BANCO HIPOTECARIO DE LA VIVIENDA
AUDITORÍA INTERNA

Informe Final
TI-ES-002-2023

AUDITORÍA ESPECIAL SOBRE EL SISTEMA SIGECE

14/03/2024

RESUMEN EJECUTIVO

Qué examinamos?
El presente estudio se centró en la evaluación de los controles implementados para la administración y operativa del sistema de información denominado Sistema de Seguimiento, Gestión, Control y Evaluación (SIGECE). El periodo de análisis va del 01 de febrero del 2023 al 30 de noviembre del 2023.

Porqué es importante?
La importancia del sistema evaluado radica en que este es utilizado por la Administración para registrar y supervisar todos los acuerdos de la Junta Directiva, para darle seguimiento a todas las recomendaciones de órganos externos, así como para controlar la gestión y administración de toda la correspondencia interna.

Cómo lo auditamos?
Para la ejecución de esta revisión se aplicaron todos los principios aceptados, vigentes y aplicables para la ejecución de este tipo de auditorías relacionadas con sistemas de información, incurriendo desde la evaluación de la normativa pertinente hasta la ejecución de entrevistas directas con los funcionarios involucrados en el proceso.

Qué encontramos?
Dentro del ámbito de las actividades de control susceptibles de mejora, se encontraron debilidades en la administración de usuarios del sistema que por diferentes razones no estén laborando temporalmente en la institución. Asimismo, se localizaron potestades lógicas establecidas en funcionarios del Departamento de TI que sobrepasan sanas prácticas de la administración y control de la información.

Un aspecto adicional que sobresalió durante la revisión fue la carencia de ambientes de desarrollo, control de calidad y producción en estructuras separadas y con los procesos de administración correspondientes. De manera complementaria, se pudo corroborar la existencia de dependencia operativa tanto del proveedor externo que da soporte a los sistemas de la familia Laserfiche, como del funcionario interno al que se le asignó el mantenimiento de tales aplicativos.

Por último y con relación a la administración de servidores de datos de producción que alojan los sistemas antes detallados, se encontró la definición y utilización de un usuario que cuenta con potestades lógicas totales sobre tales equipos.

Qué sigue?
Se emiten a la Administración Activa una serie de recomendaciones dirigidas a la mejora continua del control interno relacionado con el sistema SIGECE y su plataforma de trabajo, denominada Laserfiche. Se abarcas aspectos de mejora sobre el control de cuentas de usuario, sobre la administración de las bases de datos y los ambientes de ejecución de la herramienta, mejora en la ejecución de los flujos de trabajo y en la dependencia del personal, así como un mejor control sobre aspectos lógicos de la infraestructura Laserfiche. Todo este detalle se plasma en el cuerpo del 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 5

2.1 CONTROL SOBRE USO DE CUENTAS 5
Imagen 1- Pantalla de pruebas 5

2.2 ADMINISTRACIÓN DE BASES DE DATOS LASERFICHE 6
2.3 AMBIENTES DE DESARROLLO Y PRODUCCIÓN 7
Imagen 2- Lista Servidores Laserfiche 8

2.4 MANTENIMIENTO Y CREACIÓN DE LOS FLUJOS DE TRABAJO 9
2.5 DEPENDENCIA DE PERSONAL 11
2.6 USUARIO ADMINISTRADOR EN SERVIDOR DE PRODUCCIÓN 12
Imagen 3- Servidor de Producción SV-26 13

3. CONCLUSIÓN 15

4. RECOMENDACIONES 16

4.1 CONTROL SOBRE USOS DE CUENTAS 17
4.2 ADMINISTRACIÓN DE BASES DE DATOS LASERFICHE 17
4.3 AMBIENTES DE DESARROLLO Y PRODUCCIÓN 18
4.4 MANTENIMIENTO Y CREACIÓN DE LOS FLUJOS DE TRABAJO 18
4.5 DEPENDENCIA DE PERSONAL 18
4.6 USUARIO ADMINISTRADOR EN SERVIDOR DE PRODUCCIÓN 19

1. INTRODUCCIÓN

1.1 Justificación de la auditoría

Este estudio se realizó como una solicitud directa del Auditor Interno, como parte de la función asesora de la Auditoría Interna de conformidad con las facultades que nos otorga la Ley 7052 en el artículo No.31 y la Ley 8292 en el artículo No.22.

1.2 Objetivo

Evaluar los controles implementados para la administración y operativa del sistema de información denominado SIGECE.

1.3 Alcance

El estudio abarcó la normativa vigente con corte al 30 de Noviembre del 2023, incluyendo las políticas y procedimientos disponibles en la Intranet institucional.

