles y funciones de la institución. En ese sentido, la gestión institucional y la operación del SCI deben contemplar, de acuerdo con los niveles de complejidad y riesgo involucrados, actividades de control de naturaleza previa, concomitante, posterior o una conjunción de ellas. Lo anterior, debe hacer posible la prevención, la detección y la corrección ante debilidades del SCI y respecto de los objetivos, así como ante indicios de la eventual materialización de un riesgo relevante."

"5.1 Sistemas de información
El jerarca y los titulares subordinados, según sus competencias, deben disponer los elementos y condiciones necesarias para que de manera organizada, uniforme, consistente y oportuna se ejecuten las actividades de obtener, procesar, generar y comunicar, en forma eficaz, eficiente y económica, y con apego al bloque de legalidad, la información de la gestión institucional y otra de interés para la consecución de los objetivos institucionales. El conjunto de esos elementos y condiciones con las características y fines indicados, se denomina sistema de información, los cuales pueden instaurarse en forma manual, automatizada, o ambas." Los subrayados son nuestros.

La razón por la que no se valoraron las principales necesidades para afrontar las contingencias de las EAs, así como tampoco su participación en los cronogramas para probar las diferentes estrategias, se debe a que se está desarrollando hasta ahora la primera versión del Plan de Continuidad de Negocios, la cual se enfoca principalmente en los procesos internos del Banco.

La principal consecuencia que podría presentarse por esta situación es que en una eventual contingencia, las Entidades Autorizadas no sean capaces de

reaccionar adecuadamente y por consiguiente se pueda ver afectado alguno de los trámites referentes al bono de vivienda, como por ejemplo la carga de información, la administración de desembolsos, el control de avances de obras, entre otros.

2.3 Actualización del manual de puestos y funciones

En el documento del Plan de Continuidad de Negocio, en la Fase I relacionada con la planeación, en el apartado "*B. Estructura de Decisión y Grupos de atención*", se detallan una serie de actividades específicas para los encargados principales de la coordinación, ejecución y evaluación del plan, organizándolos por grupos de trabajo (Grupo coordinador, Ejecutor y Evaluador). Sobre este particular se localizó que a pesar de estar definidas esas tareas sobre puestos específicos, no se tiene previsto de igual forma incluir tales responsabilidades en el Manual de Puestos y Funciones institucional.

En el artículo 6.2 sobre Asignación de responsabilidades (gobernanza) de la norma de Gestión de Continuidad de Negocio INTE 01-01-18:2011 Parte I, se indica al respecto lo siguiente:

> *"6.2.2 Si la estructura de la organización así lo indica, la alta dirección debería nombrar representantes bien sea por función o por ubicación para apoyar la implementación del programa de GCN.*
> *Los roles, responsabilidades y autoridades deberían estar integradas en los manuales descriptivos de funciones y habilidades.*
> *Los procesos de auditoría organizacional deberían revisar estas responsabilidades.*
> *Estas responsabilidades podrán reforzarse mediante su inclusión en los procesos de evaluación organizacional a través de una política de recompensa y reconocimiento."* El subrayado es propio

Esta situación se presenta debido a que no existe ninguna normativa institucional que relacione y obligue la actualización del Manual de Puestos de acuerdo a las responsabilidades asignadas a puestos específicos en otros documentos oficiales del Banco, en este caso, el Plan de Continuidad.

Delimitar el detalle de obligaciones de ciertos cargos a un documento diferente al Manual de Puestos, puede causar que se dejen de ejecutar actividades de control que afecten la operativa de alguna unidad o área del Banco.

2.4 Continuidad del Outsourcing

En la revisión se logró determinar que no se tiene previsto incluir como parte del Plan de Continuidad de Negocio los productos, servicios y actividades que son

contratadas por el Banco a alguna empresa externa por medio de Outsourcing y que sean de relevancia crítica si la institución no llegara a contar con los mismos por algún tipo de contingencia, tal es el caso de la Seguridad, la Limpieza, el Mantenimientos de Aires Acondicionados, de los elevadores, de la Planta Eléctrica y de ciertos recursos tecnológicos (Unidades de Poder Ininterrumpido, Bases de datos, Sistemas Operativos).

