Banco Hipotecario de la Vivienda

Informe Final TI-OP-003-2016

AUDITORÍA SOBRE EL CUMPLIMIENTO DE LA LEGISLACIÓN EN LA INFORMACIÓN PRIVADA

7/02/2017

INDICE

A. RESUMEN EJECUTIVO

En esta auditoria se evaluaron los principales procesos relacionados con la adecuada administración y el cumplimiento de la normativa interna y externa referente al cumplimiento de la legislación vigente sobre la información privada contenida en los medios lógicos del Banco.

Como parte de las debilidades localizadas se detectó la carencia de normativa para poder acceder de forma legal a los datos personales de los funcionarios del Banco, que se localiza tanto en sus cuentas de correo electrónico como en las computadas personales que se les han asignado para ejecutar sus funciones.

Evaluando parte de lo indicado en la Ley n°9048 relacionado con los procesos de mantenimiento de sistemas de información, se identificó que se carece de un control que valore la existencia de programación indebida en el código fuente una vez que se ha solventado el requerimiento del usuario final y se va a colocar en el servidor de Producción.

También se logró comprobar la inexistencia de normativa interna que regule el accionar en caso de localizar programas maliciosos en las computadoras del Banco y que hayan sido utilizados de forma intencional.

Por último, se encontró la falta de políticas y procedimientos enfocados a administrar los posibles casos de envío de información falsa o incorrecta utilizando los equipos del Banco y donde dichos correos afecten de forma negativa a la institución o a sus empleados.

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

BANCO HIPOTECARIO DE LA VIVIENDA
AUDITORÍA INTERNA
Informe Final Nº TI-OP-003-2016
7 de Febrero del 2017

AUDITORÍA SOBRE EL CUMPLIMIENTO DE LA LEGISLACIÓN EN LA INFORMACIÓN PRIVADA

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 el proceso de administración y cumplimiento de la legislación relacionada con la información privada de los funcionarios del Banco.

1.3 Alcance

El estudio abarcó la normativa, información y procesos operativos vigentes al 30 de Noviembre del 2016 relacionados con la administración y el control sobre el cumplimiento de la legislación vigente.

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
- ✓ Ley n° 9048: "*Reforma de varios artículos y modificación de la sección VIII, denominada delitos informáticos y conexos, del título VII del Código Penal*"
- ✓ 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 del área de Soporte Técnico del Departamento de TI. Adicional se evaluó la existencia y razonabilidad de la documentación formal y procesos establecidos para controlar la información establecida según la norma como privada.

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 Normativa sobre el acceso a cuentas de correo

Al valorar la normativa vigente, se logró determinar que no se ha normado bajo cuáles circunstancias y qué pasos se deben seguir en caso de ser necesario acceder a la cuenta de correo electrónico asignada a un funcionario que por diferentes razones (por ejemplo que se encuentre fuera de la institución) no pueda hacerlo.

En el artículo 196 de la Ley 9048 "*Reforma de varios artículos y modificación de la sección VIII, denominada delitos informáticos y conexos, del título VII del Código Penal*", se indica:

> *"**Artículo 196.- Violación de correspondencia o comunicaciones***
>
> *Será reprimido con pena de prisión de tres a seis años quien, con peligro o daño para la intimidad o privacidad de un tercero, y sin su autorización, se apodere, accese, modifique, altere, suprima, intervenga, intercepte, utilice, abra, difunda o desvíe de su destino documentos o comunicaciones dirigidos a otra persona.*
>
> *La pena será de cuatro a ocho años de prisión si las conductas descritas son realizadas por:*
>
> *a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.*
>
> *b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos."* El subrayado en propio.

De acuerdo a lo conversado, no se ha normado aún esta situación ya que según lo indicado por el área de soporte Técnico, indistintamente de la justificación ofrecida por alguna jefatura o de la necesidad de obtener alguna información, los funcionarios de TI no realizan los accesos las cuentas de correo solicitadas, en vista de las consecuencias legales que podrían tener.

Como consecuencia de esta situación, podría verse afectada la operativa de una unidad al no poder obtener información necesaria para algún trabajo y que esté contenida en correos electrónicos de empleados que por distintas razones se les impida facilitarlos.

