BANCO HIPOTECARIO DE LA VIVIENDA
AUDITORÍA INTERNA

Informe Final
TI-SEG-001-2022

AUDITORÍA SOBRE LA ADMINISTRACIÓN DE LAS CUENTAS DE USUARIO EN LA INTRANET

14/02/2023

RESUMEN EJECUTIVO

La revisión estuvo enfocada en evaluar los controles generales existentes para el uso y administración de las cuentas de usuario de red de los funcionarios del Banco.

Como parte de las actividades de control que pueden mejorarse, se encontró una desactualización en la normativa relacionada con la administración de la infraestructura tecnológica.

También se encontró la falta de un control automatizado que monitoree y avise sobre los cambios en los permisos lógicos de las carpetas de red.

Así mismo referente al proceso normativo, no se cuenta con políticas enfocadas a valorar periódicamente los permisos de accesos definidos en las distintas carpetas de trabajo de la Intranet. De igual forma no se localizó normativa del área de Recursos Humanos referente a los bloqueos de las cuentas de usuario cuando deben ejecutarse de forma temporal.

Por último, se ubicó una limitación de control donde se liguen las mesas de servicio contra las desactivaciones de los usuarios que ha sido solicitadas.

Los detalles de cada aspecto indicado en los párrafos anteriores son ampliados en la sección de Resultados de este informe, donde de igual forma, se incluyen las recomendaciones tendientes a corregir 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 5

2.1 POLÍTICA SOBRE INFRAESTRUCTURA TECNOLÓGICA 5
2.2 CAMBIO DE PERMISOS LÓGICOS EN LAS CARPETAS DE RED 6
2.3 VERIFICACIÓN DE PERMISOS DE USUARIO EN LAS CARPETAS DE RED 7
2.4 BLOQUEO DE USUARIOS DE FORMA TEMPORAL 8
Imagen 1- Usuario Ricardo Chavarría Activo 9
Imagen 2- Usuario Manuel Lépiz Activo 9
Imagen 3- Proceso Deshabilitación de usuario 10
2.5 CONTROL SOBRE LOS FUNCIONARIOS DESACTIVADOS 11
Imagen 4- Detalle Usuarios Desactivos 12

3. CONCLUSIÓN 13

4. RECOMENDACIONES 14

4.1 POLÍTICA SOBRE INFRAESTRUCTURA TECNOLÓGICA 15
4.2 CAMBIO DE PERMISOS LÓGICOS EN LAS CARPETAS DE RED 15
4.3 VERIFICACIÓN DE PERMISOS DE USUARIO EN LAS CARPETAS DE RED 15
4.4 BLOQUEO DE USUARIOS DE FORMA TEMPORAL 15
4.5 CONTROL SOBRE LOS FUNCIONARIOS DESACTIVADOS 16

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 las cuentas de los funcionarios del Banco que utilizan los insumos tecnológicos de la intranet.

1.3 Alcance

El estudio abarcó la documentación vigente con corte al 30 de noviembre del 2022, incluyendo la normativa interna disponible 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
- ✓ 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 Política sobre infraestructura tecnológica

En la descripción de la política PO-INST-TI-004 denominada "*Ambiente de trabajo de infraestructura tecnológica*" y la cual tiene como propósito establecer un ambiente de trabajo controlado para brindar soporte a la infraestructura tecnológica del banco, se indica que el detalle de los permisos respectivos se ubica en el documento "*Roles para usuarios especiales*", el cual debería ubicarse en la ruta: "*G:\Inf_Inst_unidad\Dpto. Tecnología de Informacion\Controles\Área Soporte\Documentos\Roles*". Sobre este detalle, se localizó que la ruta de red no existe y que el documento indicado no se utiliza desde setiembre del año 2015.

El artículo 4.6 referente al cumplimiento del ordenamiento jurídico y técnico Normas de control interno N-2-2009-CO-DFOR, 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."*

Las Normas de Control Interno para el Sector Público de la Contraloría General de la República N-2-2009-CO-DFOE, detallan el en artículo 1.4 inciso c), lo siguiente:

> "***1.4 Responsabilidad del jerarca y los titulares subordinados sobre el SCI***
> *c. La emisión de instrucciones a fin de que las políticas, normas y procedimientos para el cumplimiento del SCI, estén debidamente documentados, oficializados y actualizados, y sean divulgados y puestos a disposición para su consulta."*

Así mismo, en el artículo 15 de la Ley de Control Interno 8292, se detalla el siguiente enunciado:

> *"Artículo 15.—**Actividades de control**. Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*

> *a) Documentar, mantener actualizados y divulgar internamente,* ***las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional*** *y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones."* El destacado es nuestro.

