BANCO HIPOTECARIO DE LA VIVIENDA
AUDITORÍA INTERNA

Informe Final TI-OP-001-2020

AUDITORÍA SOBRE LA INFORMACIÓN ALMACENADA EN LOS SERVIDORES DE DATOS

19/06/2020

RESUMEN EJECUTIVO

La revisión estuvo enfocada en valorar los principales controles implementados para asegurar la consistencia, integridad y disponibilidad de la información almacenada en los servidores de datos del Banco.

En primera instancia, se determinó que desde el mes de setiembre del 2019 que fue cuando se instaló la última versión del gestor de bases de datos del Banco (Oracle 12c), se dejaron operando varios sistemas de información sin pistas de auditoría o con algunas muy limitadas.

Referente al Sistema de Expedientes Digitales, la auditoría detectó que la aplicación ya se encuentra en producción, pero instalada en un servidor de datos que no es el correcto. Además, se localizó la existencia y uso de un usuario con permisos lógicos que atenta contra la seguridad e integridad de la información del sistema.

Para ingresar a los sistemas de información institucionales, se encontró la posibilidad de acceder a la información de ciertas aplicaciones utilizando herramientas de terceros distintas a las oficializadas, lo que genera el riesgo de alteraciones a las bases de datos de forma incorrecta y sin ser detectadas.

Por último, se localizaron debilidades de control sobre la administración y actualización de las formas, reportes, librerías y Scripts que se ejecutan en los servidores de producción.

Los detalles de cada aspecto indicado en los párrafos anteriores son ampliados a 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 PISTAS DE AUDITORÍA EN SISTEMAS DE INFORMACIÓN 6
2.2 SISTEMA DE EXPEDIENTES DIGITALES 7
2.3 HERRAMIENTAS EXTERNAS DE CONEXIÓN A LAS BASES DE DATOS 10
2.4 MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN 11

3. CONCLUSIÓN **14**

4. RECOMENDACIONES **15**

4.1 PISTAS DE AUDITORÍA EN SISTEMAS DE INFORMACIÓN 16
4.2 SISTEMA DE EXPEDIENTES DIGITALES 16
4.3 HERRAMIENTAS EXTERNAS DE CONEXIÓN A LA BASE DE DATOS 17
4.4 MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN 18

Ilustración 1 - Usuario Local Laserfiche como Administrator en SV-01/20/26 8
Ilustración 2 - Ejemplo movimientos con System efectuados por diferentes funcionarios 12

AUDITORÍA SOBRE LA INFORMACIÓN ALMACENADA EN LOS SERVIDORES DE DATOS

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 lógicos vigentes para asegurar la consistencia, integridad y disponibilidad de la información almacenada en los principales servidores de datos del Banco.

1.3 Alcance

El estudio abarcó la documentación, información y procesos operativos vigentes al 31 de Enero del 2020, relacionados con los controles utilizados para la administración de la información en los servidores de datos.

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 relacionada con la revisión, así como información solicitada a los usuarios involucrados la cual en su mayoría fue remitida por medio de correo electrónico. Adicional se evaluaron controles implementados por las áreas involucradas para mejorar la administración del tema evaluado.

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 Pistas de Auditoría en Sistemas de Información

Como parte del proceso de auditoría, se evaluó la implementación y uso en general de pistas de auditoría sobre los distintos sistemas de información utilizados en la institución. Al respecto se pudo comprobar que actualmente gran parte de las aplicaciones no están registrando de forma parcial o total los controles de cambios no autorizados o modificaciones que se ejecutan por excepciones y que en su momento se habían definido por los dueños de los sistemas como bitácoras para seguimientos posteriores. Como parte de los sistemas afectados con esta situación están el Sistema de Vivienda, Contabilidad, Préstamos, Cheques, Certificados de Depósito a Plazo, Juicios, Inventarios, Compras, entre otros.

El artículo 12.1.2 sobre la Gestión de Cambios, del estándar INTE/ISO/IEC 27002:2016, detalla como parte de su control:

> *"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….*
>
> *Deberían establecerse las responsabilidades y los procedimientos formales de gestión para asegurar el control satisfactorio de todos los cambios. Cuando se realizan los cambios, debería conservarse una bitácora de auditoría conteniendo toda la información pertinente."* Lo subrayado es propio.