2.2 Normativa sobre información del usuario en las computadoras

En la auditoría al evaluar la normativa vigente, se logró determinar que se cuenta con la política M-DTI-DS5-007 denominada "*Uso de recursos tecnológicos*", en la cual además de indicar como se debe administrar la carpeta "*Inf_inst*" creada en todas las computadoras del Banco, se detalla cómo debe administrarse la carpeta implementada para que cada funcionario resguarde su información privada en cada equipo en "*D:\username*". No obstante, se logró comprobar que no se ha definido bajo cuáles circunstancias el personal técnico podría acceder a la información privada de las computadoras, esto previa autorización del dueño de la información.

En el punto 3 de la política M-DTI-DS5-007, Uso de recursos tecnológicos, se indica lo siguiente con relación al almacenamiento de la información personal de los funcionarios:

> "…*El Departamento de TI dentro de las estaciones de trabajo definirá una carpeta, identificada con el código de usuario asignado (login), en la cual pueda el funcionario almacenar información personal, la cual no debe violentar las prohibiciones establecidas en la presente política. La administración de la información mencionada es responsabilidad del usuario*."

El artículo 196 bis de la Ley 9048 denominada "*Reforma de varios artículos y modificación de la sección VIII, denominada delitos informáticos y conexos, del título VII del Código Penal*", detalla:

> *"**Artículo 196 bis.- Violación de datos personales***
>
> *Será sancionado con pena de prisión de tres a seis años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.*
>
> *La pena será de cuatro a ocho años de prisión cuando las conductas descritas en esta norma:*
>
> > *a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.*

b) Cuando los datos sean de carácter público o estén contenidos en bases de datos públicas.

c) Si la información vulnerada corresponde a un menor de edad o incapaz.

d) Cuando las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona." El subrayado es propio.

La situación presentada se debe a que no se cuenta con ninguna normativa interna que regule ese tipo de actividades, aunado a que de acuerdo a lo indicado por el coordinador de soporte, no es una acción que ellos ejecuten aunque sea solicitado por alguna jefatura o persona que no sea dueña de los datos.

No contar con alguna política y procedimiento que detalle la forma en que debe accederse a la información privada de los demás usuarios, podría limitar el acceso a datos necesarios para un área o unidad que por error no fueron guardados en la carpeta de información institucional, sino en la personal.

2.3 Control en el mantenimiento de Sistemas de Información

A nivel de los sistemas de información existentes en el Banco, por la operativa de la institución y de las diferentes áreas, es normal que se genere la necesidad de realizar modificaciones a tales aplicaciones debido a requerimientos propios de los usuarios, mismos que van desde nuevos reportes, pantallas y hasta pequeños módulos destinados a administrar alguna tarea que anteriormente se llevaba de forma manual. Para esto el Departamento de TI ha implementado toda una estructura operativa en el área de Desarrollo y Mantenimiento de Sistemas, la cual abarca todo el proceso requerido.

No obstante lo anterior, como parte de la evaluación se nos indicó que no existe un control o filtro dirigido a identificar posible programación indebida o maliciosa inmersa en el código del programa. De acuerdo a lo explicado, esta función la realiza hasta cierto punto el Administrador de la Base de Datos (DBA) pero básicamente a nivel de objetos en bases de datos (paquetes, funciones, procedimientos, listas, tablas, etc.), pero no revisa a nivel de la Forma ni del Reporte (que sería donde se ubica la mayor parte del código de programación), ya que no es parte de las funciones del DBA.

El artículo 217 bis de la Ley n° 9048 detalla con relación a las estafas informáticas lo siguiente:

*"**Artículo 217 bis.- Estafa informática***

Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos." El subrayado es propio.

También en el artículo 229 *ter* de la Ley n° 9048 se transcribe sobre el sabotaje informático lo siguiente:

*"**Artículo 229 ter.- Sabotaje informático***

Se impondrá pena de prisión de tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

La pena será de cuatro a ocho años de prisión cuando:

a) Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.

b) La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
c) El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas.

> *d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones."*

El COBIT, en su proceso de Administración de cambios, define en los objetivos 6.1 lo siguiente:

> *"**AI6.1 Estándares y procedimientos para cambios***
> *Establecer procedimientos de administración de cambio formales para manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y patches) para cambios a aplicaciones, procedimientos, procesos, parámetros de sistema y servicio, y las plataformas fundamentales."*

Según lo que se investigó, la ausencia de revisión en el código fuente se debe a que no está delimitada esa actividad de forma específica en el manual de puestos del Departamento de TI para ninguno de los funcionarios del área.