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:

- ✓ 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
- ✓ Código de buenas prácticas para controles de seguridad de la información INTE/ISO/IEC 27002:2016
- ✓ Marco de referencia de Objetivos de Gobierno y Gestión, COBIT 2019
- ✓ Normativa Interna vigente (Metodología, Manuales, Políticas, Procedimientos, Instructivos y formularios)
- ✓ Norma 308 Comunicación de resultados.

Así mismo, se aplicaron técnicas de auditoría comúnmente aceptadas, así como información solicitada directamente a los usuarios involucrados con 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 oportunidades de mejora detectadas, tanto en aspectos de control interno, como operativas de la presente revisión, se detallan en la siguiente sección de Resultados de la Evaluación.

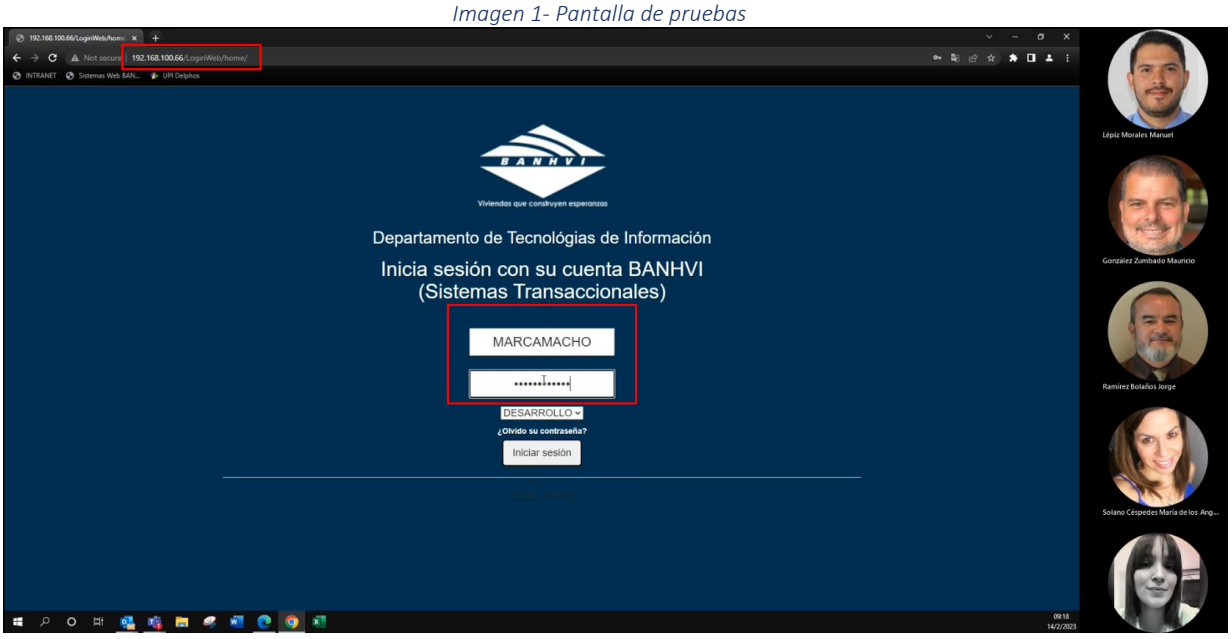
2. RESULTADOS DE LA EVALUACIÓN

2.1 Control sobre uso de cuentas

A solicitud de la Gerencia General mediante oficio BANHVI-GG-OF-1370-2022 y con la finalidad de evaluar posibles alternativas para trasladar el proceso de seguimiento de recomendaciones utilizado por la Auditoría Interna, esto en vista de las inconveniencias operativas y técnicas de la aplicación actualmente utilizada para dicho fin; se realizó una reunión el día 14 de febrero del 2023 con los funcionarios María Solano Céspedes y Manuel Lépiz Morales por parte de la Administración y Selene Serrano Delgado, Mauricio González Zumbado y Jorge Ramírez Bolaños de la Auditoría Interna, para valorar la adaptabilidad de uno de los sistemas vigentes (SIGECE) como base para un nuevo sistema de recomendaciones de auditoría.

Durante la reunión al momento de realizar ciertas pruebas, se logró corroborar la utilización del usuario de la señora Martha Camacho Murillo, ex directora de la unidad del FOSUVI, la cual en ese momento se encontraba incapacitada. Sobre este particular y después de revisarlo con el área de Tecnologías, se determinó que no se ha implementado un control que remita un aviso directo al funcionario que por distintos motivos no esté laborando en la institución de forma temporal y su usuario de sistemas sea utilizado en ese lapso.

