BANCO HIPOTECARIO DE LA VIVIENDA
AUDITORÍA INTERNA

Informe Final TI-OP-002-2022

AUDITORÍA SOBRE EL CONTROL DE LA INFORMACIÓN CONTENIDA EN LAS COMPUTADORAS PORTÁTILES

13-11-2023

RESUMEN EJECUTIVO

La revisión estuvo enfocada en evaluar los controles implementados para la administración de la información almacenada en las computadoras portátiles designadas a los usuarios del Banco.

Como parte de las actividades de control que pueden mejorarse, se destaca la necesidad de actualizar los procesos actuales de respaldos de información generados en la nube por medio del OneDrive.

Otro de los puntos de control localizados es el relacionado con las computadoras portátiles que no son gestionadas por el área de Soporte Técnico al ser equipos personales de ciertos funcionarios internos.

Así mismo, referente al proceso de parches y actualizaciones de seguridad, se localizó carencia de normativa y documentación de respaldo de actividades ejecutadas por el área de Soporte Técnico.

Por último, debe mejorarse la actividad relacionada con el proceso de inducción que se le da a los nuevos funcionarios en materia de recursos humanos, normativo y de seguridad de TI.

Los detalles de cada aspecto indicado en los párrafos anteriores son ampliados en la sección de Resultados de este informe, incluyendo además la sección de recomendaciones orientadas a mejorar las debilidades de control interno detectadas.

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 RESPALDO DE INFORMACIÓN DEL ONEDRIVE 6
2.2 EQUIPO FUERA DE SOPORTE TÉCNICO 7
Imagen 1- Usuarios con Equipo Propio 8
2.3 PARCHES Y ACTUALIZACIONES DE SEGURIDAD 10
2.4 CAPACITACIÓN A LOS NUEVOS FUNCIONARIOS 11
Imagen 2- Usuarios con capacitaciones faltantes 12

3. CONCLUSIÓN 14

4. RECOMENDACIONES 15

4.1 RESPALDOS DE INFORMACIÓN DEL ONEDRIVE 16
4.2 EQUIPOS FUERA DE SOPORTE TÉCNICO 16
4.3 PARCHES Y ACTUALIZACIONES DE SEGURIDAD 16
4.4 CAPACITACIÓN A LOS NUEVOS FUNCIONARIOS 17

1. INTRODUCCIÓN

1.1 Justificación de la auditoría

Este estudio forma parte del Plan Anual de Trabajo establecido por la Auditoría Interna para el año 2022.

1.2 Objetivo

Evaluar la suficiencia de los controles implementados para la administración de la información almacenada en las computadoras portátiles designadas a los usuarios del Banco.

1.3 Alcance

El estudio abarcó la documentación vigente con corte al 31 de diciembre del 2022, incluyendo la normativa interna disponible en la Intranet institucional.

De acuerdo con las normas de auditoría vigentes se remitió el informe borrador según oficios BANHVI-AI-OF-131-2023 y BANHVI-AI-OF-132-2023, con los cuales se solicitaron las reuniones de cierre con las áreas correspondientes. Sobre este particular, se realizó la reunión de cierre con el Departamento de Tecnologías de Información el día 19 de octubre del 2023, donde después de evacuar algunas dudas, se aceptó el contenido del informe y de sus recomendaciones. Referente a los hallazgos relacionados con la Dirección Administrativa, se vieron con la señora Margoth Campos por medio de la herramienta Microsoft Teams, el 27 de octubre del año en curso, aclarando de igual forma algunos aspectos, quedando el documento final sin cambios con relación al informe borrador.

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
- ✓ ISO 27002:2005 Tecnologías de Información – Código de buenas prácticas para la gestión de la seguridad de la información
- ✓ COBIT 5
- ✓ Normativa Interna vigente (Metodología, Manuales, Políticas, Procedimientos, Instructivos y formularios)
- ✓ Norma 308 Comunicación de resultados.

Así mismo, se aplicaron técnicas de auditoría comúnmente aceptadas como revisión documental de la normativa interna relacionada con la evaluación, así como información solicitada a los usuarios involucrados con el sistema.

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 Respaldo de información del OneDrive

Desde agosto del año 2019 se definió como insumo tecnológico de trabajo en el Banco la suite del Microsoft 365, la cual es una plataforma de productividad con tecnología en la nube con la que se puede crear**,** acceder y compartir documentos online entre distintos usuarios en Word, Excel, PowerPoint y OneNote, entre otros. Para ello, solo se necesita tener acceso a Internet y disponer de la plataforma de OneDrive. Este último es el servicio en la nube que conecta a todos los archivos, permitiendo almacenarlos, protegerlos, compartirlos con otros usuarios y acceder a ellos desde cualquier lugar utilizando los dispositivos tecnológicos previamente establecidos.

