BANCO HIPOTECARIO DE LA VIVIENDA
AUDITORÍA INTERNA

Informe Final TI-SI-001-2019

AUDITORÍA SOBRE LA DISPONIBILIDAD DEL SISTEMA DE VIVIENDA EN LAS ENTIDADES AUTORIZADAS

05/03/2020

RESUMEN EJECUTIVO

En la revisión de auditoría efectuada hacia los controles implementados para asegurar la disponibilidad del Sistema de Vivienda en las Entidades Autorizadas (EAs), se localizaron ciertas debilidades de control relevantes que deben ser tomadas en cuenta por la Administración Activa para mejorar su administración.

Dentro de los hallazgos, relacionado con el documento vigente del Plan de Contingencia de los servicios de tecnologías de información, se determinó que las Entidades Autorizadas según la infraestructura actual, no podrían seguir operando en caso de que sea necesario utilizar el Centro de Procesamiento Alterno.

Alusivo a la disponibilidad de los Servidores de Datos y equipos de comunicación que soportan el Sistema de Vivienda, se detectaron limitaciones de control relacionadas con el cableado de red y eléctrico de estos equipos, mismas que podrían afectar la continuidad del servicio.

Por último, en el año en curso se presentó un problema eléctrico generado por la UPS de la Sala de Servidores, el cual dejó al Banco sin servicios tecnológicos por dos horas.

Los detalles de cada aspecto indicado en los párrafos anteriores son ampliados a en la sección de Resultados de este informe.

INDICE

RESUMEN EJECUTIVO 2

1. INTRODUCCIÓN 4

1.1 JUSTIFICACIÓN DE LA AUDITORÍA 4
1.2 OBJETIVO 4
1.3 ALCANCE 4
1.4 METODOLOGÍA DE TRABAJO 4

2. RESULTADOS DE LA EVALUACIÓN 6

2.1 PLAN DE CONTINGENCIA PARA LAS ENTIDADES AUTORIZADAS 6
2.2 CABLEADO DE SERVIDORES DE DATOS Y EQUIPOS DE COMUNICACIÓN 7
2.3 UPS DE LA SALA DE SERVIDORES 9

3. CONCLUSIÓN 12

4. RECOMENDACIONES 13

4.1 PLAN DE CONTINGENCIAS PARA LAS ENTIDADES AUTORIZADAS 14
4.2 CABLEADO DE SERVIDORES DE DATOS Y EQUIPOS DE COMUNICACIÓN 14
4.3 UPS DE LA SALA DE SERVIDORES 15

Ilustración 1 Cableado Rack Principal 8
Ilustración 2 Incidente UPS Sala Servidores 10

AUDITORÍA SOBRE LA DISPONIBILIDAD DEL SISTEMA DE VIVIENDA EN LAS ENTIDADES AUTORIZADAS

1. INTRODUCCIÓN

1.1 Justificación de la auditoría

Este estudio forma parte del Plan Anual de Trabajo de esta Auditoría Interna para el año 2019 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 los controles implementados para valorar la disponibilidad del Sistema de Vivienda en las Entidades Autorizadas.

1.3 Alcance

El estudio abarcó la documentación, información y procesos operativos vigentes al 30 de noviembre del 2019 relacionados los procesos del Sistema de Vivienda concernientes a las Entidades Autorizadas.

1.4 Metodología de Trabajo

Se aplicó la metodología establecida en el Manual para el ejercicio de la práctica de la Auditoría Interna. 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:

- ✓ Reglamento SUGEF 14-17 – COBIT 5
- ✓ Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE).
- ✓ Ley General de Control Interno.
- ✓ Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE).
- ✓ Normas Generales de Auditoria para el Sector Publico
- ✓ Normativa Interna vigente (Metodología, Manuales, Políticas, Procedimientos, Instructivos y formularios)

- ✓ Norma 308 Comunicación de resultados.
- ✓ ISO/IEC 27002:2016 Tecnologías de la información – Código de buenas prácticas para controles de seguridad de la información

Adicionalmente se aplicaron técnicas de auditoría comúnmente aceptadas como entrevistas, revisión documental de la normativa vigente y de los procesos establecidos para controlar la disponibilidad del Sistema de Vivienda utilizado por las Entidades Autorizadas. Adicional se evaluó la existencia y razonabilidad de la documentación formal y procesos establecidos sobre este tema.