En la sección 5.5 "Actividades contratadas externamente" y en el punto 10.3.5 de la sección 10.3 "*Ejercicios de los acuerdos de partes de la GCN*", de la norma de Gestión de Continuidad de Negocio INTE 01-01-18:2011 Parte I, encontramos lo siguiente:

> *"**5.5 Actividades contratadas externamente***
> *Si un producto, servicio o actividad de la organización ha sido contratado externamente, la amenaza de riesgo permanece latente dentro de la organización. Consecuentemente, una organización debería asegurarse para ella misma que sus proveedores o terceros claves tienen en curso un programa efectivo de GCN. Un método para realizar esto, es obtener evidencias de auditoría de la viabilidad de los planes de continuidad de los proveedores o terceros y los ejercicios, pruebas y mantenimiento de sus programas.*
>
> ***10.3.5** El programa de ejercicios debería considerar los roles de todas las partes involucradas incluyendo a los proveedores clave de las terceras partes, socios externos y aquellos que se espera participarán en las actividades de recuperación. Una organización podrá incluir tales partes en sus ejercicios."*

En los procesos DS2 "*Administrar los servicios de terceros*" y DS4 "*Garantizar la continuidad de los servicios*" del COBIT 4.0, se indica lo siguiente:

> *"**DS2.3 Administración de riesgos del proveedor***
> *Identificar y mitigar los riesgos relacionados con la habilidad de los proveedores para mantener una efectiva entrega de servicios de forma segura y eficiente sobre una base de continuidad. Asegurar que los contratos están de acuerdo con los estándares universales del negocio de conformidad con los requerimientos legales y regulatorios. La administración del riesgo debe considerar además acuerdos de confidencialidad (NDAs), contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos, etc."*
>
> *"**DS4.1 IT Marco de trabajo de continuidad***
> *Desarrollar un marco de trabajo de continuidad de TI 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 de la infraestructura y de 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 TI. 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.*" Los subrayados son nuestros.

La principal razón por la que no se involucra a las empresas externas que dan algún tipo de servicio al Banco en el Plan de Continuidad, se debe a que no se tiene normado a nivel institucional la obligatoriedad de incluirlas.

Esta falencia de control puede ocasionar que no se brinde algún servicio de relevancia en la institución por falta de procedimientos y acciones claras a seguir en caso de no contar con los insumos principales utilizados directamente por las empresas subcontratadas.

2.5 Comisión de Continuidad de Negocio

Para el proceso de administración y control del desarrollo del Plan de Contingencias se estableció una Comisión de Continuidad de Negocio conformada por el subgerente financiero, la Directo Administrativa y la jefatura de la Unidad de Riesgos. En la evaluación, se determinó que en dicha Comisión no se había incluido como parte de los integrantes a la jefatura del Departamento de TI, a pesar de que la gran mayoría del proceso de gestión está relacionado con las contingencias tecnológicas, siendo esta por defecto el área de más relevancia.

Según lo indicado en el artículo 4 del Reglamento sobre Gestión del Riesgo Operativo, SUGEF 18-16, sobre la administración del riesgo operativo se rescata lo siguiente:

> *"**Artículo 4. Contexto de la gestión del riesgo operativo***
> *La entidad, de conformidad con lo dispuesto en el Acuerdo SUGEF 2-10, debe contar con una estructura organizativa que le permita implementar efectivamente su estrategia para la gestión del riesgo operativo.*

> *La Junta Directiva o autoridad equivalente, junto con la Administración Superior, deben velar por que las acciones y herramientas que desarrolle la entidad para la gestión del riesgo operativo, estén plenamente integradas a su proceso institucional de administración integral de riesgos y que sean acordes con su tamaño, complejidad, volumen de sus operaciones y perfil de riesgo. En este sentido deben asignar los recursos necesarios para su implementación, sostenibilidad y mejora a través del tiempo."*

En el objetivo de control PO9.1, perteneciente al proceso PO9 del COBIT 4.0, relacionado con la evaluación y administración de los riesgos de TI, se detalla lo siguiente:

> *"**PO9.1 Alineación de la administración de riesgos de TI y del negocio***
> *Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización"*

La razón principal por la que no se había tomado en cuenta a la jefatura de TI como parte de la Comisión de Continuidad de Negocio, se debe a que no está normado los integrantes que deben formar dicho órgano, si no que fue una decisión gerencial tomada en el momento para activar el Plan de Continuidad.