Según los resultados obtenidos, la desactualización de la política en mención, así como el desuso del documento donde se detallan los roles de acceso para el personal de soporte técnico, se debe a una falta de seguimiento sobre el uso de dichos controles por parte del supervisor del área.

Una posible consecuencia de no mantener un control sobre los accesos lógicos para el personal de soporte técnico, es que se puedan establecer permisos sobre equipos o grupos de seguridad mayores a los que se deberían tener, debilitando así la seguridad sobre la información contenida en las diferentes ubicaciones.

2.2 Cambio de permisos lógicos en las carpetas de red

Los permisos de acceso lógico de los funcionarios del Banco a las distintas unidades de red del Banco son otorgados y administrados por el área de Soporte Técnico del Departamento de TI. Tales permisos son los que cada jefatura como dueña de la carpeta solicita a TI, habilitando para los funcionarios las acciones de leer, copiar, modificar o hasta eliminar, según sea el caso. Al respecto se encontró que no se cuenta con un control que informe automáticamente a los dueños de la información cada vez que se modifiquen los permisos lógicos de los usuarios en las carpetas institucionales.

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"*

El artículo 4.6 referente al cumplimiento del ordenamiento jurídico y técnico Normas de control interno N-2-2009-CO-DFOR, 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."

De acuerdo con lo revisado con el personal de soporte técnico, no se cuenta con el control automático sobre los cambios lógicos en las carpetas de trabajo de la red en primera instancia porque nunca ha sido solicitado por los dueños de la información, y adicionalmente se indicó por el personal de Soporte Técnico que tal acción no se tiene disponible para Windows y no se ha localizado un software de un tercero que tenga dichas características.

Como consecuencia de no poder detectar automáticamente modificaciones realizadas en las carpetas de la red, se podrían efectuar cambios en los datos que ahí se resguarda o acceder a información que sea confidencial o de uso restringido, sin que los dueños de las carpetas puedan conocer la situación en el tiempo correcto para actuar según corresponda.

2.3 Verificación de permisos de usuario en las carpetas de red

Como parte de los controles definidos por el Departamento de TI, se elaboró el procedimiento PA-GTI-GSSTI-PR02 "*Revisión de Derechos de Acceso*", el cual tiene como propósito detallar las acciones para efectuar revisiones semestrales de los permisos lógico con los que cuentan los usuarios sobre los diferentes sistemas de información de la Institución. Sin embargo, en la auditoría se logró determinar que no se cuenta con normativa enfocada a valorar periódicamente los accesos definidos en las distintas carpetas de trabajo de la Intranet del Banco (G:) de las diferentes unidades del Banco, esto con el fin de determinar si tales permisos son correctos según los criterios originales.

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."* El destacado es diferente al original.

También en el dominio de Entrega y Soporte del COBIT 5, en el proceso DS11 el punto 11.7 "*Chequeos de Exactitud, Suficiencia y Autorización*", localizamos lo siguiente:

> *"Los datos de transacciones, ingresados para su procesamiento (generados por personas, por sistemas o entradas de interface) deberán estar sujetos a una variedad de controles para verificar su exactitud, suficiencia y validez. Asimismo, deberán establecerse procedimientos para asegurar que los datos de entrada sean validados y editados tan cerca del punto de origen como sea posible."*

La razón por la que no se controlan los permisos de las carpetas de trabajo de la intranet, se debe a que los dueños de cada unidad lógica no han visto la necesidad de controlar las carpetas y la información que se administra en tales repositorios, esto a pesar de que en muchas de estas unidades lógicas se resguarda información valiosa para los procesos administrativos y operativos de cada área.

En las carpetas de trabajo creadas en la intranet para resguardar información de cada unidad o departamento puede existir información de carácter confidencial o de importancia y al no tenerse un control más estricto sobre su seguridad, se podría acceder, eliminar o modificar información que afecte negativamente la operativa institucional.