Imagen 1- Pantalla de pruebas



Fuente: incorporar la fuente

El artículo 4.6 referente al cumplimiento del ordenamiento jurídico y técnico de las Normas de Control Interno N-2-2009-CO-DFOE, indica:

> *"**4.6 Cumplimiento del ordenamiento jurídico y técnico***
> *El jerarca y los titulares subordinados, según sus competencias, deben establecer las actividades de control que permitan obtener una seguridad razonable de que la actuación de la institución es conforme con las disposiciones jurídicas y técnicas vigentes. Las actividades de control respectivas deben actuar como motivadoras del cumplimiento, prevenir la ocurrencia de eventuales desviaciones, y en caso de que éstas ocurran, emprender las medidas correspondientes. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de sus operaciones y los riesgos relevantes a los cuales puedan verse expuestas, así como los requisitos indicados en la norma 4.2."*

Según el proceso de revisión efectuado, la carencia del control sobre el aviso de uso de cuentas de usuarios que por distintas razones no estén laborando, en algún momento había sido eliminado debido a valoraciones propias del Departamento de TI, estando sin implementar a la fecha de la revisión.

Un posible efecto que esta situación podría ocasionar es que se utilicen permisos de acceso lógico (tales como modificar, eliminar y hasta acceder a datos), que no sean propios de la persona que esté ejecutando la acción, habilitando vulnerabilidades lógicas a la información de los distintos aplicativos de la institución.

2.2 Administración de bases de datos Laserfiche

Uno de los temas evaluados por su relevancia y criticidad, fue el proceso de administración de las bases de datos del sistema SIGECE. Según lo indicado por los técnicos y por la herramienta utilizada para la creación y administración del sistema, este cuenta con tres instancias de bases de datos, una relacionada con todo el proceso documental, otra con las estructuras de lenguaje SQL y la otra que se encuentra en Oracle donde se lleva el seguimiento de la parte documental. En este punto, se encontró que la base de datos documental y de SQL es administrada por el Sr. Manuel Lépiz Morales, funcionario del área de sistemas del Departamento de TI, siendo este funcionario el encargado de darle mantenimiento total al sistema.

Esta situación se aplica de igual forma para la administración del Sistema de Expedientes Digitales y cualquier otro que forme parte de la infraestructura Laserfiche. Además, se encontró que los funcionarios de la empresa externa que da mantenimiento a estos sistemas (Aplicom), también tienen las mismas potestades del señor Lépiz, pudiendo entrar con todos los permisos lógicos (leer, modificar o eliminar) a los mismos servidores de Producción. Los ingresos y permisos a estos servidores por parte del sr. Lépiz o de la empresa Aplicom, son incompatibles con

una adecuada segregación de funciones referente a actualizaciones o modificaciones de versiones o archivos en los servidores de producción.

El punto 1.5 referente a las responsabilidades de los funcionarios sobre el Sistema de Control Interno, del Manual de Normas de Control Interno para el Sector Público de la Contraloría General de la República N-2-2009-CO-DFOE, indica lo siguiente:

> *"De conformidad con las responsabilidades que competen a cada puesto de trabajo, los funcionarios de la institución deben, de manera oportuna, efectiva y con observancia a las regulaciones aplicables, realizar las acciones pertinentes y atender los requerimientos para el debido diseño, implantación, operación, y fortalecimiento de los distintos componentes funcionales del SCI."*

Las Normas de Control Interno para el Sector Publico (N-2-2009-CO-DFOE) de la Contraloría General de la República, en el punto 2.5.3 relacionado con la separación de funciones incompatibles y del procesamiento de transacciones, dictan lo siguiente:

> *"El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que las funciones incompatibles, se separen y distribuyan entre los diferentes puestos; así también, que las fases de autorización, aprobación, ejecución y registro de una transacción, y la custodia de Inventarios, estén distribuidas entre las unidades de la institución, de modo tal que una sola persona o unidad no tenga el control por la totalidad de ese conjunto de labores."* El subrayado es propio.

Según se determinó, la razón por la que un funcionario del área de Sistemas esté administrando en su gran mayoría los sistemas de Laserfiche se debe a que el sr. Lépiz al ser el experto en la herramienta, fue la persona a la que se le encargó en su momento dicha tarea y se ha mantenido así hasta la fecha.

Un efecto directo de esta situación es que existe personal externo al área de Soporte Técnico que está presentando una concentración de funciones, permitiendo a nivel lógico que puedan ver, insertar, modificar o eliminar cualquier información a la que tenga acceso, aunque sean los servicios que se encuentran en producción.