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 Auditoría Interna. Las deficiencias detectadas, tanto en aspectos de control interno como operativas, de la presente revisión, se detallan en la siguiente sección de Resultados de la Evaluación.

2. RESULTADOS DE LA EVALUACIÓN

2.1 Plan de Contingencia para las Entidades Autorizadas

Al evaluar el documento del plan de contingencias de los servicios de tecnologías de información PL-DTI-DS4-006 (2018), específicamente lo relacionado a la continuidad del servicio para las Entidades Autorizadas (EAs), se localizó que el documento en algunas etapas hace mención sobre la falta de disponibilidad de los aplicativos en las Entidades y que en caso de activarse el plan debido a problemas con el centro de servidores principal, las EAs solamente deben cambiar la configuración de conectividad de sus terminales hacia el Centro de Procesamiento Alterno (CPA). Según lo investigado, al momento de la auditoría esta contingencia no era viable ya que a pesar de que en el CPA sí existen respaldos de las bases de datos, sistemas, servidores virtuales, información institucional, etc., no se cuenta con el servidor Oracle Virtual Machine donde se ejecuta el servicio del Oracle WebLogic, ambos insumos indispensables para que las EAs puedan utilizar el Sistema de Vivienda tal como lo detalla el documento del plan de contingencia. Además por el tipo de licenciamiento que posee el Banco a nivel de bases de datos, sería ilegal tener activos los mismos usuarios al mismo tiempo tanto en el Centro Principal como en el CPA.

En el punto d) del punto 5.2.2.3 sobre la no continuidad del o los servicios relacionados, del plan de contingencia para las Entidades Autorizadas, se indica:

> *"d) Nivel de Resistencia 6 Centro de Procesamiento Alterno*
> *(…)*
> *Las entidades autorizadas como ya cuentan con la infraestructura adecuada pueden acceder al CPA con solo cambial la configuración de la conectividad de sus terminales"*

Las prácticas claves de gobierno DSS04.02 Y DSS04.05 del proceso DSS04 "*Gestionar la Continuidad*" del COBIT 5, indican los siguientes aspectos:

> *"**DSS04.02 Mantener una estrategia de continuidad.***
> *Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre y otro incidente mayor o disrupción.*
>
> ***DSS04.05 Revisar, mantener y mejorar el plan de continuidad.***
> *Realizar una revisión por la Dirección de la capacidad de la continuidad a intervalos regulares para asegurar su continua idoneidad, adecuación y efectividad. Gestionar los cambios en el plan de acuerdo al proceso de control*

de cambios para asegurar que el plan de continuidad se mantiene actualizado y refleja continuamente los requerimientos actuales del negocio."