Como parte de la revisión se valoró la utilización del OneDrive como insumo para guardar información de los usuarios y por ende de cada área, esto sin eliminar la viabilidad de también guardar información en las distintas carpetas de trabajo creadas para las unidades en la red institucional. Al respecto se logró determinar que el servicio de respaldos con el que cuenta el Banco para todos los archivos que se resguarden en el OneDrive ligado a la de cada usuario, solamente tiene una vigencia de 30 días, después de los cuales se perdería cualquier información histórica que sobrepase ese lapso. Sobre este particular el área de Soporte Técnico ya ha indicado su preocupación, así como posibles soluciones y según lo indicado, se encontraban en el proceso de contratación, pero al momento de la auditoría aún se mantenía esa debilidad de control.

En la guía de implementación del punto 12.3.1 "*Respaldo de la información*", del estándar INTE/ISO/IEC 27002:2016, se detalla lo siguiente:

> *"Debería establecerse una política de respaldos para definir los requisitos de la organización para los respaldos de la información, software y sistemas.*
> *La política de respaldo debería definir los requisitos de retención y protección.*
> *Deberían proporcionarse recursos adecuados de respaldo para garantizar que toda la información y software esenciales <u>se pueden recuperar después de un desastre o falla de medios</u>….*
> *Los planes de respaldo para los sistemas y servicios individuales deberían verificarse regularmente para asegurarse de que cumplen los requisitos de los planes de continuidad del negocio. Para los sistemas y servicios críticos, <u>los planes de respaldo deberían cubrir toda la información, aplicaciones, y datos de los sistemas necesarios para recuperar el sistema completo en caso de un desastre</u>.*
> *Debería <u>determinarse el periodo de retención para la información esencial</u> de la organización, y también cualquier requisito para las copias de archivo a conservarse permanentemente."* El subrayado es propio.

También sobre el tema de respaldos, encontramos en el proceso DSS04.07 de los Objetivos de Gobierno y Gestión del COBIT 2019, lo siguiente:

> *"**DSS04.07 Administrar los acuerdos de respaldo.***
> *Mantener la disponibilidad de la información crítica para el negocio.*
> *1. Hacer una copia de seguridad de los sistemas, aplicaciones, datos y documentación conforme a un calendario definido. Considerar una frecuencia (mensual, semanal, diario, etc.), modo de copia de seguridad (p. ej., disk mirroring para copias de seguridad en tiempo real frente a DVD-ROM para retención a largo plazo), tipo de copia de seguridad (p.ej., completa vs. incremental), y tipo de medios. Considerar también copias de seguridad online automatizadas, tipos de datos (p. ej. voz, ópticos), creación de logs, datos críticos de computación de usuario final (p. ej., hojas de cálculo), ubicación física y lógica de las fuentes de datos, derechos de acceso y seguridad, y encriptación…*
>
> > *2. Definir requisitos para el almacenamiento en las instalaciones (on-site) y fuera de ellas (off-site) de copias de seguridad de datos, conforme a los requisitos de negocio. Considerar el acceso requerido para hacer copias de seguridad de los datos…*
> > *4. Garantizar que se haga una copia de seguridad o se aseguren de forma adecuada los sistemas, aplicaciones, datos y documentación mantenida o procesada por terceros. Considerar que se requiera que los terceros devuelvan las copias de seguridad. Considerar la opción de mantenimiento en fiducia (escrow, por su término en inglés) o acuerdos de depósitos."*

La razón por la que no se cuentan con respaldos mayores a 30 días del OneDrive utilizado por los usuarios institucionales, es porque la herramienta necesaria para esta actividad no había sido previamente valorada dentro del presupuesto del Departamento de TI.

Dentro de las principales consecuencias de no contar con respaldos históricos de la información contenida en el OneDrive de cada funcionario, es que se pueda ver afectada la operativa del área o unidad, esto al necesitar datos o archivos que por su vigencia ya fueron eliminados de la nube, sin tener la posibilidad de recuperarlos.