2.4 Bloqueo de usuarios de forma temporal

Al valorar la normativa relacionada con el proceso de bloqueos o desactivaciones de los usuarios que ingresan a la red del Banco y sus demás recursos, se logró determinar que el área de Recursos Humanos cuenta con la política "*PA-GRH-TP-PR04 Separación permanente del puesto*", la cual en su punto 14 indica lo siguiente:

"*14. Comunicar la separación permanente del funcionario.*
El Oficial 4 Coordinador de Recursos Humanos comunica la separación permanente del funcionario al Departamento de Tecnologías de Información, Proveeduría, Servicios Generales a efectos de que tomen las medidas de su competencia."

Sobre este aspecto y al evaluar el proceso de administración sobre los usuarios del Banco que dejan su función de forma temporal y no ingresan a los recursos tecnológicos (red, correo, sistemas, etc.) por un lapso específico, ya sea por vacaciones, incapacidad, permisos o cualquier otro motivo, se logró determinar que el área de Recursos Humanos no cuenta con normativa enfocada en este fin, esto a pesar de que el Departamento de TI sí lo tiene normado en el procedimiento "*PA-GTI-CTI-PR01-IN01 Gestión estratégica de TI".*

Como ejemplos de este hallazgo, se muestran seguidamente dos imágenes donde se muestran dos usuarios, Ricardo Chavarría Paniagua y Manuel Lépiz Morales, los cuales al momento de la revisión estaban incapacitados, pero sin embargo se encontraban activos a nivel de la red en el Active Directory. Además, se muestra una tercera imagen donde se detalla de ser necesario, la forma simple de desactivar temporalmente a los usuarios.