2.3 Ambientes de Desarrollo y Producción

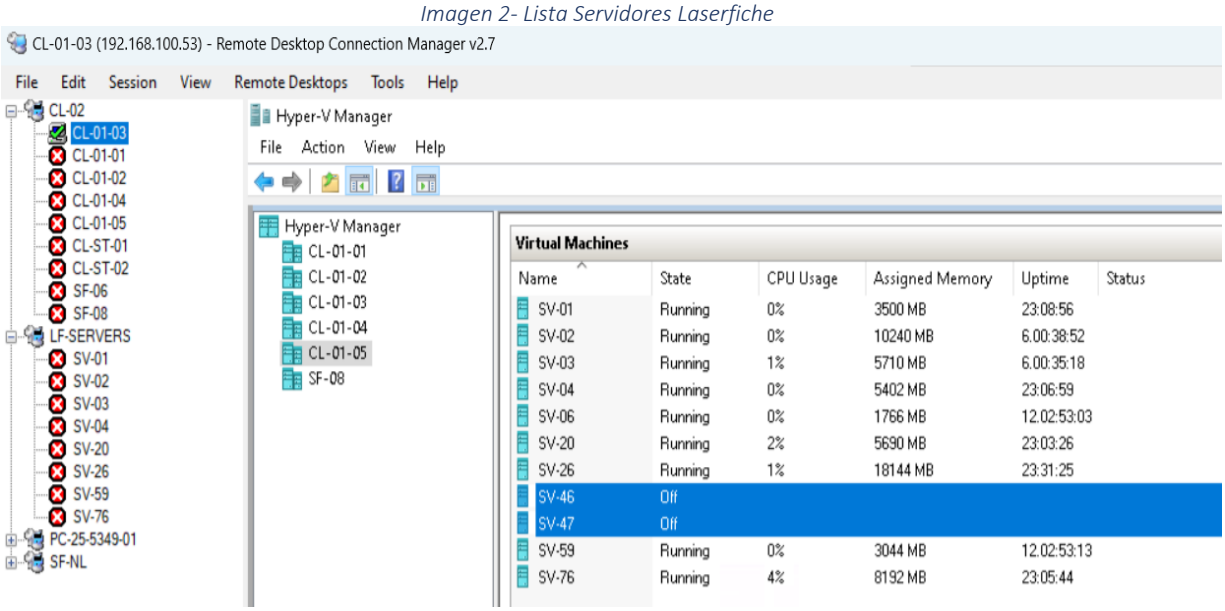
El Banco Hipotecario de la Vivienda adquirió la herramienta Laserfiche hace algunos años con el propósito inicial de automatizar el proceso relacionado con el expediente

digital del bono familiar de vivienda. En ese momento, se definieron los requerimientos necesarios en colaboración con los usuarios responsables del proceso, lo que culminó en el desarrollo de una nueva aplicación.

Tras la implementación del Sistema de Expediente Digital, se reconoció que las capacidades inherentes de Laserfiche podrían extenderse a otros procesos. En el momento de la auditoría actual, se encuentra plenamente implementado el Sistema de Seguimiento, Gestión, Control y Evaluación (SIGECE), que se utiliza para registrar y supervisar acuerdos de la Junta Directiva, recomendaciones de órganos externos y la gestión y control de la correspondencia interna.
En relación con este asunto, se ha constatado que ninguno de estos sistemas dispone de una segregación que permita establecer un entorno de Desarrollo destinado a que los miembros del área de Sistemas puedan llevar a cabo las pertinentes modificaciones, actualizaciones, pruebas y cualquier otro procedimiento requerido por los usuarios finales. De igual manera, no se ha establecido un entorno de Producción donde el sistema albergue datos veraces y se encuentre en pleno funcionamiento, estando a disposición de los usuarios.

Es fundamental resaltar que, a pesar de haber definido servidores específicos para pruebas y producción en el contexto de estos servicios, ambos son utilizados de manera exclusiva por parte del personal del área de Sistemas. Este hecho subraya la carencia de una clara separación entre los ambientes de desarrollo y producción, lo que podría generar desafíos en términos de gestión y control.

Imagen 2- Lista Servidores Laserfiche



El punto 12.1.4 del Código de buenas prácticas para controles de seguridad de la información INTE/ISO/IEC 27002:2016, detalla sobre los ambientes de desarrollo y producción lo siguiente:

"12.1.4 Separación de los ambientes para desarrollo, pruebas y producción

Los ambientes para desarrollo, pruebas y producción deberían estar separados para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.

Debería identificarse e implementarse el grado de separación entre los ambientes de desarrollo, prueba y producción que es necesario para prevenir problemas operacionales…

Las actividades de desarrollo y prueba pueden causar serios problemas, por ejemplo modificación indeseada de archivos o del ambiente del sistema, o fallo del sistema. Hay una necesidad de mantener un ambiente conocido y estable para realizar las pruebas significativas en éste y prevenir el acceso inapropiado del desarrollador al ambiente de producción.

Cuando el personal de desarrollo y de pruebas tiene acceso al sistema en producción y a su información, pueden ser capaces de introducir código no autorizado y no probado o alterar datos en producción. En algunos sistemas, esta capacidad podría ser utilizada para realizar fraude, o introducir código no probado o malicioso, que puede causar problemas operacionales serios.