En la actividad de control número 1 de la práctica de gestión DSS02.02 "*Registrar, clasificar y priorizar peticiones e incidentes*", del COBIT 5, se menciona:

> *"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***". Lo destacado es nuestro.

El motivo por el que varios de los sistemas de información del Banco estén operando sin pistas de auditoría, se debe a que desde el mes de Setiembre del año 2019, el Departamento de Tecnologías de Información migró a la versión 12c de Oracle, misma que por motivos técnicos no pudo trasladar todas las bitácoras de sistemas implementadas en la versión de Oracle anterior, unas con la herramienta AuditCase y otras de forma directa en la base de datos.

Como efecto de no contar con pistas de auditoría en las aplicaciones del Banco, es que se estén ejecutando de forma incorrecta o dolosa transacciones no autorizadas en los sistemas, como por ejemplo cambios en los montos de bonos o cédulas en beneficiarios, cambios en detalles de asientos ya registrados, modificaciones de montos de préstamos, cambios en fechas relevantes, alteraciones en montos de cheques, eliminación de algún registro, entre otros; y que ninguno de estos cambios pueda ser detectado o darle un adecuado seguimiento por los dueños de cada sistema.

2.2 Sistema de Expedientes Digitales

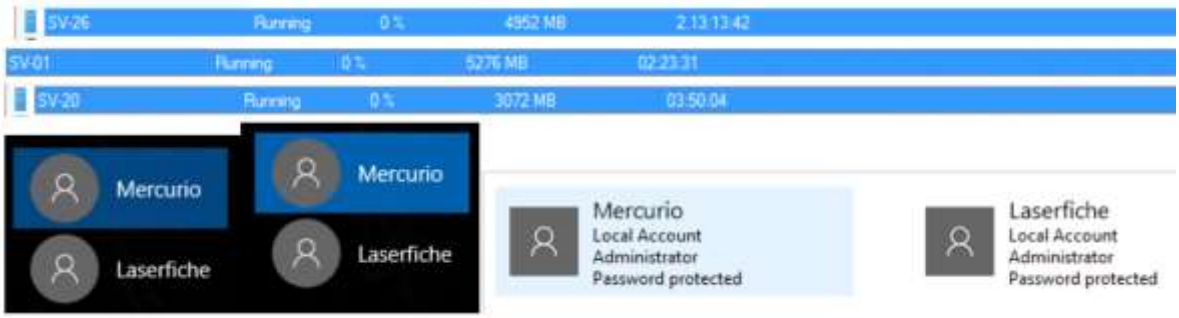
En el año 2019, se terminaron de realizar los ajustes necesarios para poner a operar el nuevo Sistema de Expedientes Digitales, el cual según lo indicado por el señor Alexis Solano, empezó a operar con casos reales desde finales del 2019 con registros de MUCAP y seguidamente con Coopeservidores, que es la Entidad con la que actualmente se está trabajando. Referente al uso de este sistema, se encontró que a pesar de que ya está operando a nivel de producción incluyendo información real (no pruebas), el servidor donde se ejecuta es el mismo donde se venían desarrollando las pruebas iniciales, sin que se haya trasladado a un servidor de producción oficializado como tal.

También relacionado con este Sistema, se encontró que la responsabilidad inicial fue dada oficialmente al señor Larry Alvarado, funcionario que ya no labora para la institución, por lo que se trasladó de forma tácitamente a la señora Martha Camacho y normalmente es atendido por el señor Alexis Solano a nivel de usuario final.

Así mismo, se encontró que para gestionar, administrar y dar mantenimiento a ciertas necesidades del Sistema de Expedientes, se creó el usuario local LASERFICHE con características lógicas de Administrador, con el pueden ingresar a los servidores donde está la aplicación (SV-01, SV-20 y SV-26), y por medio del SQLSERVER realizar operaciones de mantenimiento total a las bases datos (select, insert, update y delete), esto sin que pueda ser controlado por el Administrador de Base de Datos del Banco ni por el área de Soporte Técnico.