2.2 Equipo fuera de soporte técnico

Como parte de las acciones ejecutadas para la realizar el teletrabajo en el Banco, desde hace varios años el Departamento de TI empezó a entregar equipos portátiles a ciertos funcionarios claves. Esto sumado a una implementación de hardware y software especializado para conexiones remotas, brindó la posibilidad técnica de que algunos empleados pudieran trabajar desde sus hogares. La entrega de más computadoras portátiles se incrementó con la pandemia del COVIT-19 a inicios del año 2020, no obstante, muchos funcionarios tuvieron que trabajar con equipos

personales debido a que la demando fue más amplia que las computadoras disponibles en ese momento. Desde entonces el Departamento de TI ha venido trabajando con la adquisición y remplazo de equipos portátiles para tratar de cubrir la totalidad de computadoras faltantes, sin embargo, a la fecha de la auditoría aún existen funcionarios que utilizan computadoras personales para realizar el teletrabajo, limitando la posibilidad de que el área de Soporte le pueda brindar mantenimiento preventivo o correctivo a dichos equipos, incluyendo actualizaciones de parches de funcionalidad o seguridad.

Se muestra a continuación los empleados del Banco que en el momento de este estudio aún se encuentran utilizando computadoras propias para realizar sus funciones cuando deben hacer teletrabajo.

Imagen 1- Usuarios con Equipo Propio

LISTA DE FUNCIONARIOS QUE UTILIZAN EQUIPO PROPIO PARA HACER TELETRABAJO	
DEPARTAMENTO	**FUNCIONARIO**
Asesoría Legal	Salas Sancho Sharon
Dirección Administrativa	Ortiz Román Carolina
Departamento de Análisis y Control	Alvarez Sanchez Luis
Departamento Técnico	Rojas Chacón Arturo
Departamento Técnico	Villalobos Rivera Keberlyn
Departamento Técnico	Oreamuno Pérez Luis Alfredo
Departamento de TI	Zúñiga Barrientos Alejandro
FONAVI	Mena Monge Shirley
FONAVI	Samudio Rodriguez Jansel
FONAVI	Calderón Román Mariela
Junta Directiva	Pérez Ramírez Milena
Dirección Administrativa	Moreno Montes Jorge
Subgerencia de Operaciones	Coto Jimenez Rosemary
Unidad de Comunicaciones	Flores Segura Luis Fernando
Unidad de Comunicaciones	Morales Ramírez Marianela
Unidad de Riesgos	Escalante Flores Jeannette

En los Objetivos de Gobierno y Gestión del COBIT 2019, se indican varios procesos actividades de control relacionadas con este hallazgo, que se detallan a continuación:

> *"**BAI03.10 Mantener las soluciones.***
> *Desarrollar y ejecutar un plan para mantener los componentes de la solución y la infraestructura. Incluir revisiones periódicas frente a las necesidades del negocio y los requisitos operativos.*
>
> *2. Evaluar la importancia de una actividad de mantenimiento propuesta sobre el diseño, funcionalidad y/o procesos de negocio de la solución actual. Considerar el riesgo, el impacto en el usuario y la disponibilidad*

de recursos. Asegurar que los dueños del proceso de negocio entiendan el efecto de los cambios designados como mantenimiento.

BAI09.02 Gestionar activos críticos.
Identificar los activos que son críticos para garantizar la capacidad de prestación del servicio. Maximizar su confiabilidad y disponibilidad para apoyar las necesidades de negocio...

5. Mantener la resiliencia de los activos críticos aplicando un mantenimiento preventivo regular. Monitorizar el rendimiento y, de ser necesario, proporcionar activos alternativos y/o adicionales para minimizar la probabilidad de fallo.

6. Establecer un plan de mantenimiento preventivo para todo el hardware considerando un análisis de coste beneficio, las recomendaciones de los proveedores, el riesgo de suspensión del servicio, el personal calificado y otros factores relevantes…

***DSS03.01 Identificar y clasificar los problemas**.*
Definir e implementar criterios y procedimientos para identificar e informar sobre los problemas. Incluir la clasificación, categorización y priorización del problema…

3. Definir grupos de soporte adecuados para ayudar en la identificación de problemas, análisis de la causa raíz y determinación de soluciones para respaldar la gestión de problemas. Determinar grupos de soporte conforme a las categorías predefinidas, como hardware, red, software, aplicaciones y software de soporte." El subrayado es nuestro.

