**BANCO HIPOTECARIO DE LA VIVIENDA**
**AUDITORÍA INTERNA**

# Informe Final TI-OP-002-2020

## AUDITORÍA SOBRE LA ADMINISTRACIÓN Y ATENCIÓN DE INCIDENTES DE TI

28/01/2021

## RESUMEN EJECUTIVO

La revisión estuvo enfocada en valorar los controles existentes relacionados con la administración y atención de incidentes de los servicios ofrecidos por Tecnologías de Información.

Dentro de los aspectos a mejorar, se encontró que no se cuenta con un esquema para administrar y agrupar los incidentes tecnológicos de forma completa y correcta.

Otro de los resultados obtenidos es que no se registran las causas más probables que pueden afectar los servicios que ofrece el área de tecnologías. De igual forma falta definir soluciones temporales o permanentes para dichos problemas.

En la revisión también se resaltó la falta de un proceso de escalado de incidentes y de acciones previamente definidas para resolver los problemas presentados.

Por último, se denota la carencia de un control disciplinario cuando se presenten violaciones a la seguridad de la información.

Los detalles de cada aspecto indicado en los párrafos anteriores son ampliados 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* ESQUEMAS DE ADMINISTRACIÓN DE INCIDENTES DE TI ..... 6
2.2 CAUSAS Y CRITERIOS SOBRE PROBLEMAS TECNOLÓGICOS ..... 7
2.3 ESCALAMIENTO DE INCIDENTES TECNOLÓGICOS ..... 8
2.4 PROCESO DISCIPLINARIO POR VIOLACIONES DE SEGURIDAD ..... 10

**3. CONCLUSIÓN** ..... **12**

**4. RECOMENDACIONES** ..... **13**

*4.1* ESQUEMAS DE ADMINISTRACIÓN DE INCIDENTES DE TI ..... 14
*4.2* CAUSAS Y CRITERIOS SOBRE PROBLEMAS TECNOLÓGICOS ..... 14
*4.3* ESCALAMIENTO DE INCIDENTES TECNOLÓGICOS ..... 15
4.4 PROCESO DISCIPLINARIO POR VIOLACIONES DE SEGURIDAD ..... 15

# AUDITORÍA SOBRE LA ADMINISTRACIÓN Y ATENCIÓN DE INCIDENTES DE TI

## 1. INTRODUCCIÓN

### 1.1 Justificación de la auditoría

Este estudio forma parte del Plan Anual de Trabajo de esta Auditoría Interna para el año 2020 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 existentes para la administración y atención de incidentes de los servicios de TI.

### 1.3 Alcance

El estudio abarcó los controles, la documentación, información y procesos operativos vigentes al 30 de Julio del 2020.

### 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

Además, se aplicaron técnicas de auditoría comúnmente aceptadas como revisión documental de la normativa interna y externa relacionada con la evaluación, así como información solicitada a los usuarios involucrados en el proceso.

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* Esquemas de Administración de incidentes de TI

Al evaluar el proceso de administración de incidentes relacionados con tecnologías de información, se encontró como parte de las debilidades de control que no se ha definido un esquema para tipificar, clasificar y priorizar los posibles incidentes tecnológicos según los servicios con los que cuenta la institución y que podrían presentar inconvenientes, por ejemplo, sistemas de información, correo electrónico, Internet, equipos estacionarios o portátiles, entre otros.

En el proceso DSS02 relacionado con la gestión de peticiones e incidentes de servicio del estándar mundial COBIT 5, es su práctica de gestión DSS02.01 "*Definir esquemas de clasificación de incidentes y peticiones de servicio"*, en sus actividades de control se detalla:

> *"**DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio**. Definir esquemas y modelos de clasificación de incidentes y peticiones de servicio.*
>
> 1. *Definir esquemas y modelos de clasificación de incidentes y peticiones de servicio.*
>
> 2. *Definir esquemas de clasificación y priorización de incidentes y peticiones de servicio y criterios para el registro de problemas, para asegurar enfoques consistentes en el tratamiento, informando a los usuarios y realizando análisis de tendencias.*
>
> 3. *Definir modelos de incidentes para errores conocidos con el fin de facilitar su resolución eficiente y efectiva.*
>
> 4. *Definir modelos de peticiones de servicio según el tipo de petición de servicio correspondiente para facilitar la auto-ayuda y el servicio eficiente para las peticiones estándar..."*

También en el COBIT 5, en las actividades de control número 1 y 3 de la práctica de gestión DSS02.02 sobre el registro, clasificación y priorización de los posibles incidentes tecnológicos, se menciona lo siguiente:

> *"**DSS02.02 Registrar, clasificar y priorizar peticiones e incidentes**.*
> *Identificar registrar y clasificar peticiones de servicio e incidentes, y asignar una prioridad según la criticidad del negocio y los acuerdos de servicio.*

*1. Registrar todos los incidentes y peticiones de servicio, registrando toda la información relevante de forma que pueda ser manejada de manera efectiva y se mantenga un registro histórico completo…*

*3. Priorizar peticiones de servicio e incidentes según la definición de impacto en el negocio del ANS y la urgencia."*

Dentro de las razones principales por las que no se cuenta con la definición, clasificación y priorización aquí indicada, es que no se cuenta con normativa interna que regula la obligatoriedad de ejecutar estos controles.

Una de las consecuencias de no contar con un detalle específico sobre los controles de incidentes tecnológicos detallados, es que podrían presentarse eventuales complicaciones en TI que afecten la continuidad operativa del Banco y que no se logren solventar con la prontitud y acciones adecuadas.

## 2.2 Causas y criterios sobre problemas tecnológicos

La revisión sobre el tema de incidentes de TI, arrojó como parte de sus resultados que no se tienen registradas las causas más probables que afectan directa o indirectamente los diferentes servicios que ofrece el área de tecnologías, así como tampoco se han determinado según los conocimientos disponibles, soluciones temporales o permanentes para dichos problemas. En este sentido tampoco se cuenta con criterios preestablecidos para decidir cuándo un nuevo problema debe ser plasmado en la lista de incidentes tecnológicos que deben controlarse.

Sobre estos temas, las actividades 1 y 2 de la práctica de gestión DSS02.04 concerniente a la investigación y solución de incidentes tecnológicos, del estándar COBIT 5, indica:

*"**DSS02.04 Investigar, diagnosticar y localizar incidentes.***
*Identificar y registrar síntomas de incidentes, determinar posibles causas y asignar recursos a su resolución.*

*1. Identificar y describir síntomas relevantes para establecer **las causas más probables de los incidentes**. Hacer referencia a los recursos de conocimiento disponibles (incluyendo errores y problemas conocidos) para identificar posibles resoluciones de incidentes (soluciones temporales y/o soluciones permanentes).*

*2. Registrar un nuevo problema si un problema relacionado o error conocido no existe aún y **si el incidente satisface los criterios acordados para registro de problemas**."* El destacado es propio.

Una de las causas de que no se estén controlando las causas de los incidentes, así como la definición de posibles soluciones, es que en el Departamento de TI se han venido desarrollando otras actividades tanto para el cumplimiento normativo como para la mejora en los servicios ofrecidos, quedando con un tiempo limitado para la implementación de más controles.

La carencia de este tipo de controles puede ocasionar atrasos en el restablecimiento de cualquiera de los servicios tecnológicos con los que cuenta el Banco, al no contar con estudios previos que determinen la manera más conveniente y efectiva para corregir las situaciones más probables.

## 2.3 Escalamiento de incidentes tecnológicos

De acuerdo con los problemas de tecnologías de información que se presente, puede ser necesario que se deba escalar la situación a distintas instancias según el impacto que la misma tenga en la institución, así como las acciones necesarias a ejecutar para solucionar el evento. Al respecto se determinó que no se cuenta con un control para dar seguimiento al escalado de incidentes, ni a las acciones empleadas para solventar las situaciones generadas. Sobre este particular, tampoco se localizó un detalle de tendencias ni patrones sobre los problemas recurrentes, que puedan utilizarse como insumos para una mejora continua.

En la práctica de gestión DSS02.07 "*Seguir el estado y emitir informes*", del COBIT 5, encontramos ciertas actividades de control que regulan el tema tratado:

> *"**DSS02.07 Seguir el estado y emitir de informes**.*
> *Hacer seguimiento, analizar e informar de incidentes y tendencias de cumplimiento de peticiones, regularmente, para proporcionar información para la mejora continua.*
>
> *1. Supervisar y hacer seguimiento del escalado de incidentes y de resoluciones y de los procedimientos de gestión de resoluciones para progresar hacia la resolución o cumplimentación…*
>
> *3. Analizar incidentes y peticiones de servicio por categoría y tipo para establecer tendencias e identificar patrones de asuntos recurrentes, infracciones de ANSs o ineficiencias. Utilizar la información como entrada a la planificación de la mejora continua."* El subrayado es propio.