Adicionalmente, se localizó que este usuario administrador de LASERFICHE, es utilizado por distintas personas, entre ellas por los funcionarios internos Alexis Solano de la Dirección FOSUVI, Manuel Lepiz del área de Sistemas, así como también por personal de la empresa externa Aplicom; lo que imposibilita saber qué persona ejecutó determinada acción en la base de datos, diluyendo cualquier tipo de responsabilidad administrativa o civil.

Ilustración 1 - Usuario Local Laserfiche como Administrator en SV-01/20/26



El proceso DSS01.03 denominado "*Supervisar la infraestructura de TI*", del COBIT 5, detalla el siguiente control:

> *"Supervisar la infraestructura de TI y los eventos relacionados con ella. Almacenar la suficiente información cronológica en los registros de operaciones para permitir la reconstrucción, revisión y examen de las secuencias de tiempo de las operaciones y las actividades relacionadas con el soporte a esas operaciones"*

En el artículo 4.4 denominado "*Exigencia de confiabilidad y oportunidad de la información*", del Manual de Control Interno de la Contraloría N-2-2009-CO-DFOE, se detalla:

> *"El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente que se recopile, procese, mantenga y custodie información de calidad sobre el funcionamiento del SCI y sobre el desempeño institucional, así como que esa información se comunique con la prontitud requerida a las instancias internas y externas respectivas..."*

También el artículo 14.2.2 "*Procedimientos de control de cambios del sistema*", de la sección 14.2 sobre seguridad en los procesos de desarrollo y soporte, del ISO 27002:2016, detalla:

> *"Los cambios en los sistemas dentro del ciclo de vida de desarrollo deberían ser contralados mediante el uso de procedimientos formales de control de cambios…*
>
> *Para garantizar la integridad del sistema, aplicaciones y productos, deberían documentarse y hacerse cumplir los procedimientos formales de control de*

cambios, desde las etapas tempranas de diseño a través de todas las tareas de mantenimiento posteriores. La introducción de nuevos sistemas y cambios importantes a sistemas existentes debería seguir un proceso formal de documentación, especificación, pruebas, control de calidad, y gestión de implementación.

Este proceso debería incluir una evaluación de riesgo, el análisis de los impactos de los cambios, y la especificación de los controles de seguridad necesarios. Este proceso también debería asegurar que los procedimientos existentes de seguridad y control no sean comprometidos, que a los programadores de apoyo se les da el acceso sólo a aquellas partes del sistema necesario para su trabajo y que se tenga un acuerdo formal y aprobación para cualquier cambio."

Según lo evaluado, en general las debilidades indicadas sobre el Sistema de Expediente Digital, se deben a que tanto la Dirección FOSUVI, las Entidades Autorizadas, la empresa Aplicom y el Departamento de TI; han venido trabajando en la definición e implementación de requerimientos y solución de problemas, esto sobre la marcha de ejecución del Sistema, sin que se haya definido un tiempo oficial para liberarlo, dejando los mantenimientos necesarios para una siguiente etapa.

Como parte de los efectos directos de que el Sistema de Expedientes Digital esté ejecutándose en un servidor que no es de producción, es que esto habilita la posibilidad de que se realicen cambios directos en bases de datos sin que se seguían los protocoles de seguridad lógica definidos para un adecuado mantenimiento de sistemas; esto es que exista un servidor de pruebas o desarrollo separado lógicamente de un servidor de producción y donde este último sea administrado exclusivamente por el área de Soporte Técnico, pudiendo implementar cambios o modificaciones a base de datos o a la aplicación según la normativa vigente.

Dentro de las consecuencias de utilizar el usuario LASERFICHE con las características lógicas vigentes, es que con su uso se puede acceder, insertar, modificar o eliminar cualquier información del Sistema de Expedientes Digitales sin que exista restricción alguna. Además, por ser varias las personas que lo utilizan, no habría forma de identificar quién ejecutó la acción determinado registro o campo.