El personal de desarrollo y prueba también representa una amenaza a la confidencialidad de la información operativa. Las actividades de desarrollo y de prueba pueden causar cambios involuntarios al software o a la información si comparten el mismo ambiente. Por lo tanto, es conveniente separar los recursos para desarrollo, prueba y producción para reducir el riesgo de cambio accidental o acceso no autorizado al software en producción o los datos del negocio (ver apartado 14.3 para la protección de los datos de prueba)."

El motivo principal por el que no se cuente con los entornos de Desarrollo y Producción para los servicios Laserfiche, es que la herramienta cuando se adquirió no fue contemplada para que llegara a ser desarrollada internamente, pero después por su versatilidad se estableció como otra forma de desarrollar e implementar sistemas institucionales.

Los datos en los servidores de Producción pueden ser sensibles o hasta privados, y al no contar con entornos separados, hay un riesgo de que los datos de prueba o desarrollo sean expuestos en la producción, lo que podría comprometer la seguridad, confidencialidad o hasta la integridad de la información.

2.4 Mantenimiento y creación de los Flujos de trabajo

Como parte de los procesos que se utilizan en el desarrollo de los sistemas de Laserfiche (SIGECE y Expediente Electrónico), se encuentran los flujos de trabajo, también conocido como Workflow en inglés, los cuales consisten en una secuencia de pasos, tareas o actividades que se realizan de manera ordenada y sistemática para lograr un objetivo específico dentro de un proceso o proyecto. Estos flujos de trabajo son comunes en una variedad de contextos, desde entornos empresariales hasta proyectos individuales, y se utilizan para gestionar y optimizar la ejecución de tareas.

Al respecto de la creación y mantenimiento de los Workflows implementados en el Banco, en la investigación se logró determinar que tales flujos de trabajo son ejecutados exclusivamente por el proveedor externo (Aplicom) encargado de dar el soporte a dichos sistemas; creando con esto una dependencia total hacia dicha empresa, más tomando en cuenta que el desarrollo y ejecución de dichos flujos de trabajo están ligados directamente con la operativa diaria de los sistemas de Laserfiche.

En el punto 12.1.3 del Código de buenas prácticas para controles de seguridad de la información INTE/ISO/IEC 27002:2016, referente con la gestión de la capacidad, se cita lo siguiente:

> ***"12.1.3 Gestión de la capacidad***
>
> *El uso de los recursos debería ser supervisado, ajustado y basado en proyecciones de los futuros requisitos de capacidad para asegurar el rendimiento del sistema requerido.*
>
> *Los requisitos de capacidad deberían ser identificados, tomando en cuenta la criticidad para el negocio del sistema en cuestión. El ajuste y seguimiento deberían ser aplicados al sistema para asegurar y, cuando sea necesario, mejorar la disponibilidad y la eficacia de los sistemas. Deberían ejecutarse controles de detección para indicar problemas a su debido tiempo. Las proyecciones de los requisitos de capacidad futura deberían tomar en cuenta los nuevos requisitos del negocio y del sistema, así como tendencias actuales y proyectadas en la capacidad de procesamiento de la información de la organización.*
> *Es necesario poner atención a cualquier recurso cuya adquisición toma mucho tiempo o requiere costos elevados; por lo tanto los administradores deberían supervisar la utilización de los recursos clave del sistema. Ellos deberían identificar tendencias en el uso, particularmente en lo referente a las aplicaciones del negocio o herramientas de gestión de sistemas de información.*
> *Los administradores deberían utilizar esta información para identificar y evitar posibles cuellos de botella, así como dependencia de personal clave que*

pudiera presentar una amenaza a la seguridad del sistema o servicios, y planificar la acción apropiada."

La práctica de gestión APO12.03 del Marco de Referencia COBIT 2019,

"***APO12.03 Mantener un perfil de riesgo***.

Mantener un inventario de los riesgos conocidos y los atributos de riesgo, incluidos la frecuencia esperada, impacto potencial y respuestas. Documentar los recursos, capacidades y actividades de control actuales relacionados con elementos de riesgo…

1. Hacer un inventario de los procesos de negocio y documentar su dependencia con los procesos de gestión de servicios de I&T y los recursos de infraestructura de TI. Identificar el personal de apoyo, aplicaciones, infraestructura, instalaciones, registros manuales críticos, contratistas, proveedores, y terceros…"

La causa del porque la creación y el mantenimiento de los flujos de trabajo son realizados por la empresa Aplicom, es que no se ha brindado la capacitación suficiente al personal del área de Sistemas sobre dicha actividad.