El artículo 4.1 "*Actividades de control*", del anual de Normas de Control Interno N-2-2009-CO-DFOE de la Contraloría General de la República (CGR), dicta lo siguiente:

> *"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."* La sección subrayada no pertenece al texto original.

El punto a) del artículo 16.1.1 sobre responsabilidades y procedimientos del estándar INTE/ISO/IEC 27002:2016, detalla los siguientes temas normativos:

> *"Las siguientes directrices para las responsabilidades y procedimientos de gestión relacionado con la gestión de incidentes de seguridad de la información deberían considerarse:*
>
> *a) deberían establecerse responsabilidades de gestión para asegurarse de que los siguientes procedimientos sean desarrollados y comunicados adecuadamente dentro de la organización:*
>
> *1) procedimientos para la planificación y preparación de respuesta a incidentes;*
>
> *2) procedimientos para el seguimiento, detección, análisis e informe de eventos e incidentes de seguridad de la información;*
>
> *3) procedimientos para el registro en bitácora de las actividades de gestión de incidentes;*
>
> *4) procedimientos para el manejo de evidencia forense;*
>
> *5) procedimientos para la evaluación y la decisión sobre los eventos de seguridad de la información así como la evaluación de las debilidades de seguridad de la información;*
>
> *6) procedimientos de respuesta incluyendo aquellos para el escalamiento, la recuperación controlada de un incidente y la comunicación a personas internas o externas u organizaciones"*

Como principal razón de la carencia de los controles detallados en este hallazgo, se encuentra la falta de normativa que regule y obligue tener administradas las debilidades detectadas.

Una de las principales consecuencias de no tener oficializado un proceso de escalamiento de incidentes tecnológicos, es que no se cuente con la jerarquía suficiente para tomar determinadas decisiones según el impacto que el problema esté incidiendo en el Banco, viéndose afectada la prontitud en la solución del mismo.

## 2.4 Proceso disciplinario por violaciones de seguridad

Al evaluar ciertas secciones sobre la administración de incidentes de TI, no se logró identificar un proceso de comunicación hacia la Dirección Administrativa o Gerencia General (según corresponda), cuando cualquiera de los empleados del Banco que por error, negligencia o alevosía provoquen violaciones a la seguridad lógica de la información (sistemas, bases de datos, información institucional, etc.) o al hardware institucional (portátiles, equipos estacionario, equipos de comunicación, servidores de datos, entre otros).

En el artículo 16.1.1, inciso c), puntos 3 y 4 del estándar INTE/ISO/IEC 27002:2016, se indica sobre el proceso disciplinario de incidentes lo que se detalla:

> *"**16.1.1 Responsabilidades y procedimientos***
>
> *Las siguientes directrices para las responsabilidades y procedimientos de gestión relacionado con la gestión de incidentes de seguridad de la información deberían considerarse:*
>
> *(…)*
>
> *c) los procedimientos de presentación de informes deberían incluir:*
>
> *3) la referencia a un **proceso disciplinario formal establecido para tratar con los empleados que cometen violaciones de la seguridad***
>
> *4) procesos de retroalimentación adecuados para asegurarse de que **las personas que informan los eventos** de seguridad de la información sean **notificadas de los resultados** después de que el asunto haya sido tratado y cerrado;"* El destacado es nuestro.

La principal razón por la que no se cuenta con un proceso de comunicación sobre las violaciones a la seguridad tecnológica, se debe a que al momento de la auditoría no se contaba con documentación formal que normara las acciones específicas que deben ejecutarse para gestionar tales situaciones.

Una eventual consecuencia de no contar con este tipo de controles, es que en una situación donde exista ya sea pérdida o robo de información, o daños sobre los equipos del Banco por parte de algún funcionario interno, indistintamente de su origen, podría presentarse vacíos legales en caso de que la institución desee continuar con algún proceso sancionatorio o judicial si fuera necesario.

## 3. CONCLUSIÓN

Al evaluar las actividades ejecutadas por el Departamento de Tecnologías de Información concernientes con la administración y atención de los incidentes tecnológicos, se evidencia un avance en lo que a normativa y controles sobre este particular se refiere, tomando en cuenta principalmente los esfuerzos para ir cumpliendo con muchos temas adicionales que solicitan las normativas externas aplicables, tanto de la Contraloría General de la República como de SUGEF.