2.3 Herramientas externas de conexión a las bases de datos

Al evaluar los controles utilizados por los usuarios para ingresar a cada uno de los sistemas de información institucionales, en la revisión se encontró que la gran mayoría de unidades o áreas del Banco se conectan utilizando el servidor de aplicaciones WebLogic, de esta forma se aplica toda la seguridad lógica que previamente se ha definido a nivel de roles y perfiles para cada usuario validado en los sistemas. Sin embargo, se localizó que ciertos departamentos, por ejemplo Contabilidad, FOSUVI, FONAVI, Comunicaciones, entre otros, hacen uso de conexiones ODBC (Open DataBase Connectivity), el cual es un estándar de acceso a las bases de datos y que a nivel institucional se utiliza para cargar o extraer cierta información, con el inconveniente de que la herramienta también habilita la opción de acceder, modificar o borrar datos de los sistemas si se utilizan los comandos adecuados.

Relacionado con este tema, se encontró que cuando un usuario ingresa a la base de datos lo hace con los permisos otorgados de forma individual o por medio de los roles asignados. Cuando la conexión se hace utilizando el Weblogic, la herramienta misma es la que habilita o deshabilita todos los permisos lógicos que tenga dicho usuario, pudiendo ejecutar en las bases de datos solo lo que previamente fue definido por el dueño del sistema (según su rol). El riesgo se presenta cuando la conexión a la base de datos se da con herramientas de terceros como un ODBC, ya que el usuario haciendo uso de los comandos apropiados, puede intentar activar determinados roles y así encender permisos adicionales con los que podría hacer Select, Insert, Update o Delete sobre los diferentes objetos a los que tengan acceso.

En el proceso DSS06.05 relacionado a gestionar los controles de proceso de negocio, del COBIT 5, se especifica la siguiente práctica de gestión:

> *"**DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades y de información.***
> *Asegurar que la información de negocio puede ser rastreada hasta los responsables y eventos de negocio que la originan. Esto permite trazabilidad de la información a lo largo de su ciclo de vida y procesos relacionados. Proporciona garantía de que la información que conduce el negocio es de confianza y ha sido procesada acorde a los objetivos definidos."*

El artículo 4.3 sobre la administración de datos, del Manual de Normas técnicas para la gestión y el control de las Tecnologías de Información de la Contraloría General de la República, detalla en el capítulo de prestación de servicios y mantenimiento lo siguiente:

> *"**4.3 Administración de los datos***
> *La organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura."*

Una de las principales causas por las que se utilizan conexiones a las bases de datos por medio distintos a los oficiales tales como el ODBC, se debe a que por años se acostumbró en el Banco desarrollar aplicaciones "caseras" utilizando el Microsoft Access, con las que los usuarios finales podían acceder a su información y extraerla para fines operativos propios de cada área, ya que el sistema de información no les solventaba tales necesidades. Con esto y a través de los años cada Departamento o Unidad se adaptó a su uso y hasta la fecha no han efectuado las gestiones correspondientes al área de Sistemas para el desarrollo oportuno en cada aplicación.

Además, una de las razones por las que no se lleva actualmente un control más detallado y estricto sobre todas las conexiones utilizadas con ODBC, es porque la plaza del Departamento de TI del oficial de seguridad se encuentra sin ser asignada, debiendo ser este puesto el encargado de tal gestión.

Uno de los riesgos latentes que presenta la situación indicada, es que se puedan modificar o eliminar datos de los sistemas de información de forma incorrecta y que no pueda ser detectado por los dueños de los sistemas o por los controles automatizados existentes.

2.4 Mantenimiento de Sistemas de Información

Al evaluar el proceso de seguridad y mantenimiento de los sistemas de información institucionales, nos encontramos que desde años atrás se implementó por el Departamento de TI el Sistema de Control de Actualizaciones desarrollado en Microsoft Access, con la finalidad de registrar las formas, reportes y librerías que por mantenimiento deben ser modificadas y que se encuentran en los directorios de los servidores de producción, para lo cual solo el personal de Soporte Técnico tiene los privilegios lógicos de ingresar y cambiar los archivos enviados por el área de Sistemas.