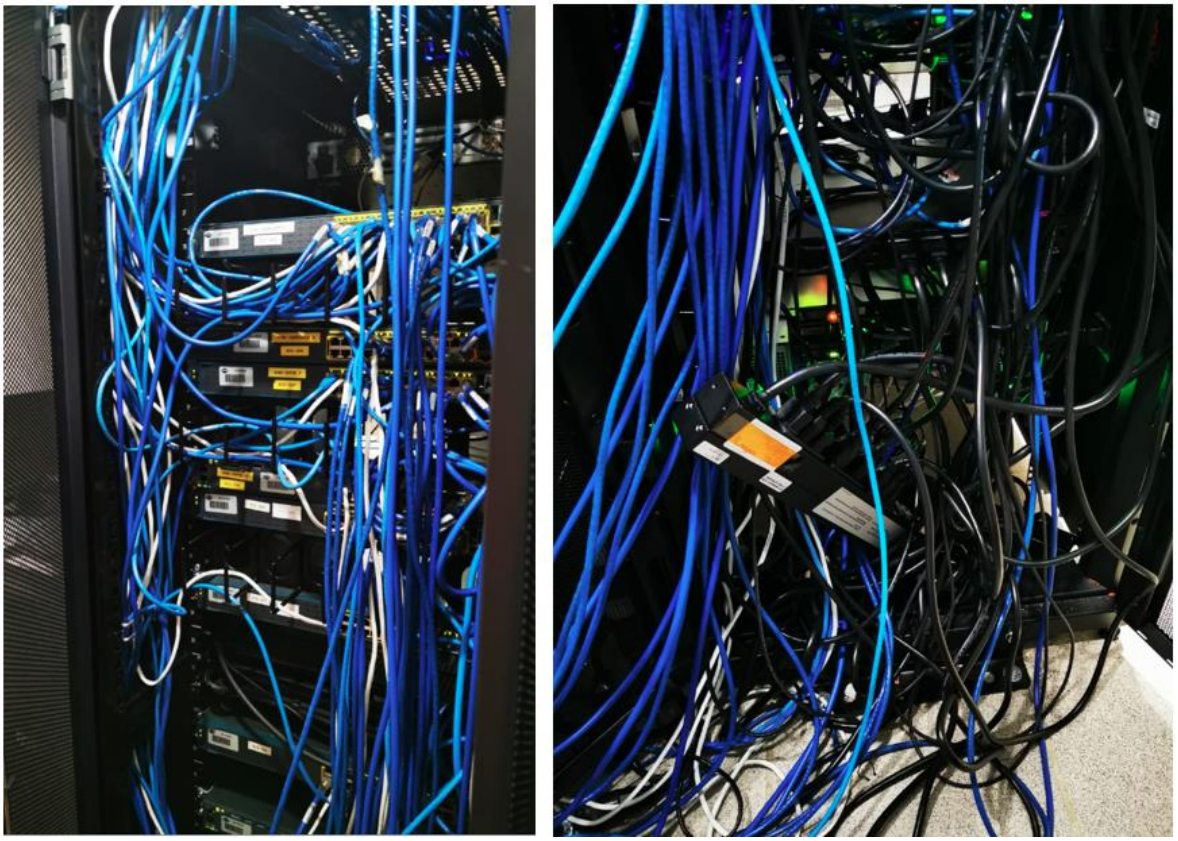
El Departamento de TI ha venido trabajando sobre la mejora de los productos disponibles en el Centro Alterno de Procesamiento, sin embargo, uno de los principales motivos por los que no se han implementado todas las necesidades tecnológicas en ese Centro, es que estas dependen en gran parte de la disponibilidad de recurso económico importantes por el tipo de equipo y licenciamiento que se necesita, así como de procesos de adquisición que en su mayoría conllevan un lapso considerable.

Además de limitar los recursos disponibles para las Entidades Autorizadas, esta situación en caso de materializarse el riesgo de diferentes tipos de fallas generales en el Centro de Servidores principal y sea necesario habilitar el CPA, puede afectar directamente la operativa del Banco al no disponer de los insumos tecnológicos suficientes para continuar la gestión del Bono de Vivienda tramitado por cualquiera de las EAs.

2.2 Cableado de Servidores de Datos y Equipos de Comunicación

Efectuando una revisión física de la disponibilidad de los equipos donde se ejecuta el Sistema de Vivienda, se localizó que los racks donde están instalados estos activos, entre estos los Servidores de Datos y los equipos de Comunicación (Routers y Switches), los cables de corriente y de red no contaban con una adecuada distribución, al punto de limitar un correcto mantenimiento preventivo o correctivo en caso de ser necesario. También se denotó el uso de una regleta de corriente que por su posición incrementa el riesgo de que se vea afectado la corriente de esos equipos.

