Banco Hipotecario de la Vivienda

Informe Final TI-OP-002-2016

AUDITORÍA SOBRE EL CENTRO DE PROCESAMIENTO ALTERNO

6/10/2016

INDICE

A. RESUMEN EJECUTIVO

En esta auditoria se examinaron los principales procesos de administración, uso y control del Centro de Procesamiento Alterno (CPA) contratado por el Banco para poder dar continuidad a los primordiales productos tecnológicos de la institución en caso de verse limitado el acceso y utilización de la sala de servidores principal.

Dentro de las debilidades detectadas se localizó la inexistencia de pruebas de contingencia que debían realizarse en coordinación con el proveedor del servicio y que consistían en utilizar el CPA como centro principal por un tiempo determinado y así valorar y mejorar su funcionalidad.

Por ser un servicio externo, como parte del proceso fue necesario instalar servidores de datos del Banco en la empresa proveedora, con la finalidad de respaldar la información institucional (bases de datos, configuración de servidores, información de las unidades y del personal, etc) que pudiera ser necesaria en un proceso contingente. Al respecto se determinó que no se han realizado revisiones sobre las bitácoras de acceso al gabinete donde se ubican los equipos del Banco que almacenan toda esa información.

De ser necesario utilizar el Centro de Procesamiento Alterno en una contingencia real, se encontró que desde el punto de vista legal no se cuenta con ninguna cláusula o acuerdo de nivel de servicio (SLA) que obligue al proveedor a brindar una asistencia al personal técnico del Banco en cada etapa de la eventualidad. Al respecto, tampoco existe un proceso formal que detalle los pasos a seguir por el Departamento de TI cuando se inicie el protocolo de activación del CPA.

Otro aspecto localizado, fue la carencia de documentación que respaldara la ejecución de pruebas de recuperación sobre la información respaldada en el sitio alterno, básicamente debido a que la normativa actual se encuentra descontinuada según el uso del Centro de Procesamiento Alterno.

A nivel operativo la mayoría de los aplicativos del Banco actualmente podrían ejecutarse en el Centro Alterno, con la excepción del Sistema de Recursos Humanos, el cual por algunos aspectos técnicos no se podría utilizar en una contingencia sin antes coordinar y ejecutar ciertas instalaciones en los equipos que se van a ejecutar.

Por último, se encontró que la toda la información institucional que es respaldada en los diferentes medios lógicos y físicos a nivel internos y externo, no cuenta con una vigencia establecida en que debe ser resguardada de forma histórica.

Los detalles de cada aspecto indicado, son ampliados a lo largo del informe.

BANCO HIPOTECARIO DE LA VIVIENDA
AUDITORÍA INTERNA
Informe Borrador Nº TI-OP-002-2016
6 de Octubre del 2016

AUDITORÍA SOBRE EL CENTRO DE PROCESAMIENTO ALTERNO

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 los principales controles relacionados con la administración, control y utilización del Centro de Procesamiento Alterno (CPA).

1.3 Alcance

El estudio abarcó la normativa, información y procesos operativos vigentes al 30 de Junio del 2016 relacionados con el uso y la administración del Centro de Procesamiento Alterno.

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:

- ✓ Las normas ISO 27002:2005 Tecnologías de Información – Código de buenas prácticas para la gestión de la seguridad de la información
- ✓ Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información N-2-2007-CO-DFOE
- ✓ El reglamento SUGEF 14-09
- ✓ 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, revisión documental de la gestión administrativa y visitas de campo para la verificación del control interno.

Específicamente se ejecutaron entrevistas con los funcionarios responsables de la administración y seguimiento del Centro Alterno de Procesamiento. Adicional se evaluó la existencia y razonabilidad de la documentación formal, referente al contrato, uso y control ejecutado sobre el Centro de Procesamiento Alterno.

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 la sección de Resultados.

2. RESULTADOS DE LA EVALUACIÓN

2.1 Pruebas de contingencias en el Centro de Procesamiento Alterno

Según consta en la licitación pública 2014LN-000001-01, el Banco contrató un Centro de Procesamiento Alterno (CPA) que pudiera asegurar la continuidad de las operaciones en una eventual contingencia donde no se pueda tener acceso a la sala de servidores de datos primaria. La empresa que ganó el concurso fue ADN Solutions Sociedad de Responsabilidad Limitada, quedando el producto final implementado y aceptado en Mayo del año 2015.

Al evaluar el cumplimiento del cartel de contratación, se determinó que a la fecha de la auditoría no existía documentación que respaldara la ejecución de pruebas de contingencias en el CPA en coordinación con el proveedor, donde se utilice ese Centro Alterno de Procesamiento como sitio principal por un lapso previamente definido. Se aclara que fue indicado por el personal del Departamento de TI que en el año 2015 sí se realizaron otro tipo de pruebas, pero no se dejaron las evidencias respectivas.