Imagen 1- Usuario Ricardo Chavarría Activo

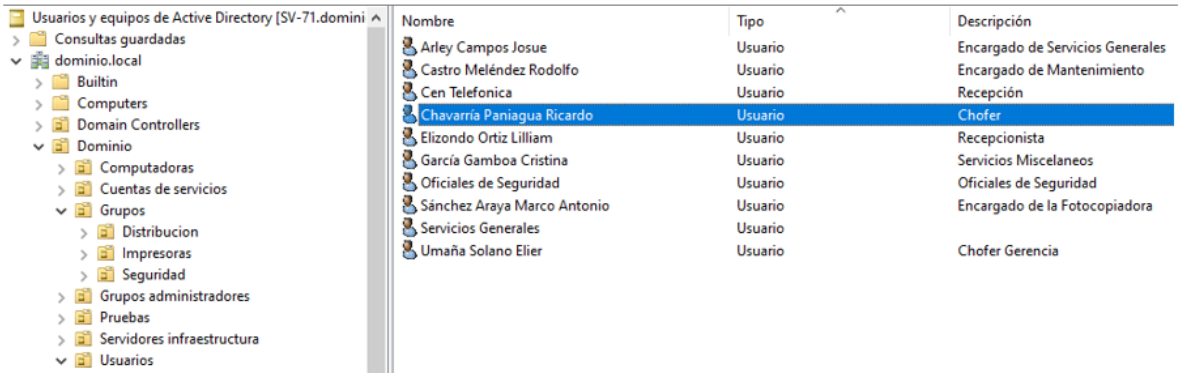


Imagen 2- Usuario Manuel Lépiz Activo

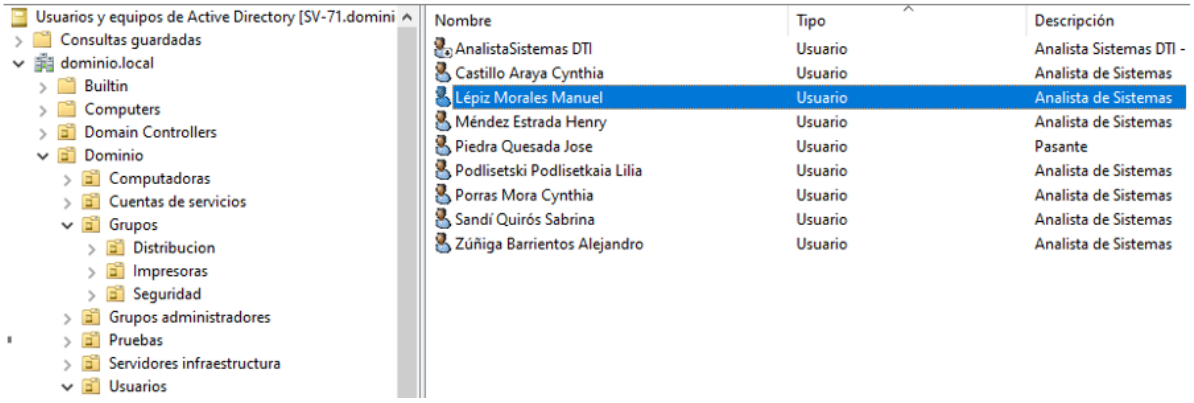
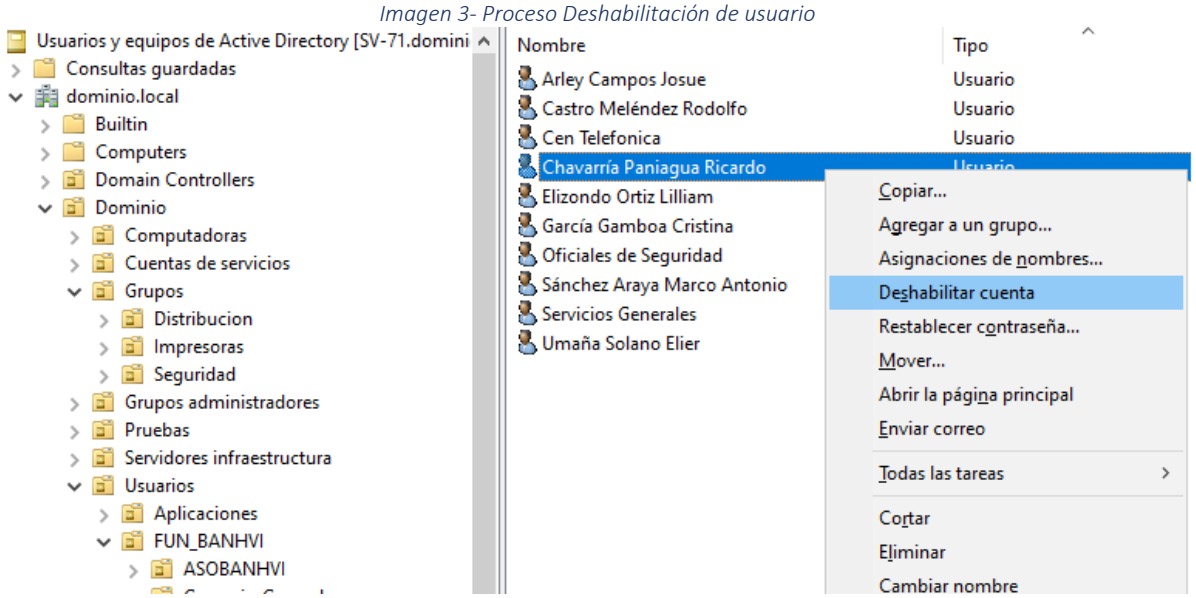


Imagen 3- Proceso Deshabilitación de usuario



En el procedimiento "*PA-GTI-CTI-PR01-IN01 Gestión estratégica de TI*", sobre la apertura, activación, inactivación, eliminación de cuentas de acceso a la red de datos institucional, se detalla:

"Control de acceso a los servicios de red PO-INST-TI-020"

- *A la red institucional pueden ingresar únicamente los usuarios autorizados (internos o externos), quienes deben superar el proceso de autenticación correspondiente para acceder a la red de datos institucional. Por lo tanto, para minimizar los riesgos de ataques a la integridad y validez de la información y equipos de cómputo institucionales,* ***se deben bloquear los accesos de funcionarios que se encuentren en períodos de vacaciones, permisos, incapacidades y de cualquier otra acción que represente el alejamiento temporal*** *de funcionarios de sus responsabilidades para con la Institución, e igualmente, se deben eliminar los accesos a aquellas personas que han finalizado la relación laboral con la Institución.*
- *Cada jefe de área o departamento, es el encargado de definir los permisos de acceso a la información que tiene bajo su responsabilidad y que se encuentra almacenada en la red institucional. Los permisos de acceso deben ser asignados de acuerdo con el rol funcional de cada usuario. El acceso debe ser solicitado al Departamento de TI, utilizando el mecanismo definido para esos efectos."* (El destacado es propio)

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…"

