BANCO HIPOTECARIO DE LA VIVIENDA
AUDITORÍA INTERNA

Informe Final TI-OP-003-2020

AUDITORÍA SOBRE LOS SERVICIOS DE RED INSTITUCIONAL

18/03/2021

RESUMEN EJECUTIVO

La revisión estuvo enfocada en valorar los controles existentes relacionados con los servicios de red institucional administrados por Tecnologías de Información.

Dentro de los aspectos a mejorar, se encontró que no se cuenta con normativa sobre los criterios a utilizar para segregar las diferentes subredes con las que cuenta la institución.

El estudio también arrojó como resultado la inexistencia de normativa para administrar los incidentes de emergencias debido a las conexiones remotas.

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 SEGREGACIÓN DE REDES 6
2.2 PROTOCOLO DE EMERGENCIA 7

3. CONCLUSIÓN **9**

4. RECOMENDACIONES **10**

4.1 SEGREGACIÓN DE REDES 11
4.2 PROTOCOLO DE EMERGENCIA 11

AUDITORÍA SOBRE LOS SERVICIOS DE RED INSTITUCIONAL

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 relacionados con la administración de los servicios de red institucionales ofrecidos por el Departamento de Tecnologías de Información.

1.3 Alcance

El estudio abarcó los controles, la documentación, información y procesos operativos vigentes al 30 de Noviembre 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:

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

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 Segregación de Redes

Al evaluar ciertos controles referentes a la administración de la red, se logró determinar que no se han establecido a nivel normativo los requisitos de seguridad para la definición y establecimiento de los criterios a utilizar para segregar las distintas subredes establecidas en el Banco y por ende el respectivo acceso lógico que se le debe brindar a cada funcionario según los privilegios previamente establecidos.

En la sección 13.1.3 relacionada con la segregación de la red del apartado 13 "*Seguridad de las comunicaciones*", del código de buenas prácticas para controles de seguridad de la información ISO 27002:2016, se detalla lo siguiente:

> *"El criterio para la segregación de las redes en dominios y permitir el acceso a través de puertas de enlace debería basarse en una evaluación de los requisitos de seguridad de cada dominio. La evaluación debería ser acorde con la política de control de acceso (ver apartado 9.1.1), los requisitos de acceso, el valor y la clasificación de la información procesada y también tomar en consideración el costo relativo y el impacto en el desempeño de incorporar tecnologías de puertas de enlace apropiadas."*

También en el punto 9.1.1 de la política de control de acceso, de la norma ISO 27002:2016, se indica:

> *"Los propietarios de los activos deberían determinar las reglas de control de acceso apropiadas, los derechos de acceso y las restricciones para las funciones específicas de los usuarios, con respecto a sus <u>activos con el nivel de detalle y el rigor de los controles que reflejan los riesgos asociados de seguridad de la información</u>."* El subrayado es propio.

De acuerdo a lo comentado por el área de TI, como parte de las principales razones por las que no se han normado los criterios para la segregación de las subredes, es porque a nivel institucional aún se carece de una política que norme el modelo de clasificación de la información.

Como posible consecuencia de no tener establecido el control definido, es que se puedan dar por error u omisión una incorrecta asignación de permisos lógicos, habilitando la opción de accesos o modificaciones a información relevante del Banco.

2.2 Protocolo de emergencia

Dentro de los controles establecidos para la administración de las conexiones remotas, se detectó la inexistencia de normativa que detalle los protocolos de emergencias a seguir en caso de que se vean comprometidos alguno de los insumos tecnológicos del Banco a causa de cualquiera de las conexiones remotas habilitadas por el Departamento de TI. Según la información recabada, sí existe un procedimiento para evaluar los incidentes de seguridad, pero no de forma específica sobre las conexiones indicadas, mismas que en el año 2020 incrementaron considerablemente debido al teletrabajo implementado en la institución.

El punto h) del artículo 12.1.2 sobre gestión de cambios, el punto 12.1 *"Procedimientos y responsabilidades operacionales", de la norma* ISO 27002:2016, indica lo que prosigue:

> ***"12.1.2 Gestión de cambios***
>
> *Se deberían controlar los cambios de la organización, en los procesos de negocio, recursos de procesamiento de la organización y en los sistemas que afecten la seguridad de la información.*
>
> *(…)*
>
> *h) provisión de un proceso de cambio de emergencia para permitir la <u>implementación rápida y controlada de los cambios necesarios para resolver un incidente</u>…"* El subrayado es propio

De igual forma, en la sección a) del artículo 16.1.1 referente a las responsabilidades y procedimientos, del punto 16.1 *"Gestión de incidentes y mejoras en la seguridad de la información"*, detalla:

> ***"16.1.1 Responsabilidades y procedimientos***
>
> *Se deberían establecer responsabilidades y procedimientos de gestión para asegurarse de tener una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.*
>
> *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…"

Una de las causas por las que no se tenga definido formalmente este tipo de protocolos, se debe a que el área de TI ha venido trabajando en el diseño e implementación de otra gran cantidad de controles referentes a las regulaciones externas que aplican a la institución, mismas que han acaparado el recurso humano disponible para este tipo de actividades.

Al no contar con protocolos establecidos para las posibles emergencias que se presenten en las conexiones remotas, cabe la posibilidad de que se ejecuten actividades o tareas que en el momento de la eventualidad se consideren como la mejor alternativa, pero que al no ser analizadas previamente, puede que no sean la opción correcta para solventar el incidente, generando afectaciones en otras instancias.

3. CONCLUSIÓN

En la auditoría sobre los servicios de red ofrecidos por el Departamento de Tecnologías de Información, se logró determinar un esfuerzo importante para administrar tales servicios y ofrecer un ambiente controlado según los recursos e insumos disponibles.

No obstante, se localizaron algunos aspectos de control y administración en este ámbito que pueden ser mejorados con el desarrollo e implementación de ciertos controles adicionales tanto a nivel normativo como operativo, todo con el fin primordial de mantener los servicios disponibles la mayoría del tiempo y de paso resguardar los activos tecnológicos del Banco.

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 Segregación de Redes

Al Departamento de TI

4.1.1 Deben establecerse a nivel normativo los criterios de seguridad que deben ser implementados al definir la segregación de las redes y subredes del Banco. Al respecto debe valorarse si para el desarrollo de esta actividad es obligatorio contar previamente con la política de clasificación de la información institucional o si por el contrario sí se puede implementar la norma y posteriormente se podría ajustar en caso de ser necesario.

Nivel de Riesgo: **Alto**

4.2 Protocolo de emergencia

Al Departamento de TI

4.2.1 Se debe elaborar la normativa necesaria que detalle los protocolos a seguir cuando se presenten emergencias o alarmas relacionadas con las conexiones remotas y que puedan dañar los equipos o la información del Banco. Dicha normativa debe incluir los flujos de comunicación al personal correspondiente, según el escalamiento del evento y su impacto en la continuidad de la operativa institucional; así como el proceso de generación de los informes que detallen al menos el incidente presentado, los motivos o causas, el impacto en los activos y las acciones ejecutadas para solventar el problema. Este reporte podría servir de insumo para siguientes investigaciones.

Nivel de Riesgo: **Alto**

Estudio realizado por:

JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)

Firmado digitalmente por JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)
Fecha: 2021.03.18 15:29:07 -06'00'

MATI. Jorge Ramirez Bolaños
Auditor Encargado

Firmado digitalmente por GUSTAVO FLORES OVIEDO (FIRMA)
Fecha: 2021.03.19 10:38:08 -06'00'

Aprobado MBA Gustavo Flores Oviedo
Auditor Interno