Según se logró determinar en el estudio, el motivo por el que aún existan funcionarios realizando teletrabajo con equipos personales, se debe a que el porcentaje de rotación de cambios de equipos establecido por el Departamento de TI, nunca previó el impacto que podría tener la pandemia del COVIT-19 sobre la operativa institucional, situación que se replicó mundialmente en la gran mayoría de las empresas y que en su momento estuvo fuera del alcance operativo y económico del Banco; de ahí que se haya venido subsanando de forma paulatina.

Esta situación a nivel de ciber seguridad es un punto álgido con respecto a la seguridad de la información institucional, ya que, al usar equipos personales para realizar teletrabajo, no es posible que los funcionarios de Soporte Técnico realicen las actualizaciones o parches de seguridad que surjan tanto en los sistemas operativos como en los antivirus (en caso de que tales computadoras cuenten con alguno); habilitando las vulnerabilidades latentes en el momento y permitiendo por defecto posibles ataques o amenazas directas a los insumos informáticos (hardware o software) del Banco, incluyendo toda la información de los Sistemas actuales.

2.3 Parches y actualizaciones de seguridad

Según lo detallado por el área de Soporte Técnico del Departamento de TI, en el Banco existe un software denominado System Center de Microsoft, el cual es una suite de aplicaciones que sirve para administrar recursos locales y en la nube, y que permite al personal de Soporte gestionar todos los equipos conectados a la red institucional. Como parte de las posibilidades que posee ese software, cuenta con la opción de poder determinar si existen computadoras conectadas a la red o por medio del VPN que no cuenten con las actualizaciones o parches que son instalados automáticamente por parte de Soporte Técnico, esto para solventar cualquier problema de operatividad o seguridad que surgen periódicamente en los sistemas operativos o antivirus de las computadoras. Sobre este particular no se encontró ningún procedimiento o normativa enfocada a controlar y administrar este tipo de actividades, así como tampoco se localizaron reportes que demostraran las tareas ejecutadas sobre este tema.

El punto 12.6.1 que trata sobre la gestión de vulnerabilidades técnicas, del estándar INTE/ISO/IEC 27002:2016, detalla lo siguiente:

> *"Control*
>
> *Se debería obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información usados,* ***se debería evaluar la exposición de la organización a estas vulnerabilidades y tomar las medidas apropiadas para abordar el riesgo asociado****…*
>
> *a) la organización debería definir y establecer los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas, incluyendo el seguimiento de la vulnerabilidad, la evaluación de riesgo de la vulnerabilidad,* ***la aplicación de parches****, el seguimiento de activos, y cualquier responsabilidad de coordinación requerida…*
>
> *d) una vez que ha sido identificada una potencial vulnerabilidad técnica, la organización debería identificar los riesgos asociados y las acciones a ser tomadas;* ***tal acción podría implicar la aplicación de parches a sistemas vulnerables o la aplicación de otros controles****…*
>
> *g)* ***los parches deberían probarse y evaluarse antes de ser instalados*** *para asegurarse de que sean efectivos y no causen efectos secundarios que no pueden ser tolerados;* ***si no está disponible ningún parche, deberían considerarse otros controles****…"* El destacado es propio.

En el proceso DSS05.01 relacionado con el control que debe existir contra el software malicioso, de los Objetivos de Gobierno y Gestión del COBIT 2019, indica sobre este particular:

"***DSS05.01 Proteger contra software malicioso***
Implementar y mantener en toda la empresa medidas preventivas, detectivas y correctivas (especialmente parches de seguridad y control de virus actualizados) para proteger los sistemas de información y la tecnología del software malicioso (p. ej., ransomware, malware, virus, gusanos, spyware y spam).
3. Comunicar acerca de concienciación sobre software malicioso y hacer cumplir los procedimientos y responsabilidades de prevención. Impartir formación periódica sobre malware en el uso de correo electrónico e Internet. Formar a los usuarios para que no abran e informen sobre correos electrónicos sospechosos y no instalen software compartido o no aprobado."

Según lo indicado, la actividad de controlar y administrar el uso de la herramienta System Center de Microsoft, incluyendo el inventario de parches o actualizaciones en todas las computadoras institucionales, no se encuentra normada debido a que su implementación y aplicación es relativamente reciente, estando en el proceso de documentación inicial.

Los parches de seguridad se lanzan para corregir vulnerabilidades conocidas en el software. No aplicar parches de seguridad aumenta significativamente el riesgo de ser víctima de ataques cibernéticos y de sufrir pérdida de datos, acceso a información sensibles o daños en la reputación del Banco, de ahí la importancia de tener normado el proceso de actualizaciones de seguridad, actividad fundamental para mantener la seguridad de las computadoras y la integridad de la información.