Sobre este particular, según lo indicado por el coordinador del área de Sistemas, la herramienta desarrollada sirve para registrar y llevar un historial de todos los cambios a las formas, reportes y librerías que sean requeridas, no así para las modificaciones a los Scripts de base de datos, para los cuales no se cuenta con un repositorio que agrupe todos los cambios solicitados, sino que los cambios se

registran por medio de correo electrónico enviado por el analista respectivo hacia el Administrador de Base de Datos (DBA), siendo necesario buscar en toda la lista de correos para ubicar los Scripts solicitados en caso de ser requerido.

Para las formas, reportes y librerías que se copian a los servidores de producción, se utilizan los usuarios denominados Mercurio y Administrator, y para las modificaciones de los Scripts se ejecutan con el usuario System, además este último también es utilizado para desbloquear usuarios de bases de datos o establecer nuevas contraseñas. La debilidad de control sobre este tema es que estos tres usuarios que tiene permisos lógicos totales, son compartidos por el personal del área de Soporte Técnico, imposibilitando determinar quién fue el que realizó cada cambio; aunado a que se limita la trazabilidad desde que se origina la necesidad de la modificación hasta que se instala en producción. Para evitar este problema y debido a una recomendación de la Auditoría Interna, se habían creado los usuarios SOPORTE_INF, SOPORTE_RED y SOPORTE_SEG, para que fueran utilizados por un funcionario respectivo de Soporte Técnico, sin embargo a la fecha de la revisión se encontró que no se están utilizando.

Ilustración 2 - Ejemplo movimientos con System efectuados por diferentes funcionarios

USER_OS	USER_HOST	USER_IP	USER_DB	DATE_TIME
andmoya	PC-25-5347-01	192.168.200.86	SYSTEM	01/06/2020 10:57:23
andmoya	PC-25-5347-01	192.168.200.86	SYSTEM	01/14/2020 15:41:17
andmoya	PC-25-5347-01	192.168.200.86	SYSTEM	01/20/2020 14:22:24
margonzalez	DOMINIO\PC-25-5744-01	192.168.213.11	SYSTEM	11/05/2019 16:10:51
margonzalez	DOMINIO\PC-25-5744-01	192.168.213.11	SYSTEM	11/05/2019 16:10:51
margonzalez	DOMINIO\PC-25-5744-01	192.168.213.11	SYSTEM	11/05/2019 16:10:51
marpavon	DOMINIO\PC-25-5352-01	192.168.200.84	SYSTEM	09/25/2018 14:46:01
maumora	PC-25-5351-01	192.168.200.95	SYSTEM	01/09/2020 13:02:26
maumora	PC-25-5351-01	192.168.200.95	SYSTEM	01/14/2020 15:37:20
maumora	PC-25-5351-01	192.168.200.95	SYSTEM	01/20/2020 10:31:37
josvega	DOMINIO\PC-25-5349-01	192.168.200.102	SYSTEM	01/21/2020 12:30:39
josvega	DOMINIO\PC-25-5349-01	192.168.200.102	SYSTEM	01/21/2020 14:53:02
josvega	DOMINIO\PC-25-5349-01	192.168.200.102	SYSTEM	01/21/2020 14:53:08

El BAI05.05 que trata sobre facilitar la operación y el uso, del COBIT 5, cuenta con el siguiente enunciado:

> *"Planificar e implementar todos los aspectos técnicos, operativos y de modo de uso de forma que todos aquellos involucrados en el entorno futuro puedan ejercer sus responsabilidades."*

También el proceso BAI06.01, "*Evaluar, priorizar y autorizar peticiones de cambio*", del COBIT 5, indica:

> *"Evaluar todas las peticiones de cambio para determinar su impacto en los procesos de negocio y los servicios TI, y analizar si el cambio afectará negativamente el entorno operativo e introducirá un riesgo inaceptable. Asegurar que los cambios son registrados, priorizados, categorizados, analizados, autorizados, planificados y programados."*

Por último, en la práctica de gestión DSS06.03 del COBIT 5, relacionada con gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización; se encuentra el siguiente criterio:

> *"Gestionar los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Autorizar el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia del negocio, de TI y de terceras partes. Esto asegura que el negocio sabe dónde están los datos y quien los está manejando en su nombre."*

Se considera que las debilidades sobre el control en las actualizaciones de formas, reportes, librerías y Scripts de base de datos, se presentan en su mayoría porque la herramienta utilizada (Sistema de Control de Actualizaciones) por haber sido desarrollada en Microsoft Access, no se logra adaptar técnicamente a todas las necesidades operativas del proceso de mantenimiento de sistemas.