Dentro de los efectos directos de mantener la relación actual con la empresa Aplicom a nivel de soporte externo, es que además de generar una dependencia funcional y operativa sobre los productos Laserfiche, no existe la transferencia de conocimiento necesaria para poder desarrollar paulatinamente la actividad con los recursos internos, implicando adicionalmente un gasto considerable todos los años sobre este rubro.

2.5 Dependencia de Personal

Con el fin de llevar un mejor control sobre las necesidades de los usuarios y sobre el avance de los proyectos de los sistemas Laserfiche, a nivel institucional se contrató en su momento a personal interino que sirviera de contraparte técnica para ayudar a controlar tales servicios, esto hasta el punto de tener la necesidad de contar con personal en propiedad que supliera dichas necesidades. Sobre este tema, se contrató al señor Manuel Lépiz Morales, funcionario que actualmente labora para el Banco pero que, en el momento de la auditoría, se encontraba incapacitado por temas de salud, evidenciando en ese momento una dependencia muy marcada de este empleado sobre el mantenimiento y conocimiento de los sistemas que tiene bajo su responsabilidad, específicamente todos los relacionados con Laserfiche.

En la práctica de gestión APO07.02 de los Objetivos de Gobierno y Gestión del COBIT 2019, detalla sobre el personal clave de TI:

*"**APO07.02 Identificar al personal clave de TI.***
Identificar al personal clave de TI. Usar la captura de conocimientos (documentación), intercambio de conocimientos, planificación de sucesión y personal de respaldo para minimizar la dependencia en un único individuo que realice un trabajo crítico…

3. Usar la captura de conocimientos (documentación), intercambio de conocimientos, planificación de sucesión y personal de respaldo para minimizar la dependencia en un único individuo que realice un trabajo crítico."

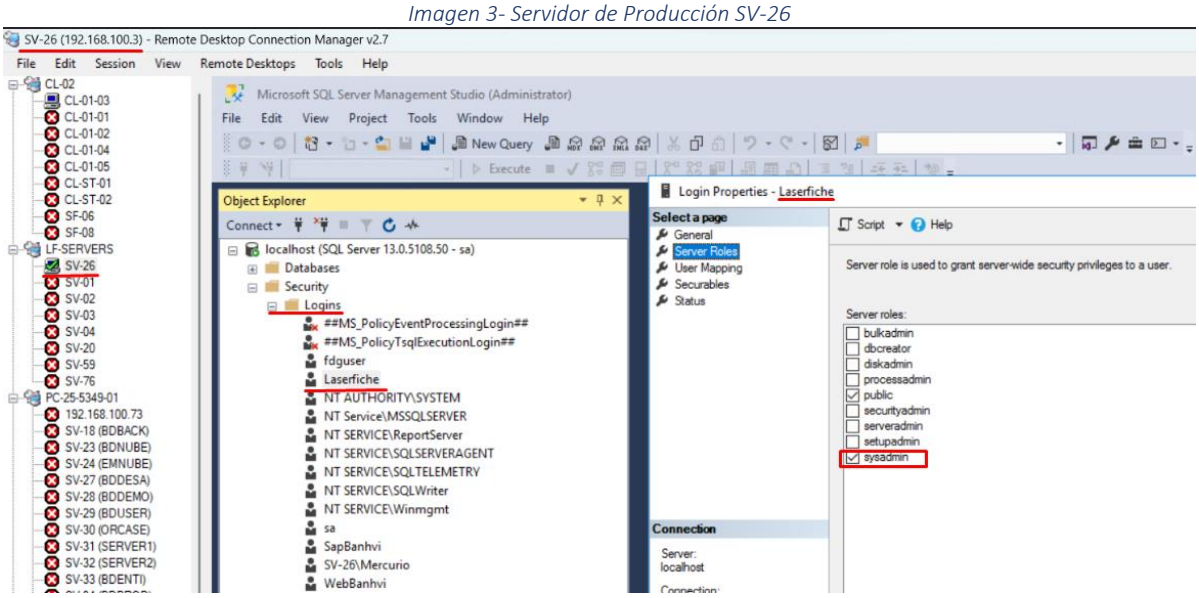
Uno de los motivos principales de que se presenten inconvenientes sobre el mantenimiento o desarrollo de aplicativos en Laserfiche en ausencia del sr. Lépiz, es que en se ha carecido de un proceso de capacitación más especializada sobre el uso de dicha herramienta, aunado a una limitada rotación de funciones sobre esos mismos sistemas.

Algunos de los efectos de contar con la dependencia de un funciono es que se vea afectada la continuidad del negocio en caso de ausencias, renuncias o cambios en el personal. Además, se puede limitar la operación propia de las áreas funcionales que dependen de esos sistemas en su labor diaria, situación que se logró evidenciar al momento de la revisión.