Una de las consecuencias de mayor relevancia de esta situación, es que se tomen decisiones o acciones que no sean las adecuadas para atacar una contingencia relacionada con tecnologías de información, afectando por consiguiente los servicios ofrecidos por el Banco.

2.6 Centro de Procesamiento Alterno

De acuerdo al documento N° 2014LN-000001-1 del 23 de Enero del 2015, el Banco realizó un contrato con la empresa ADN Solution SRL para contar con un Centro de Procesamiento Alterno (CPA) o Data Center externo, lo cual además de cumplir con la regulación respectiva, garantiza la continuidad en la prestación de servicios ofrecidos por el Departamento de TI tanto para usuarios internos como externos; estando entre tales servicios principalmente los sistemas de información y sus respectivas bases de datos. No obstante según lo evaluado, se encontró que no se respalda toda la información institucional ubicada en los equipos personales (Inf_Inst) ni en de las diferentes unidades del Banco (Inf_inst_Unidad); esto a pesar de que gran cantidad de los procesos operativos de las diferentes áreas son administradas y ejecutadas utilizando dichas unidades lógicas de trabajo.

Relacionado directamente con la función del CPA, también se localizó que aún no se tenía normado bajo cuáles circunstancias se puede y debe activar el uso del mismo en una contingencia; así como tampoco los procedimientos respectivos para ejecutar su funcionamiento.

En los objetivos DS3.4 de la sección DS3 "*Administrar el desempeño y la capacidad*" y el DS4.9 del proceso DS4 relacionado a garantizar la continuidad de los servicios del COBIT 4.0, se detalla:

> *"**DS3.4 Disponibilidad de recursos de TI***
> *Brindar la capacidad y desempeño requeridos tomando en cuenta aspectos como cargas de trabajo normales, contingencias, requerimientos de almacenamiento y ciclos de vida de los recursos de TI. Deben tomarse medidas cuando el desempeño y la capacidad no están en el nivel requerido, tales como dar prioridad a las tareas, mecanismos de tolerancia de fallas y prácticas de asignación de recursos. La gerencia debe garantizar que los planes de contingencia consideran de forma apropiada la disponibilidad, capacidad y desempeño de los recursos individuales de TI."*
>
> ***DS4.9 Almacenamiento de respaldos fuera de las instalaciones***
> *Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI 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 TI. 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."* El subrayado es propio.

El motivo por el que no se tienen respaldados todos los procesos en el CPA, se debe a que la Gerencia General no ha normado oficialmente todos los procesos críticos del Banco que deben estar respaldados externamente.

Una consecuencia directa de no tener respaldados los insumos suficientes en el CPA, es que a cualquiera de las áreas o unidades que a nivel operativo dependan de tales recursos, se les limite o impida su actividad normal, dejándola inactiva el tiempo total que dure la contingencia.

3. CONCLUSIÓN

En la evaluación del Plan de Continuidad Institucional se valoró de forma prioritaria la estructura, consistencia, completitud y controles involucrados en el documento denominado Plan de Continuidad de Negocio.

Se logró determinar que a pesar de que la Administración ha venido trabajando de forma constante en el desarrollo del documento del Plan de Continuidad de Negocio (mismo que está en proceso de ejecución), existen debilidades propias tanto en el documento como en ciertas actividades que tiene relacionado, donde se incluyen falencia de controles, ausencia de normativa, falta de involucramiento de terceras partes, procesos administrativos pendientes y limitaciones en continuidad con tercerización.

En la sección siguiente se explica con mucho más detalla las recomendaciones que según la Auditoría Interna deben implementarse para mejorar el proceso de continuidad del negocio, en una posible contingencia que afecte los recursos tecnológicos.