Una de las consecuencias de no poder identificar cuál funcionario realizó determinado cambio a nivel de los servidores de producción, es que no se puedan establecer las debidas responsabilidades ante un posible registro inadecuado o un proceso doloso.

3. CONCLUSIÓN

En la auditoría sobre los controles implementados para asegurar la consistencia, integridad y disponibilidad de la información almacenada en los servidores de datos del Banco; se concluye que en el transcurso de los últimos años el Departamento de TI ha venido mejorando los procesos que aseguran y mejoran la seguridad lógica del proceso.

Sin embargo, se localizaron ciertas debilidades que tienden a debilitar las medidas de control implementadas a nivel de la seguridad de los datos almacenados en los servidores de producción, como por ejemplo la inexistencia de pistas de auditoría en varios sistemas de información, ejecución de una de las últimas aplicaciones del Banco en servidores de pruebas, existencias de un usuario con permisos administrativos lógicos que no es bien administrado, uso de softwares especiales para acceder a bases de datos de producción, así como debilidades de control concernientes con el mantenimiento de sistemas de información.

El trabajo se realizó aplicando las técnicas de auditoria vigentes, evaluando la normativa referente a la información almacenada en los servidores de datos del Banco, así como los principales controles implementados sobre este tema.

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 Pistas de Auditoría en Sistemas de Información

Al Departamento de TI

4.1.1 Se deben efectuar las gestiones correspondientes para trasladar todas las pistas de auditoría previamente definidas en todos los sistemas de información del Banco y que no pudieron ser implementadas en la nueva versión de Oracle 12c, esto con la finalidad de poder evaluar borrados, modificaciones o inserciones realizadas de forma sospechosa o inusual. Para controlar el avance de esta recomendación, debe crearse un inventario del total de pistas que corrían en la versión anterior, con el detalle suficiente para que la Auditoría Interna pueda darle un seguimiento a su implementación en la nueva versión.
Nivel de Riesgo: **Alto**

4.1.2 Una vez implementadas la totalidad de pistas de auditoría, debe capacitarse a los dueños de sistemas en cómo extraerlas, revisarlas y valorar posibles tablas y campos que podrían ir adicionándose a dichas pistas. Para esto podría valorarse el uso de la nueva herramienta de seguridad denominada Security.
Nivel de Riego: **Medio**

4.2 Sistema de Expedientes Digitales

Al Departamento de TI

4.2.1 Se debe trasladar el Sistema de Expedientes Digitales a un Servidor de Datos de Producción, el cual sea administrado por el área de Soporte Técnico y se adapte a las políticas, procedimientos y demás normativa relacionada con el desarrollo y mantenimiento de sistemas.
Nivel de Riesgo: **Alto**

4.2.2 Es necesario revocar los permisos de Administrador local del usuario LASERFICHE en los servidores SV-01, SV-20 y SV-26; evitando que tenga un control total sobre las bases de datos del Sistema de Expedientes Digitales. Para esto deben crearse los roles necesarios y con los privilegios correspondientes para cada tarea pueda ser ejecutada en el Sistema sin comprometer la integridad y seguridad de la información.
Nivel de Riesgo: **Alto**

4.2.3 Debe eliminarse la posibilidad de que varias personas o departamentos utilicen un mismo usuario, en este caso el LASERFICHE que además es un administrador local. Esto porque debe ser viable identificar concretamente quién ejecutó determinada acción en el sistema o en la base de datos.
Nivel de Riesgo: **Alto**

A la Gerencia General

4.2.4 Se debe definir oficialmente al dueño del Sistema de Expedientes Digitales, el cual vendría a sustituir al señor Larry Alvarado y debería contar con todas las responsabilidades y potestades ya definidas a nivel institucional para los funcionarios que en los demás sistemas de información del Banco tienen este tipo de asignaciones.
Nivel de Riesgo: **Medio**