Sin embargo, se localizaron algunos aspectos de control y administración en este ámbito que necesitan replantearse o definirse, todo con la finalidad de que la continuidad de cualquiera de los servicios tecnológicos se mantengan activos la mayoría del tiempo o en caso de necesitar reestablecerse, se ejecute el proceso a la brevedad posible, siendo el Banco el mayor beneficiado con tales mejoras.

El enfoque de la Auditoría Interna en este tipo de evaluaciones es recalcar aspectos que pueden mejorar tanto el control interno como la operativa del proceso, para lo cual se detallan en la siguiente sección las recomendaciones específicas de cada hallazgo encontrado.

## 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."*

## *4.1* Esquemas de Administración de incidentes de TI

**Al Departamento de TI**

4.1.1 Debe normarse la necesidad de identificar, clasificar y priorizar los incidentes tecnológicos, donde se incluya para cada tema los responsables de su ejecución y supervisión.
Nivel de Riesgo: **Medio**

4.1.2 Es necesario establecer un inventario con los diferentes tipos de incidentes a nivel tecnológico que se puedan presentar en el Banco de acuerdo con los insumos y servicios con los que cuenta la institución. Como parte de este control deben incluirse una clasificación según el tipo de eventualidad, así como un establecimiento de prioridades de solución según su impacto, en caso de tener varios acontecimientos para resolver.
Nivel de Riesgo: **Alto**

## *4.2* Causas y criterios sobre problemas tecnológicos

**Al Departamento de TI**

4.2.1 Deben puntualizarse las causas más probables de ocasionar los incidentes tecnológicos de acuerdo con la totalidad de insumos institucionales en este ámbito. Parte del control debe incluir un apartado para soluciones transitorias o permanentes según el problema que pueda acontecer, con el fin de que la continuidad del Banco se vea afectada lo menos posible.
Nivel de Riesgo: **Alto**

4.2.2 Cuando se presenten nuevos incidentes tecnológicos en el Banco, como parte de su control, es necesario establecer criterios técnicos y operativos que ayuden a determinar si es necesario incluir los nuevos problemas (mismos que generaron la situación) en el inventario de situaciones que deben ser administradas.
Nivel de Riesgo: **Medio**

## *4.3* Escalamiento de incidentes tecnológicos

**Al Departamento de TI**

4.3.1 Debe elaborarse un procedimiento que norme oficialmente el escalado de incidentes tecnológicos, con el objetivo de tener claridad cuál funcionario, cargo o área sería el responsable de tomar determinadas decisiones de acuerdo a las circunstancias que se estén presentando y al impacto que estas tengan en la operativa de la institución.
Nivel de Riesgo: **Alto**

4.3.2 Debe normarse un control con el que se lleve un histórico o bitácora de las acciones que fueron ejecutadas para solucionar determinados incidentes tecnológicos, el cual pueda utilizarse como insumo para resolver más ágilmente situaciones futuras similares.
Nivel de Riesgo: **Medio**

4.3.3 Es necesario implementar un control sobre el establecimiento de tendencias a nivel de problemas tecnológicos, así como la identificación de patrones sobre problemas recurrentes, esto con la finalidad de ir creando un proceso de mejora continua en lo que a administración de incidentes tecnológicos se refiere.
Nivel de Riesgo: **Bajo**

## 4.4 Proceso disciplinario por violaciones de seguridad

**Al Departamento de TI**

4.4.1 En el momento en que el Departamento de TI detecte que por error, negligencia o alevosía, que algún usuario cometa violaciones a la seguridad desde el punto de vista tecnológico (lógico o físico), y que tales violaciones afecten o no, los activos de TI la institución; deberá generar un informe para la Dirección Administrativa y/o Gerencia General con copia a la jefatura inmediata, en donde se detallen al menos los siguientes aspectos:

- Nombre y/o credenciales de acceso del funcionario.
- Detalle de la violación a la Seguridad detectada.
- Impacto de la violación sobre los activos de TI de la Institución.
- Un detalle de las consecuencias (de existir) de la acción ejecutada, incluyendo posibles costos en caso de poder ser identificados.

Nivel de Riesgo: **Alto**

**Estudio realizado por:**

JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)

Firmado digitalmente por JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)
Fecha: 2021.01.28 12:19:12 -06'00'

**MATI. Jorge Ramirez Bolaños**
**Auditor Encargado**

GUSTAVO FLORES OVIEDO (FIRMA)

Firmado digitalmente por GUSTAVO FLORES OVIEDO (FIRMA)
Fecha: 2021.01.28 14:49:19 -06'00'

**Aprobado MBA Gustavo Flores Oviedo**
**Auditor Interno**