Ilustración 1 Cableado Rack Principal



Las prácticas de control DSS01.03 y DSS05.01 de los procesos DSS01 sobre la gestión de operaciones y DSS 05 relacionado con la gestión de servicios de seguridad, del COBIT 5, detallan los siguientes criterios:

> *"**DSS01.05 Gestionar las instalaciones.***
> *Gestionar las instalaciones, incluyendo equipos de electricidad y comunicaciones, en línea con las leyes y regulaciones, requerimientos técnicos y de negocio y directrices de salud y seguridad en el trabajo.*
>
> ***DSS05.02 Gestionar la seguridad de la red y las conexiones**.*
> *Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión."*

Una de las razones por las que los cables de corriente y de red de datos carezcan de una distribución más segura, es debido a que el Departamento de TI ha venido adquiriendo nuevos equipos para actualizar la infraestructura tecnológica del Banco y después de la instalación y puesta en operación de estos activos, no se reubicó el cableado de acuerdo con las mejores prácticas de la industria.

La consecuencia principal de esta situación es que todos los servicios que dependan de los Servidores de Datos y equipos de comunicación, se vean afectados por algún manejo inadecuado del cableado y por consiguiente no se tenga acceso a los sistemas de información ni demás insumos tecnológicos.

2.3 UPS de la Sala de Servidores

Según la documentación que administra el Departamento de TI sobre los incidentes que han afectado la continuidad de los servicios administrados por esa área, se encontró que en el mes de febrero del 2019 se presentó un problema con la Unidad de Poder Ininterrumpido (UPS) ubicada en la Sala de Servidores, el cual originó que se suspendieran todos los servicios tecnológicos ofrecidos por ese Departamento; esto a pesar de que las dos principales UPS del Banco que se localizan en el primer piso funcionaban con normalidad, siendo posible que dichos equipos administraran la carga eléctrica total de los componentes tecnológicos de la Sala de Servidores.

En la siguiente imagen se muestra un resumen de este incidente:

Ilustración 2 Incidente UPS Sala Servidores

F-DTI-DS8-011 Formulario de registro de incidentes	
ID mesa de servicio:4805	
Inicio incidente	**Cierre incidente**
Fecha/Hora: 04-02-2019 –7:30 a.m.	Fecha/Hora: 04-02-2019 – 9:40 a.m.
Tiempo total incidente:	2 horas
Descripción de síntomas: Se activó la alarma de la UPS localizada en el cuarto de servidores, indicaba falla 05 e indicaba que se encontraba en BYPASS.	

Impacto	Afecta (servicios/usuarios/ áreas de negocio)
☐ Bajo	
☑ Alto	Toda la Infraestructura de la Plataforma Operativa (Base de Datos, Aplicativos y Redes)
☐ Crítico	
Descripción del impacto en el negocio: Todos los servicios prestados por del DTI, en un caso fortuito donde falle el fluido eléctrico, la planta y las UPS (primer piso) la ups de 10 KV debe alimentar los equipos que se encuentran en el cuarto de servidores.	

Servicios afectados	
☑ DTI-SRN-001 Correo Electrónico	☑ DTI-SRN-002 Internet
☑ DTI-SRN-003 Intranet Institucional	☑ DTI-SRN-004 Web Institucional
☑ DTI-SRN-005 Sistemas de Información	☑ DTI-SRN-006 Información Documental Inst
☑ DTI-SRN-007 Telefonía	

La práctica de control DSS01.03 del proceso DSS01 sobre la gestión de operaciones, del COBIT 5, muestra la siguiente actividad:

> *"**DSS01.03 Supervisar la infraestructura de TI.***
> *Supervisar las infraestructuras de TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones."*

De acuerdo con las entrevistas efectuadas, el motivo por el que se suspendieron los servicios tecnológicos tales como los sistemas de información, correo electrónico, Internet, Intranet, etc., fue debido a una incorrecta distribución de la carga eléctrica tanto de los servidores de Datos como de los equipos de comunicación, esto por estar todos redireccionados únicamente hacia la UPS ubicada en la Sala de Servidores y no de manera bipartita, esto es con otra línea hacia las UPS del primer piso.

Como efecto directo de que la incorrecta distribución de las cargas eléctricas hacia las tres UPS que soportan los equipos de la Sala de Servidores, se suspendieron todos los servicios tecnológicos afectando la operativa del Banco por dos horas.