2.6 Usuario Administrador en servidor de Producción

En el proceso de evaluación de los servidores destinados para alojar todos los productos de Laserfiche, se encontró que en el servidor de producción SV-26 (donde se encuentran el sistema de SIGECE y Expediente Digital), existe un usuario denominado Laserfiche, mismo que tiene asignado el rol de administrador sobre dicho equipo, siendo además utilizado para darle mantenimiento y soporte a esos sistemas, actividad que tal como se indicó en párrafos anteriores, es ejecutada por el personal del área de Sistemas y por la empresa Aplicom. Seguidamente se muestra una imagen sobre este punto.

Imagen 3- Servidor de Producción SV-26



En el artículo 4.5 de las Normas de Control Interno para el Sector Publico (N-2-2009-CO-DFOE), se dicta lo siguiente:

> ***"4.5 Garantía de eficiencia y eficacia de las operaciones***
> *El jerarca y los titulares subordinados, según sus competencias, deben establecer actividades de control que orienten la ejecución eficiente y eficaz de la gestión institucional. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de sus operaciones y los riesgos relevantes a los cuales puedan verse expuestas, así como los requisitos indicados en la norma 4.2"*

Adicionalmente el punto c) del artículo 2.1 sobre el ambiente de control, del Manual de Normas de Control Interno N-2-2009-CO-DFOE de la CGR, detalla lo siguiente:

> *"El jerarca y los titulares subordinados, según sus competencias, deben establecer un ambiente de control que se constituya en el fundamento para la operación y el fortalecimiento del SCI, y en consecuencia, para el logro de los objetivos institucionales. A los efectos, debe contemplarse el conjunto de factores organizacionales que propician una actitud positiva y de apoyo al SCI y a una gestión institucional orientada a resultados que permita una rendición de cuentas efectiva…"*

En el artículo 9.4.5 del Código de buenas prácticas para controles de seguridad de la información INTE/ISO/IEC 27002:2016, también se indica:

"***9.4.5 Control de acceso al código fuente de programas***

El acceso al código fuente de programas e ítems asociados (como diseños, especificaciones, planes de verificación y validación) debería estar estrictamente controlado, para prevenir la introducción de una funcionalidad no autorizada y evitar cambios involuntarios, así como mantener la confidencialidad de la propiedad intelectual valiosa…"

De acuerdo con la investigación, el motivo por el que se cuente con un usuario Laserfiche con privilegios de administrador sobre un equipo de producción, es porque en la definición de ciertos procesos de los sistemas SIGECE o Expediente Electrónico, es necesaria esa configuración para que puedan ser ejecutados correctamente, esto porque así fueron definidos desde un inicio y no se han realizado las modificaciones correspondientes para que se ejecuten de otra manera.

Un posible efecto de que se mantenga un usuario administrador en un equipo de producción que sea usado para el mantenimiento de los sistemas, es que se pueden ver afectados temas de confidencialidad e integridad de la información de tales aplicativos.

3. CONCLUSIÓN

Como parte de los productos tecnológicos que el Banco ha adquirido y desarrollado en los últimos años, se empezaron a implementar sistemas de información basados en tecnologías diferentes a los estándares normalmente utilizados por el Departamento de TI, específicamente con estructuras de bases de datos en SQL (Structured Query Language) y desarrollos en Visual Basic.Net. Esto provocó la necesidad de adaptarse a nuevos insumos tecnológicos tanto a nivel técnico como a nivel operativo.

En la revisión realizada por la Auditoría Interna se pudieron identificar ciertos temas específicos que pueden ser mejorados con el desarrollo e implementación de controles normativos y operativos detallados en este informe, mismos que forman parte del ciclo normal en la puesta en práctica de herramientas tecnológicas y son parte esencial del control interno para garantizar la integridad operativa, la rendición de cuentas y la mitigación de riesgos, contribuyendo así al éxito a largo plazo y la sostenibilidad de la institución.

La finalidad de este informe es que la Administración Activa pueda identificar y mejorar puntos específicos en el uso de estas tecnologías, tratando de mantener una mejora continua necesaria en lo que a control interno se refiere. Para esto, se detallan en la siguiente sección de este informe recomendaciones específicas orientadas a dicho fin.

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 Control sobre usos de cuentas

Al Departamento de TI

Se recomienda que se implemente un control que avise automáticamente cada vez que se utilice un usuario de los sistemas de información del Banco que por distintas situaciones no se encuentre laborando en la institución, ya sea por vacaciones, incapacidad, permisos, despidos, renuncias, etc. El aviso debe ser remitido por medio de correo electrónico directamente al dueño de la cuenta, a la jefatura inmediata, a la jefatura del Departamento de TI y a la jefatura de la Unidad de Riesgos. Además, debe generarse un historial de dichos movimientos, para futuras revisiones de órganos fiscalizadores.