En el punto 2.10 del cartel de licitación pública 2014LN-000001-01, se detalla lo siguiente:

> *"22.10* ***Pruebas de Contingencias***
>
> *El oferente deberá contemplar en su oferta, el acompañamiento al BANHVI en el proceso de al menos dos pruebas de contingencias de los servicios contratados por año. Estas pruebas consisten en utilizar el Centro de Procesamiento Alterno (CPA) como Sitio de Procesamiento Principal durante un plazo determinado. Los alcances del acompañamiento para las pruebas en sus fases de preparación, puesta en marcha, tiempo de operación y recuperación del sitio principal, serán establecidos en los acuerdos de niveles de servicio (SLA) que el BANHVI y el adjudicatario establezcan.*"

Una de las posibles causas por las que no se realizaron las pruebas de contingencias en el Centro Alterno de Procesamiento, se debe a la falta de seguimiento por parte de la Comisión de Continuidad de Negocio, la cual debería incluir dentro de sus actividades este tipo de pruebas, mismas que debería afectar a las áreas más relevantes del Banco.

Un efecto sobre el incumplimiento de actividades de control, es que se dejen de efectuar tareas o procesos que pudieran afectar la operativa del Banco en una posible contingencia y que no haya sido probado previamente para verificar su funcionalidad.

2.2 Bitácora de acceso al Servidor de Datos Externo

El Banco contrató al Centro de Procesamiento Alterno (CPA) un gabinete o Rack que se encuentra cerrado con llave, donde se ubican los equipos necesarios a ser utilizados en una posible continencia y así poder dar un servicio alterno de las principales aplicaciones institucionales. Como parte de del proceso de contratación y por ser un lugar "remoto", el proveedor tiene la potestad por medio del servicio contratado de "*manos remotas*", de abrir y acceder a los equipos del Banco; esto únicamente cuando sea requerido y solicitado por el BANHVI y para lo cual se define en el cartel una bitácora de acceso a dicho gabinete. En la auditoría se logró determinar que desde que se puso a operar el CPA en Mayo del 2015, no se han realizado revisiones sobre la totalidad de accesos físicos efectuados al Rack.

Sobre este tema, tampoco existe un control que informe de manera automática al personal del Departamento de TI, cada vez que se abran las puertas frontales y traseras de dicho gabinete.

En el apartado 22.1.4 de la sección 22 relacionada con las especificaciones técnicas del contrato, se detalla en lo siguiente:

> *"22.1.4 En cuanto al tema de seguridad física, el sitio debe asegurar todas las condiciones necesarias para el control de acceso físico de las instalaciones* ***mediante el uso de bitácoras de ingreso*** *a las instalaciones, definidas de la siguiente manera:*
>
> *(…)*
>
> *22.1.4.4 Cuarto Nivel: Llave para acceso al gabinete dedicado..."* El destacado es propio.

La razón por la que no se han efectuado revisiones sobre los accesos físicos al gabinete ubicado en el CPA, se debe a que no existe un procedimiento enfocado a evaluar la bitácora definida para dicho fin. Referente al control que avise de forma remota cuando se abran las puertas del Rack, aún no se ha implementado en vista de que las actividades realizadas en el CPA ha venido desarrollándose paulatinamente, estando pendiente aún tal tarea.

Una posible consecuencia de no controlar los accesos al gabinete donde se ubica el servidor de datos, es que personal ajeno a la institución acceder de forma irregular a los equipos del Banco y por ende a la información que contengan.

2.3 Asistencia y activación del Centro de Procesamiento Alterno

Actualmente en caso de presentarse alguna emergencia con la sala de servidores principal y siendo necesario activar el Centro de Procesamiento Alterno y los insumos tecnológicos que ahí se encuentran, no se tiene establecido en el contrato un proceso de asistencia técnica por parte de la empresa ADN Solutions en caso de ser requerido.

Sobre este tema, se determinó que tampoco se cuenta con un procedimiento por parte del Departamento de TI que detalle cómo proceder una vez que la Administración le indique la necesidad de activar del CPA.

En el objetivo DS3.4 de la sección DS3 "*Administrar el desempeño y la capacidad*" del COBIT 4.0, se detalla lo siguiente:

> *"**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."* El subrayado es nuestro.

Esta situación se presenta debido a que no fue previsto en el contrato vigente alguna cláusula que obligara al proveedor a acompañar al personal de soporte técnico del Banco cuando se active el protocolo de contingencia. Con respecto a la falta del procedimiento de activación del CPA, se debe a que ha viene como parte del proceso en desarrollo de administración y control de ese nuevo recurso.