Un efecto directo de la carencia de revisión de código malicioso en los sistemas del Banco, es que se puedan ejecutar acciones indebidas en las aplicaciones que se ejecuten en el servidor de producción y que no puedan ser detectadas; tales actividades pueden ir desde la modificación de datos, acceso a información privada, suspensión de seguridad, alteración de procesos, entre otros.

2.4 Utilización de programas maliciosos

En el Banco existe el procedimiento P-DTI-DS5-002 denominado "*Atención de Incidentes de Seguridad de TI*", en el cual de forma general se detalla los pasos a seguir en caso de que se localice un incidente que violente la seguridad a nivel tecnológico. Sin embargo, no se ha definido cómo se debe proceder cuando el incidente tiene relación al uso de un programa malicioso y se haya comprobado que fue ejecutado por el funcionario de forma intencional para buscar algún tipo de beneficio.

En el artículo 232 de Ley 9048: "*Reforma de varios artículos y modificación de la sección VIII, denominada delitos informáticos y conexos, del título VII del Código Penal*", se indica con respecto a uso de programación maliciosa:

> **"*Artículo 232.- Instalación o propagación de programas informáticos maliciosos***
>
> *Será sancionado con prisión de uno a seis años quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos.*

La misma pena se impondrá en los siguientes casos:

***b)** A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.*

***b)** A quien, sin autorización, instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertirlos en medios idóneos para propagar programas informáticos maliciosos, conocidos como sitios de Internet atacantes.*
***c)** A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos.*

***d)** A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.*

***e)** A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.*

La pena será de tres a nueve años de prisión cuando el programa informático malicioso:

***i)** Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal.*
***ii)** Afecte el funcionamiento de servicios públicos.*
***iii)** Obtenga el control a distancia de un sistema o de una red informática para formar parte de una red de ordenadores zombi.*
***iv)** Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero.*
***v)** Afecte sistemas informáticos de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas.*
***vi)** Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático.*" Los subrayados son nuestros.

De acuerdo a lo conversado con el área de soporte Técnico, a la fecha no se había incluido un enfoque de los incidentes maliciosos, en vista de que se había suficiente con la inclusión del proceso para cerrar la brecha de seguridad y mitigar el riesgo, dejando de lado las violaciones de seguridad intencionales y efectuadas con algún fin indebido.

Una de las consecuencias de no tener normado como actuar en este tipo de situaciones, es que no se logre recuperar correctamente la evidencia del incidente, produciendo vacíos legales en un eventual procedimiento administrativo o acto judicial.

2.5 Difusión de información falsa

En la auditoría se logró determinar que no están normadas las acciones a seguir en caso de que se compruebe le remisión de información o noticias falsas utilizando cualquiera de los equipos tecnológicos del Banco y que pueda perjudicar de directa o indirectamente cualquier unidad de la institución o alguno de sus funcionarios.

En el artículo 236 de Ley n° 9048: "*Reforma de varios artículos y modificación de la sección VIII, denominada delitos informáticos y conexos, del título VII del Código Penal*"

> *"**Artículo 236.- Difusión de información falsa***
>
> *Será sancionado con pena de tres a seis años de prisión quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios."*

La razón por la que a la fecha de la revisión no exista política ni procedimiento en ese sentido, se debe a que el Banco ha venido en un proceso de maduración a nivel normativo y hasta el momento no se había valorado la necesidad de regular lo relacionado con propagación de información falsa.

Una de las posibles consecuencias de no tener normado el proceso de revisión de difusión de información falsa, es que no se tenga claro cómo actuar ni qué datos recolectar en una eventualidad de este tipo y por ende no sirva lo recabado como pruebas para un proceso sancionatorio o judicial.

3. CONCLUSIÓN

Al efectuar la auditoría sobre el proceso de administración y cumplimiento de las normas que regulan los temas principales de privacidad y confidencialidad de la información de los funcionario del Banco que poseen en los equipos de trabajo, se logró determinar que a nivel de maduración y culturización del tema en general, la institución ha incursionado muy poco sobre los controles que deberían aplicarse.

La ejecución del trabajo fue realizada aplicando las técnicas de auditoria correspondiente, incluyendo la ejecución de entrevistas y valoración de documentos vigentes al momento de la auditoría.

También se considera necesario reforzar los controles relacionados con la programación para mantenimiento de sistemas; el posible uso de programas maliciosos que vulneren la seguridad de la institución y la difusión o envío de información falsa del Banco y que pueda afectarlo.