4. RECOMENDACIONES

En relación con los informes de la Auditoria Interna dirigidos a los titulares subordinados, la Ley General de Control Interno No. 8292 en su artículo 36 establece:

> *"Artículo 36.—**Informes dirigidos a los titulares subordinados**. Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*
>
> *a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.*
>
> *b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.*
>
> *c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda."*

A continuación se presentan las recomendaciones de acuerdo al orden en que fueron expuestas en la sección de resultados.

A la Gerencia General

4.1 Plan de Continuidad de Negocio

4.1.1 Modificar, actualizar o adicionar (según corresponda), cada uno de las debilidades de control detalladas en la sección 2.1 de área de resultados de este informe, con la finalidad de que el Plan de Continuidad de Negocio cubra los aspectos de control esenciales en caso de que se vean afectados los principales insumos tecnológicos del Banco.

Nivel de Riesgo: **Alto**

4.1.2 Realizar un estudio de costo/beneficio enfocado a determinar lo adecuado o no de contratar una asesoría externa especializada en planes de continuidad, la cual pueda brindar enfoques y soluciones más amplios y detallados, según las características y necesidades tecnológicas del Banco.

Nivel de Riesgo: **Medio**

4.2 Inclusión de las Entidades Autorizadas en el Plan de Continuidad

Adicionar en la segunda etapa del Plan de Continuidad a las Entidades Autorizadas (EAs) como sujetos claves dentro del proceso de gestión, administración, control y desembolso del bono familiar de vivienda. Como parte de los aspectos que deben incluirse para las EAs en la actualización del documento están los procesos críticos y fechas de mayor riesgo, los períodos máximos de interrupción permitidos, las necesidades de recursos, los servicios de TI mínimos para operar, el personal clave y los responsables directos, las vías de comunicación oficiales a utilizar, la determinación de posibles estrategias de continuidad y las actividades para reanudar el servicio a la normalidad. Una vez definidos todos esos aspectos, deben programarse las pruebas respectivas.

Nivel de Riesgo: **Alto**

4.3 Actualización del Manual de Puestos y Funciones

Normar a nivel institucional la obligatoriedad de actualizar en el Manual de Puestos y Funciones todas las tareas y responsabilidades que se le asignan a alguno de los puestos existentes por medio de otros documentos formales del Banco, en este caso, el Plan de Continuidad de Negocio. Una vez normado, debe establecerse un control con el que se asegure el proceso de actualización de funciones entre la demás normativas internas y el Manual de Puestos.

Nivel de Riesgo: **Medio**

4.4 Continuidad del Outsourcing

Crear la política institucional destinada a incluir como parte del Plan de Continuidad de Negocio en todo momento a las empresas externas que ofrezcan algún producto, servicio o actividad al Banco; esto en todos los procesos que para la institución se consideren críticos y puedan afectar su operatividad si no fueran suministrados en el momento necesario.

Nivel de Riesgo: **Medio**

4.5 Comisión de Continuidad de Negocio

Incluir como parte activa de la Comisión de Continuidad de Negocio a la jefatura del Departamento de Tecnologías de Información, con la finalidad de obtener una mejor visión y las recomendaciones pertinentes sobre las diversas alternativas a elegir en caso de materializarse alguna contingencia que limite los recursos tecnológicos de la institución.

Nivel de Riesgo: **Alto**

4.6 Centro de Procesamiento Alterno

4.6.1 Normar a nivel institucional la información crítica que debe estar respaldada en el Centro de Procesamiento Alterno (CPA) y el orden en que debe ser recuperada. Como parte de dicha información deben incluirse todos los insumos tecnológicos que sean necesarios y suficientes para que las principales unidades o áreas del Banco puedan operar correctamente en una eventual contingencia donde se necesite hacer uso del CPA.

Nivel de Riesgo: **Medio**

4.6.2 Como aún no se detalla en el documento del Plan de Continuidad de Tecnologías de Información DTI-PL-DS4-006 del año 2015, deben elaborarse para el CPA los procedimientos suficientes que indiquen de qué forma lo usuarios del BANHVI van a acceder a los servicios, las actividades o pasos a seguir una vez que empiece a utilizarse, el personal involucrado, así como los pasos necesarios para volver a la normalidad después de que se restablezcan los servicios principales.

Nivel de Riesgo: **Medio**

MBA. Gustavo Flores Oviedo.
Auditor Interno