Una de las consecuencias que pueden presentarse en caso de no tener la asistencia del personal adecuado al presentarse una emergencia que impida utilizar la sala de servidores primaria, es que se pueda atrasar o limitar la habilitación del centro alterno, siendo afectados en tiempo y calidad tanto los funcionarios internos como los clientes externos del Banco.

2.4 Pruebas de recuperación de datos del CPA

No se tiene definido realizar pruebas periódicas de recuperación de datos, sobre la información que se tiene respaldada en el Centro de Procesamiento Alterno

(CPA). Se indicó en la auditoría que ya se han realizado ciertas pruebas de este tipo, pero no se localizó evidencia que respaldara tal actividad.

Sobre las pruebas a los datos respaldados fuera de las instalaciones, el objetivo DS4.9 del proceso DS4 relacionado a garantizar la continuidad de los servicios del COBIT 4.0, indica:

> *"**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.

Como causa principal de que no se estén realizando las pruebas de recuperación de la información contenida en el CPA y no se tenga evidencia de las veces que se ha realizado la tarea (según lo indicado), se debe a que el procedimiento vigente P-DTI-SLA-007 "*Revisar la validez de respaldos*" relacionado con este tema, no se adapta a la situación actual de respaldos y sus procesos de recuperación.

Esta situación puede ocasionar que se realicen respaldos de toda la información contenida en los servidores de datos, pero que al momento de necesitarla en una verdadera contingencia, no se pueda recuperar de forma oportuna, completa o exacta por algún inconveniente técnico.

2.5 Sistemas de Información respaldados externamente

Al revisar las aplicaciones que actualmente se encuentran respaldadas en el Centro de Procesamiento Alterno (CPA), se determinó que a nivel de bases de datos se cuentan con toda la información necesaria para que la mayoría de los sistemas del Banco puedan ejecutarse; lo cual fue lo previsto por el Departamento de TI en la primera fase del uso del CPA. Sin embargo, se encontró que para el Sistema de Recursos Humanos a pesar de que sí se respalda su base de datos, actualmente para que la aplicación funcione sería

necesario desarrollar otras actividades técnicas por parte del Departamento de TI, para las que primeramente la Administración Activa debe indicar de qué forma quiere desarrollarlo.

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."*

El artículo 5.1 del Manual de Normas de control interno para el Sector Público N-2-2009-CO-DFOE, detalla:

> *"**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."*

La razón por la que se limita la ejecución del Sistema de Recursos Humanos desde el CPA en caso de utilizarse como centro principal en una contingencia, se debe a que ese sistema requiere en el equipo (físico o virtual) que se vaya a conectar, la instalación de un cliente (ambiente necesario para su ejecución) de Oracle para que ingrese a la base de datos y otro cliente del aplicativo (Power Builder); esto a diferencia del resto de sistemas que fueron desarrollados con Developer de Oracle, en los que solamente se configura el cliente de Oracle en el servidor correspondiente.

Esta situación limitaría o atrasaría la continuidad de los servicios relacionada con todo el proceso de recursos humanos del Banco (planillas, horas extras, vacaciones, médico de empresa, acciones de personal, entre otros), en caso de ser requerido en una contingencia el Centro de Procesamiento Externo.

2.6 Información histórica institucional

No se ha definido un tiempo específico en que la información histórica institucional debe ser resguardada en los respaldos de información. Actualmente el Departamento de Tecnologías de Información está desarrollando sus procesos para mantener al menos los últimos 5 años de los datos institucionales, esto a pesar de que no se les ha dado ninguna directriz al respecto por parte de la Gerencia General.

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..."*

Como principal motivo por el que no se ha definido el lapso histórico de respaldo de la información del Banco, se debe a la carencia de una directriz gerencial que regule las pautas a seguir sobre dicho asunto.

La situación podría tener dos consecuencias, que no se resguarde para trabajos operativos o legales la información histórica el tiempo suficiente o que se inviertan recursos tecnológicos y económicos más de lo necesario.

3. CONCLUSIÓN

En la evaluación del Centro de Procesamiento Alterno se valoraron los procesos de administración, uso y pruebas de la información contenida en ese lugar, así como los principales aspectos de control detallados en el contrato vigente con la empresa proveedora ADN Solutions SLR.

La ejecución del trabajo fue realizado aplicando las técnicas de auditoria correspondiente, evaluando la normativa vigente aplicable al proceso de la continuidad del negocio y los controles asociados identificados y definidos hasta el momento de la revisión. También fueron aplicados cuestionarios y entrevistas al personal clave involucrado directamente en su ejecución.