Nivel de Riesgo: **MEDIO**

4.2 Administración de bases de datos Laserfiche

Al Departamento de TI

4.2.1 Es necesario que se desligue de las funciones operativas del señor Manuel Lépiz Morales, todas aquellas que tengan relación con la administración y control de los procesos de Producción para todos los sistemas actuales que forman parte de la infraestructura Laserfiche, incluyendo el SIGECE y el Expediente Electrónico. Esto también debe implementarse para cualquier otra aplicación o sistema que sea desarrollado en un futuro bajo la estructura Laserfiche.

Nivel de Riesgo: **ALTO**

4.2.2 Se deben realizar las modificaciones pertinentes para que en adelante los funcionarios de la empresa Aplicom no puedan ingresar ni dar mantenimientos directos sobre los servidores de Producción.
Con este control implementado se asegura que exista un proceso de segregación adecuado, al ser otros funcionarios totalmente aparte del área de Sistemas o de una empresa externa (específicamente personal de Soporte Técnico) los que ejecutan las actualizaciones correspondientes en los servidores de Producción.

Nivel de Riesgo: **ALTO**

4.3 Ambientes de Desarrollo y Producción

Al Departamento de TI

Se deben realizar las gestiones correspondientes tanto a nivel operativo como administrativo, para que se creen y separen los entornos donde se administran los sistemas de Laserfiche, incluyendo el SIGECE. Para esto, además de crear los entornos de Desarrollo y Producción tal como se tienen en los sistemas de Oracle, es necesario que se incluya como parte de los procesos de control de TI un entorno de Control de Calidad (QA) tanto para los sistemas Laserfiche como para los sistemas de Oracle, con el cual se pueda mejorar la calidad de los productos finales, se puedan validar adecuadamente los requisitos y expectativas de los usuarios, se reduzcan los costos y tiempos asociados con la corrección de problemas en etapas avanzada de desarrollo o después de la implementación, sea factible realizar pruebas extensivas antes de la implementación en producción, se pueda asegurar que el software cumple con los estándares de calidad aplicables al Banco y en general contribuya a la eficiencia del desarrollo y a la satisfacción del cliente final.

Nivel de Riesgo: **ALTO**

4.4 Mantenimiento y creación de los flujos de trabajo

Al Departamento de TI

Es necesario que se capacite al personal del área de Sistemas en la creación, mantenimiento y soporte de los flujos de trabajo implícitos en los sistemas de Laserfiche, en este caso el SIGECE, el Expediente Digital y cualquier otro que se desarrolle teniendo esa herramienta como base. Con esto, en un lapso razonable toda la actividad relacionada con dichos Workflows podrá ser ejecutada por personal del Departamento de TI, trasladando implícitamente el conocimiento entre tales funcionarios.

Nivel de Riesgo: **ALTO**

4.5 Dependencia de Personal

Al Departamento de TI

4.5.1 Es necesario que se defina un proceso de capacitación más especializada en el uso de las herramientas con las que se le brinda soporte a los sistemas relacionados con el Laserfiche (SIGECE y Expediente Digital), esto para que diferente personal del área de Sistemas pueda hacer los mantenimientos o cambios necesarios a los aplicativos, en ausencia del personal clave de este producto.

Nivel de riego: **ALTO**

4.5.2 Como parte de la mejora continua del proceso de administración de recursos del Departamento de TI, deben implementarse actividades enfocadas a incentivar la rotación del personal de TI sobre las distintas actividades, tareas y productos que son ejecutados normalmente por una sola persona. Con esto se asegura una mayor resiliencia a largo plazo sobre futuras contingencias relacionadas con tecnologías de información.

Nivel de riego: **ALTO**

4.6 Usuario Administrador en servidor de Producción

Al Departamento de TI

Se deben efectuar los cambios pertinentes para que se deje de utilizar el usuario Laserfiche o cualquier otro que sea utilizado bajo la misma premisa de dar mantenimiento a los sistemas de dicha suite, para esto además de revocar los permisos de administrador de cualquier equipo de producción donde sea utilizado, se deben modificar los procesos de los aplicativos que lo ameriten, permitiendo un adecuado flujo en los procesos de mantenimiento y soporte de esos equipos según los estándares aplicables a la institución.

Nivel de Riesgo: **ALTO**

Estudio realizado por:

JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)

Firmado digitalmente por JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)
Fecha: 2024.03.14 15:14:44 -06'00'

MATI. Jorge Ramírez Bolaños
Auditor Encargado

Firmado digitalmente por GUSTAVO FLORES OVIEDO (FIRMA)
Fecha: 2024.03.14 15:27:19 -06'00'

Aprobado MBA. Gustavo Flores Oviedo
Auditor Interno