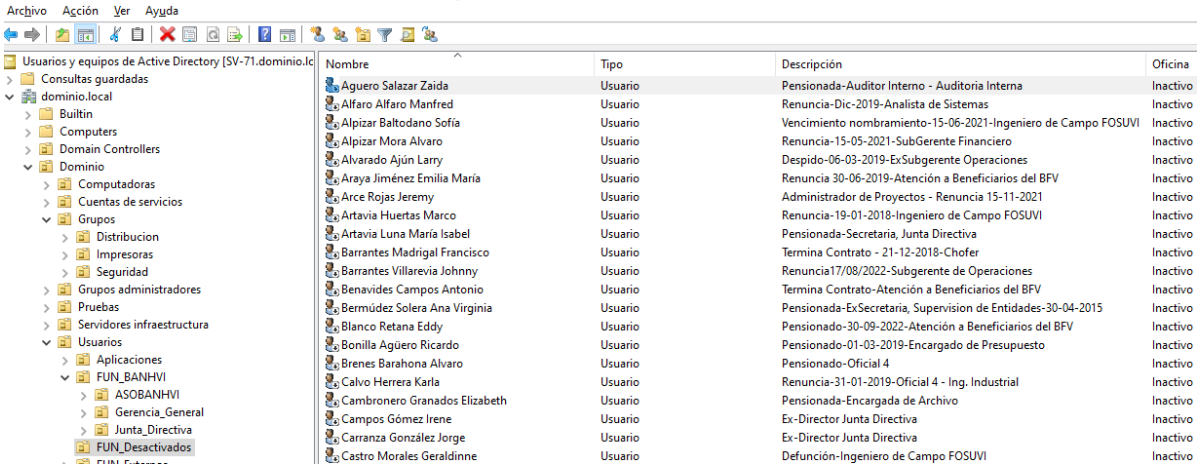
Esta situación se presenta debido a que en los últimos años se han venido actualizando las políticas y procedimientos del Banco, y en alguna de las actualizaciones, se eliminaron de la normativa de Recursos Humanos, el control sobre las suspensiones temporales de acceso a la red para los funcionarios que fueran necesarios.

Al tener usuarios institucionales activos que por distintas circunstancias no estén laborando en el Banco de forma temporal, se habilita la posibilidad de que tales cuentas sean utilizadas por otras personas ya sea para fines operativos lícitos del área o con propósitos incorrectos, siendo en cualquiera de las dos alternativas improcedentes e inconsistente con las normas de control interno establecidas para el uso y administración de los usuarios de red.

2.5 Control sobre los funcionarios desactivados

Como parte de las funciones ejecutadas por el área de Soporte Técnico de TI y siguiendo la normativa relacionada con el uso de la herramienta de la Mesa de Servicio, el área de Recursos Humanos siguiendo la política "*PA-GRH-TP-PR04 Separación permanente del puesto*", realiza las solicitudes para la desactivación de aquellos funcionarios que dejan de laborar en la institución ya sea por despido, renuncia, pensión, deceso o cualquier otro motivo. Una vez que se ejecuta la mesa de servicio, los usuarios se trasladan a un apartado del Active Directory donde se ubican los usuarios desactivados, tal como se muestran en la imagen siguiente. Sobre este proceso, a pesar de que en la descripción se detalla un pequeño comentario sobre el motivo de la inactivación del funcionario, no hay forma de ligar a qué mesa de servicio corresponde la desactivación ni cuál fue el funcionario de TI que realizó el trabajo, esto para darle el seguimiento respectivo o poder determinar movimientos que no se liguen a alguna mesa de servicio.