2.4 Capacitación a los nuevos funcionarios

Como parte de la valoración de la información o los datos que se resguardan y administran en las computadoras de los funcionarios internos, se realizó investigación sobre las capacitaciones que se les brinda a los nuevos empleados como parte de la inducción a su puesto de trabajo. Para esto se realizó un muestreo sobre las contrataciones realizadas en el año 2022 y 2023, en el cual se puedo corroborar que a algunos de los nuevos funcionarios sí se les brindó capacitación en materia de Recursos Humanos, Seguridad de TI y Cumplimiento Normativo. Sin embargo, como parte de los resultados también se localizaron empleados a los que no se les ofreció capacitación en los tópicos antes detallados, con el agravante de que a ninguno de los funcionarios se le brindó capacitación sobre las herramientas y sistemas informáticos que tenían que utilizar.

En la siguiente tabla se muestra el detalle de lo indicado:

Imagen 2- Usuarios con capacitaciones faltantes

Funcionario	Fecha Ingreso	RECIBIÓ CAPACITACIÓN EN:			
		Recursos Humanos	Seguridad de TI	Cumplimiento Normativo	Herramientas o Sistemas Informáticos
ANGULO RAMIREZ CINDY ROCIO	27/2/2023	**NO**	**NO**	**NO**	**NO**
GUERRERO ACUÑA MONTSERRAT	16/1/2023	**NO**	**NO**	**NO**	**NO**
SALAS SANCHO SHARON	2/1/2023	SÍ	**NO**	SÍ	**NO**
BOLAÑOS SANDOVAL GUILLERMO	12/12/2022	SÍ	**NO**	SÍ	**NO**
MUÑOZ CARAVACA WALTER	28/11/2022	SÍ	**NO**	SÍ	**NO**
ZUÑIGA MESEN KEISY STEPHANIE	24/10/2022	**NO**	**NO**	**NO**	**NO**
BUSTOS CHACON CATHERINE PRISCILA	16/5/2022	SÍ	SÍ	**NO**	**NO**
ORTIZ ROMAN CAROLINA	3/1/2022	SÍ	SÍ	**NO**	**NO**

Al respecto de las capacitaciones ofrecidas, se localizó que tampoco existe un acta firmada donde los nuevos funcionarios se comprometen a resguardar la seguridad de la información institucional a la que van a tener acceso según sus funciones.

En el APO07.03 relacionado con mantener las habilidades y competencias del personal, del Marco de Referencia del COBIT 2019, se indica lo siguiente:

> *"**Definir y administrar las habilidades y competencias que necesita el personal**. Verificar periódicamente que el personal cuente con las competencias necesarias para realizar sus funciones conforme a su educación, capacitación y/o experiencia. Verificar que estas competencias se mantengan con programas de aptitud y certificación cuando sea apropiado. Dar a los empleados oportunidades de aprendizaje continuas para mantener sus conocimientos, habilidades y competencias al nivel requerido para alcanzar las metas empresariales…*
>
> > *2.Identificar las brechas entre las habilidades requeridas y las disponibles. **Desarrollar planes de acción, como capacitación** (habilidades técnicas y de conducta), **contratación**, reasignación y cambio de las estrategias de abastecimiento, para resolver las brechas desde el punto de vista individual y colectivo.*
> > *3.Revisar los materiales y programas de capacitación de forma regular. **Garantizar su idoneidad con respecto a los requisitos en constante evolución de la empresa** y su impacto sobre el conocimiento, capacidades y habilidades necesarias…*
> > *5.Desarrollar y ofrecer programas de capacitación conforme a los requisitos del proceso y organizativos, **incluidos los requisitos para el conocimiento empresarial, control interno, conducta ética, seguridad y privacidad**."* El destacado es nuestro

Una posible causa de que no se estén capacitando a los nuevos funcionarios en los temas antes indicados, es porque la normativa existente no abarca la totalidad de rubros que actualmente se están enseñando. Relacionado con la seguridad de TI, se localizó como motivo de que no se capacitaran a los funcionarios indicados, la

falta de personal que remplace al funcionario encargado de dar esa capacitación, así como la falta de seguimiento de las actividades ejecutadas.

La capacitación adecuada de los nuevos empleados en el uso de las computadoras y sistemas de información es esencial para garantizar la eficiencia operativa, la seguridad de la información y la colaboración efectiva en el lugar de trabajo. Ignorar o limitar las inducciones iniciales pueden llevar a una serie de problemas que afectan tanto a los empleados en el desarrollo de sus funciones, como al Banco en su operativa diaria o hasta en la seguridad de los datos generados por los Sistemas de Información que son utilizados.