4.3 Herramientas externas de conexión a la base de datos

Al Departamento de TI

4.3.1 Se deben efectuar las gestiones correspondientes para eliminar a nivel institucional la utilización de conexiones a los sistemas de información por medio de ODBC (Open DataBase Connectivity), o cualquier otra herramienta que no utilice el servidor de aplicaciones WebLogic para ingresar a las aplicaciones. Para esto debe inventariarse la totalidad de este tipo de accesos y así identificar entre otros temas cuáles departamentos o unidades los utilizan, los motivos de su uso, la actividad lógica que realizan a los datos (ingreso, extracción, modificación), la posible incorporación al sistema de información que corresponda y en caso de que no sea factible técnicamente, detallar las razones y así poder controlar sus accesos de forma individual.
Nivel de Riego: **Medio**

4.3.2 Se deben efectuar los ajustes técnicos necesarios para que los roles de los usuarios de base de datos estén siempre inactivos por defecto y que sea únicamente por medio de la herramienta institucionalmente definida (Weblogic en este caso) que se puedan encender o activar. Si fuera obligatorio a nivel operativo de cada unidad que los usuarios deban conectarse a las bases de datos con herramientas de terceros (ODBC), los roles igual deberían estar inactivos y para encenderlos el sistema debería solicitar la clave de acceso respectiva; esto con la finalidad de mantener una trazabilidad adecuada de la información y controlar los accesos lógicos cuando se ejecuten por estos medios.
Nivel de Riego: **Medio**

A la Gerencia General

4.3.3 Deben continuarse las gestiones administrativas para la contratación del oficial de seguridad de la información, el cual dentro de sus funciones debe tener la responsabilidad de controlar y dar seguimiento a cualquier tipo de conexión a las bases de datos institucionales que no sean por los medios oficiales definidos por el Departamento de TI.
Nivel de Riego: **Medio**

4.4 Mantenimiento de Sistemas de Información

Al Departamento de TI

4.4.1 Debe valorarse la posibilidad de adquirir una nueva herramienta que venga a sustituir el Sistema de Control de Actualizaciones, el cual pueda servir como un repositorio total para todas las modificaciones de formas, reportes, librerías y Scripts que se realicen, además de brindar una mejor trazabilidad a todo el proceso de mantenimiento de sistemas de información.
Nivel de Riesgo: **Medio**

4.4.2 Evaluar la factibilidad técnica de incluir un control automatizado que registre y avise cada vez que se modifica una formar, reporte o librería en los servidores de producción; preferiblemente donde se pueda visualizar al menos la fecha y hora del movimiento, la estación de trabajo y su IP desde donde se originó, el servidor de datos afectado, el usuario utilizado y el nombre del archivo que cambió.
Nivel de Riesgo: **Medio**

4.4.3 Es necesario reactivar el uso de los usuarios SOPORTE_INF, SOPORTE_RED y SOPORTE_SEG para dar mantenimiento a las formas, reportes y librerías que deban ser actualizadas en los servidores de producción, quedando así la evidencia de cuál funcionario fue el que realizó determinada acción y dejando los usuarios de Mercurio y Administrador para otras funciones propias de los equipos, siempre y cuando se pueda determinar cuál funcionario ejecutó la actividad.
Nivel de Riesgo: **Alto**

4.4.4 Se recomienda implementar un usuario de base de datos exclusivo para desbloquear usuarios de bases de datos y establecer nuevas contraseñas. De esta forma el usuario System se utilizaría para la actualización de los Scripts y operaciones propias que ameriten ser ejecutadas con este rol.
Nivel de Riesgo: **Medio**

Estudio realizado por:

JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)

Firmado digitalmente por JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)
Fecha: 2020.06.19 15:37:12 -06'00'

MATI. Jorge Ramirez Bolaños
Auditor Encargado

MAURICIO GONZALEZ ZUMBADO (FIRMA)

Firmado digitalmente por MAURICIO GONZALEZ ZUMBADO (FIRMA)
Fecha: 2020.06.19 16:05:44 -06'00'

Aprobado Lic. Mauricio González Zumbado
Auditor Interno a.i.