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 Normativa sobre el acceso a cuentas de correo

A la Gerencia General

Debe normarse el acceso a cuentas de correo electrónico institucional que no sean propias del funcionario que las va a acceder, ya sea una jefatura, personal de soporte Técnico o algún tipo de investigación o revisión. Para esto debe quedar documentado el permiso escrito que brinde previamente el dueño de la cuenta, así como el detalle de bajo qué situaciones se podrá realizar esta actividad, el tipo de información que podrá ser extraída y de qué forma, el personal que debe estar a cargo del proceso así como el o las personas que deben estar presentes (la tarea no debería realizarse de forma individual), la minuta o documento donde se indique que información se recuperó y todos los demás pasos o actividades necesarias para ejecutar correctamente el acceso a la información. Una vez implementado el control, debe implementarse un histórico que resguarde la información recolectada.

Nivel de Riesgo: **Medio**

4.2 Normativa sobre información del usuario en las computadoras

A la Gerencia General

Debe crearse la normativa necesaria enfocada a administrar correctamente los accesos a la carpeta de información personal ("*D:\username*") existente en todas las computadoras del Banco y que deban ser ejecutados por el personal del Departamento de TI. Para esto debe creare un histórico de trabajo donde se documente al menos las autorizaciones previas que deban existir, los motivos por los que fue necesario el acceso, los funcionarios de TI que ejecutaron la tarea (no debería ser una única persona), los procedimientos correspondientes, los datos extraídos y las firmas de todos los involucrados, incluyendo la del dueño de la información privada.

Nivel de Riesgo: **Medio**

4.3 Control en el mantenimiento de Sistemas de Información

Al Departamento de TI

4.3.1 Debe implementarse de manera formal para los sistemas de información, un proceso de validación y revisión del código fuente para cuando deba ser modificado por cualquier motivo, esto tanto en la Forma como en el Reporte. Esta revisión debe quedar documentada y debe indicar además del cumplimiento del requerimiento del usuario final, que el código no presentó ninguna anomalía o característica fuera de lo requerido y en caso de encontrarse, debe quedar anotado y efectuar el comunicado respectivo a la jefatura de TI.

Nivel de Riesgo: **Medio**

4.3.2 Implementar un histórico de todas las Formas y Reportes que han sido modificadas, el cual al menos tenga la siguiente información: el sistema al que pertenece o al que afecta, las fechas de modificación, el detalle en prosa del cambio, el código fuente anterior y el modificado, el funcionario encargado de realizar el cambio así como la persona que validó su cumplimiento y el funcionario que finalmente trasladó el archivo al servidor de producción.

Nivel de Riesgo: **Medio**

A la Gerencia General

4.3.3 Normar a nivel del Manual de Puestos y funciones, al puesto responsable de velar por el correcto cumplimiento y ejecución del proceso de mantenimiento de los sistemas de información del Banco.

Nivel de Riesgo: **Medio**

4.3.4 Valorar la implementación de sanciones administrativas y judiciales, en caso de que se localicen anomalías en el código fuente de algún sistema de información, y donde la misma genere algún beneficio directo o indirecto para el funcionario que lo desarrolló.

Nivel de Riesgo: **Medio**

4.4 Utilización de programas maliciosos

A la Gerencia General

Se debe normar correcta y ampliamente la forma de actuar y los pasos a seguir cuando se determine que algún incidente de seguridad detectado en los equipos del Banco, fue realizado con alevosía buscando algún bienestar para el funcionario que lo ejecutó. En este sentido, es necesario buscar la asesoría correspondiente para que el proceso de recolección de evidencia lógica y física (de existir), se realice de forma adecuada y suficiente para posibles procesos legales posteriores a la investigación.

Nivel de Riesgo: **Medio**

4.5 Difusión de información falsa

A la Gerencia General

Debe crearse la normativa suficiente tanto a nivel de política como de procedimiento el tema referente la propagación de información o noticias inexistentes o privadas, que sean capaces de perjudicar al Banco o a sus funcionarios. Para esto además de la política respectiva, debe elaborarse un procedimiento donde se indique como mínimo la persona o área encargada de ejecutar la revisión, los pasos que deben seguirse, el personal que va a estar involucrado, la documentación necesaria de resguardar y de qué forma hacerlo, entre otros.

Nivel de Riesgo: **Medio**

MBA. Gustavo Flores Oviedo.
Auditor Interno.