3. CONCLUSIÓN

En la evaluación sobre la disponibilidad del Sistema de Vivienda en las Entidades Autorizadas, la Auditoría Interna logró determinar que se han venido implementado por el Departamento de TI una serie de control técnicos y operativos para asegurar una mejor disposición del sistema, tanto así que en el lapso evaluado fueron pocos los incidentes localizados al respecto.

Sin embargo, existen aspectos que deben mejorarse tales como la mejora en la disponibilidad de los servicios implementados en el Centro de Procesamiento Alterno desde la perspectiva del plan de contingencias; el orden de la estructura del cableado de red y eléctrico del Centro de Datos principal, así como la distribución eléctrica de los servidores de datos y equipos de comunicación del Centro Principal hacia las UPS institucionales.

El trabajo se realizó aplicando las técnicas de auditoria vigentes, evaluando la normativa referente a la administración de los aires de precisión, así como los principales controles implementados sobre este tema.

En la sección siguiente se explica con más detalle las recomendaciones que según la Auditoría Interna deben implementarse para mejorar el proceso de administración y control de los requerimientos de sistemas de información de todas las aplicaciones vigentes.

4. RECOMENDACIONES

En relación con los informes de la Auditoría 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 con el orden en que fueron expuestas en la sección de resultados.

4.1 Plan de contingencias para las Entidades Autorizadas

Al Departamento de TI

4.1.1 Es necesario definir la forma en que el Banco y las Entidades Autorizadas van a utilizar el Centro de Procesamiento Alterno en caso de una contingencia en el Centro de Datos principal. Para esto además de valorar los tipos de licenciamiento que el Banco decida utilizar (Activos o Pasivos), es necesario definir las áreas o unidades del Banco que deberían conectarse, los funcionarios claves, los posibles lugares, las formas de conexión, entre otros.

Nivel de Riesgo: **Alto**

4.1.2 Debe continuarse la implementación del servidor Oracle Virtual Machine donde se ejecuta el servicio del Oracle WebLogic, para lo cual es necesario valorar si los equipos ubicados en el CPA cuentan con las características técnicas suficientes para correr todos los procesos según la posible demanda de servicios y en caso de que no sea factible, gestionar los cambios correspondientes.

Nivel de Riesgo: **Alto**

4.2 Cableado de Servidores de Datos y Equipos de Comunicación

Al Departamento de TI

4.2.1 Es necesario efectuar las gestiones correspondientes para corregir la estructura del cableado de red y eléctrico de los Racks de Servidores de Datos y equipos de comunicación que se encuentran en la sala de Servidores. Como parte de esta reestructuración debe valorarse la necesidad de etiquetar aquellos cables de red que lo ameriten y reacomodar las conexiones a la regleta detallada en este informe, evitando posibles contratiempos o daños de los equipos que estén conectados a esta fuente.

Nivel de Riesgo: **Alto**

4.3 UPS de la Sala de Servidores

Al Departamento de TI

4.3.1 Es necesario evaluar el diseño de las cargas eléctricas distribuidas actualmente hacia la UPS de la Sala de Servidores y las UPS del primer piso, con el objetivo de asegurar que, en caso de fallo con la UPS de la Sala, se redistribuya la solicitud de electricidad de todos los equipos hacia las UPS del primer piso y así ninguno de los servicios se vean afectados. Esto aplica también para cualquier equipo de comunicación o servidor de datos que por su diseño cuenten con sola una fuente de poder.

Nivel de Riesgo: **Alto**

Estudio realizado por:

JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)

Firmado digitalmente por JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)
Fecha: 2020.03.05 12:19:52 -06'00'

MATI. JORGE RAMIREZ BOLAÑOS
AUDITOR

Aprobado:

GUSTAVO FLORES OVIEDO (FIRMA)

Firmado digitalmente por GUSTAVO FLORES OVIEDO (FIRMA)
Fecha: 2020.03.05 14:23:51 -06'00'

MBA. GUSTAVO FLORES OVIEDO
AUDITOR INTERNO