3. CONCLUSIÓN

En la revisión sobre la información contenida en las computadoras portátiles, la Auditoría Interna pudo determinar la existencia de controles generales implementados por el Departamento de TI tanto para su operativa como para su gestión.

No obstante, se localizaron algunos aspectos que pueden ser mejorados en actividades relacionadas con respaldos de información, administración de equipos portátiles, procesos de parches y actualización de seguridad, y por último temas referentes a la capacitación que se brinda a los nuevos empleados que ingresan al 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 Respaldos de información del OneDrive

A Andrés Moya Brizuela, jefe del Departamento de TI
Se deben efectuar las gestiones administrativas necesarias para adquirir e implementar una herramienta definida para efectuar los respaldos de la información contenida en el OneDrive de todos los usuarios del Banco. Como parte de este proceso es necesario definir previamente por cuánto tiempo debe ser resguarda la información y qué tipo de seguridad se debe establecer sobre ella. Una vez que se cuente con el software respectivo, debe implementarse la normativa interna necesaria para su administración y control.

Nivel de Riesgo: **Alto**

4.2 Equipos fuera de soporte técnico

A Andrés Moya Brizuela, jefe del Departamento de TI
Se deben realizar las gestiones necesarias para facilitar de computadoras portátiles a todos los funcionarios internos que están realizando teletrabajo con equipos propios, teniendo así la posibilidad de que el área correspondiente del Departamento de TI les brinde todo el soporte necesario. Para solventar este requerimiento, debe valorarse la viabilidad técnica y económica de adquirir la totalidad de los 16 equipos faltantes detallados en este informe, minimizando de forma considerable la posibilidad de ataques a los activos informáticos actuales, riesgo que en caso de materializarse podría generar afectaciones considerables a nivel económico, operativo y reputacional para la institución.

Nivel de Riesgo: **Alto**

4.3 Parches y actualizaciones de seguridad

A Andrés Moya Brizuela, jefe del Departamento de TI
Es necesario que se elabore la normativa necesaria relacionada con la administración y control de los parches o actualizaciones de seguridad que se realizan de forma automática en los equipos institucionales, incluyendo como parte de sus valoraciones, llevar un control más estricto sobre los posibles equipos que por alguna razón no se les logró implementar el parche. Como parte de esta actividad, se debe normar también la documentación de respaldo que servirá como evidencia de la labor ejecutada.

Nivel de Riesgo: **Alto**

4.4 Capacitación a los nuevos funcionarios

A Margoth Campos Barrantes, Directora Administrativa

4.4.1 Se debe actualizar toda la normativa institucional relacionada con el entrenamiento de inducción que se le brinda actualmente a los funcionarios que empiezan a laborar en la institución, incluyendo como parte de las actividades de mayor relevancia, la referente a la capacitación sobre las herramientas informáticas y sistemas de información o aplicativos que van a ser utilizadas por los nuevos usuarios, incluyendo los mecanismos de protección de la información.

Nivel de Riesgo: **Medio**

4.4.2 Como parte de la documentación que los nuevos funcionarios deben firmar a nivel de aceptación, un acta firmada donde se comprometen a resguardar la seguridad de la información institucional a la que van a tener acceso según sus funciones.

Nivel de Riesgo: **Medio**

A Andrés Moya Brizuela, jefe del Departamento de TI

4.4.3 Se debe establecer un control de seguimiento sobre las capacitaciones que se brindan en materia de seguridad de TI a los funcionarios que ingresan a laborar en la institución, con el fin de que por los diferentes motivos que puedan presentarse, este tipo de inducciones no se dejen sin realizar debido a su importancia en materia de seguridad de la información. En este sentido, también debería implementarse un rol de sucesión en caso de que la capacitación no se pueda brindar por la persona encargada oficialmente de la actividad.

Nivel de Riesgo: **Medio**

Estudio realizado por:

JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)

Firmado digitalmente por JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)
Fecha: 2023.11.13 13:25:36 -06'00'

MATI. Jorge Ramirez Bolaños
Auditor Encargado

Firmado digitalmente por GUSTAVO FLORES OVIEDO (FIRMA)
Fecha: 2023.11.14 12:46:51 -06'00'

Aprobado MBA Gustavo Flores Oviedo
Auditor Interno