Se determinó que la posibilidad de procesar en un lugar remoto los principales servicios tecnológicos del Banco en una posible contingencia, es una actividad relativamente nueva en la institución y por ende sus etapas se encuentran en mejora continua; de ahí que las debilidades indicadas en el informe se consideren propias de un proceso de maduración.

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.

4.1 Pruebas de contingencias en el Centro de Procesamiento Alterno

A la Gerencia General

4.1.1 Definir la responsabilidad a la Comisión de Continuidad de Negocio sobre el seguimiento necesario sobre el desarrollo de las pruebas de continuidad relacionadas con el Centro de Procesamiento Alterno, las cuales involucrarían además de al Departamento de TI, a diferentes unidades operativas del Banco.

Nivel de Riesgo: **Alto**

Al Departamento de TI

4.1.2 Establecer de forma general los diferentes tipos de pruebas técnicas que se puedan realizar en el Centro de Procesamiento Alterno tanto de forma independiente (solo el personal de TI), como en coordinación con el personal de la empresa proveedora; las cuales deben contar con la programación respectiva. Al respecto deben establecerse el tipo y forma de la documentación que respaldará dichas actividades.

Nivel de Riesgo: **Medio**

4.2 Bitácora de acceso al Servidor de Datos Externo

Al Departamento de TI

4.2.1 Elaborar un procedimiento que abarque las evaluaciones periódicas de la bitácora de acceso al gabinete alquilado en el Centro de Procesamiento Alterno, el cual abarque tanto en los accesos realizados por el personal del Banco, como los ejecutados por el personal del proveedor del servicio cada vez que sea solicitado por el BANHVI en la función de “manos remotas”.

Nivel de Riesgo: **Medio**

4.2.2 Evaluar el costo/beneficio de implementar un control físico que de forma automática informe al personal de TI cada vez que se abran las puertas delanteras y traseras del Rack, tanto en horario de oficina como en horas no laborales. Debe evaluarse la posibilidad de crear un registro de las veces que se active dicho control y validar los datos periódicamente contra la bitácora de accesos del gabinete definida para este fin.

Nivel de Riesgo: **Alto**

4.3 Asistencia y activación del Centro de Procesamiento Externo

A la Gerencia General

4.3.1 Evaluar la posibilidad de formalizar ya sea a nivel del contrato vigente con la empresa ADN Solutions o con un nuevo documento, la obligatoriedad de asistir técnicamente al personal del Departamento de TI en caso de activarse el protocolo de contingencia para el uso del Centro de Procesamiento Alterno; esto en cada una de las etapas (inicio, durante y después) que conlleve el proceso. Para este trabajo además de contar con la asesoría del Departamento de la Asesoría Legal, se debe coordinar con el Departamento de TI las partes técnicas que le correspondan.

Nivel de Riesgo: **Alto**

4.3.2 Gestionar la elaboración de un procedimiento que detalle las fases necesarias poner a operar el Centro de Procesamiento Alterno cuando sea solicitado por la Administración Activa. Tales etapas deben incluir la preparación, puesta en ejecución, lapso de operación y la vuelta a la normalidad una vez corregido el problema con el sitio principal.

Nivel de Riesgo: **Medio**

4.4 Pruebas de recuperación de datos del CPA

Al Departamento de TI

Actualizar el procedimiento de recuperación de información enfocado a los datos que ahora se están resguardando en el Centro de Procesamiento Alterno; así como elaborar los demás procedimientos que sean necesarios para su correcta administración y control. La actividad de validar los datos respaldados debe abarcar tanto la información contenida lógicamente en el servidor de datos definido para dicho fin, así como la contenida en las cintas de respaldo que prontamente van a estar instaladas en ese centro alterno.

Nivel de Riesgo: **Medio**

4.5 Sistemas de Información respaldados externamente

A la Gerencia General

Definir las diferentes estrategias que se podrían utilizar para acceder al Sistema de Recursos Humanos del Banco y que han venido siendo valoradas en el Plan de Continuidad Institucional que se encuentra en proceso de desarrollo. Una vez

identificadas, se debe coordinar con el Departamento de TI la instalación y configuración en los equipos que correspondan de los insumos necesarios, para que de ser necesario, pueda operarse dicho sistema en una eventual contingencia.

Nivel de Riesgo: **Alto**

4.6 Información histórica institucional

A la Gerencia General

Establecer de acuerdo a la normativa vigente y a la realidad operativa y tecnológica del Banco, una política institucional que determine el tiempo máximo que deba mantenerse la información histórica de las diferentes bases de datos con las que cuenta la institución. Este insumo debe ser el utilizado por el Departamento de TI para administrar y controlar sus procesos de respaldo de información.

Nivel de Riesgo: **Medio**

MBA. Gustavo Flores Oviedo
Auditor Interno.