Imagen 4- Detalle Usuarios Desactivos



Nombre	Tipo	Descripción	Oficina
Aguero Salazar Zaida	Usuario	Pensionada-Auditor Interno - Auditoria Interna	Inactivo
Alfaro Alfaro Manfred	Usuario	Renuncia-Dic-2019-Analista de Sistemas	Inactivo
Alpizar Baltodano Sofía	Usuario	Vencimiento nombramiento-15-06-2021-Ingeniero de Campo FOSUVI	Inactivo
Alpizar Mora Alvaro	Usuario	Renuncia-15-05-2021-SubGerente Financiero	Inactivo
Alvarado Ajún Larry	Usuario	Despido-06-03-2019-ExSubgerente Operaciones	Inactivo
Araya Jiménez Emilia María	Usuario	Renuncia 30-06-2019-Atención a Beneficiarios del BFV	Inactivo
Arce Rojas Jeremy	Usuario	Administrador de Proyectos - Renuncia 15-11-2021	Inactivo
Artavia Huertas Marco	Usuario	Renuncia-19-01-2018-Ingeniero de Campo FOSUVI	Inactivo
Artavia Luna María Isabel	Usuario	Pensionada-Secretaria, Junta Directiva	Inactivo
Barrantes Madrigal Francisco	Usuario	Termina Contrato - 21-12-2018-Chofer	Inactivo
Barrantes Villarevia Johnny	Usuario	Renuncia17/08/2022-Subgerente de Operaciones	Inactivo
Benavides Campos Antonio	Usuario	Termina Contrato-Atención a Beneficiarios del BFV	Inactivo
Bermúdez Solera Ana Virginia	Usuario	Pensionada-ExSecretaria, Supervision de Entidades-30-04-2015	Inactivo
Blanco Retana Eddy	Usuario	Pensionado-30-09-2022-Atención a Beneficiarios del BFV	Inactivo
Bonilla Agüero Ricardo	Usuario	Pensionado-01-03-2019-Encargado de Presupuesto	Inactivo
Brenes Barahona Alvaro	Usuario	Pensionado-Oficial 4	Inactivo
Calvo Herrera Karla	Usuario	Renuncia-31-01-2019-Oficial 4 - Ing. Industrial	Inactivo
Cambronero Granados Elizabeth	Usuario	Pensionada-Encargada de Archivo	Inactivo
Campos Gómez Irene	Usuario	Ex-Director Junta Directiva	Inactivo
Carranza González Jorge	Usuario	Ex-Director Junta Directiva	Inactivo
Castro Morales Geraldinne	Usuario	Defunción-Ingeniero de Campo FOSUVI	Inactivo

El proceso DSS06 del COBIT 5, en la práctica de gestión DSS06.02, se menciona con relación al procesamiento de la información:

> ***"DSS06.02 Controlar el procesamiento de la información***
> *Operar la ejecución de las actividades de proceso de negocio y controles relacionados, basados en el riesgo corporativo, para asegurar que el procesamiento de la información es válido, completo, preciso, oportuno y seguro (es decir, refleja el uso de negocio autorizado y legitimado.)"*

En el proceso DS13 del COBIT 5, Administración de Operaciones, se declara en el punto 13.6 lo siguiente:

> ***"13.6 Bitácora de Operación***
> *Los controles de la Gerencia deberán garantizar que se almacene en bitácoras suficiente información cronológica de las operaciones para permitir la reconstrucción, la revisión y el examen oportunos de las secuencias de tiempo de procesamiento y otras actividades que rodean y soportan el procesamiento."*

Una posible causa de que no se estén ligando este tipo de mesas de servicio con las descripciones de las desactivaciones de las cuentas, es que la normativa interna del Departamento de TI no contemple este proceso como relevante como un mecanismo más de sus controles.

Al no poder ubicar si cada desactivación de usuarios en el Active Directory procede de un requerimiento exclusivo del área de Recursos Humanos, de algún funcionario específico o de alguna jefatura o Dirección (según lo normado), se podrían presentar problemas con el proceso de administración de las cuentas o hasta posible eliminación de usuarios, con las distintas implicaciones que tales acciones podrían generar a nivel operativo y administrativo.

3. CONCLUSIÓN

En la revisión sobre la administración de las cuentas de usuario en la intranet, 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 específicos que pueden ser mejorados con el desarrollo e implementación de controles adicionales tanto a nivel normativo como operativo, siendo necesario que la Administración activa gobierne su recurso humano y tecnológico de forma adecuada para su implementación.

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 Política sobre infraestructura tecnológica

Al Departamento de TI

En vista de la relevancia que genera el control sobre el soporte a la infraestructura tecnológica del Banco, debe actualizarse la política PO-INST-TI-004 "*Ambiente de trabajo de infraestructura tecnológica*", lo cual implica actualizar el documento de los "*Roles para usuarios especiales*", la ubicación en la unidad de red respectiva, así como cualquier otra información contenida en el documento que no se apegue a la actualidad de las tecnologías y procesos de la institución.

Nivel de riesgo: **Alto**

4.2 Cambio de permisos lógicos en las carpetas de red

Al Departamento de TI

Debe efectuarse un estudio de costo beneficio enfocado a la implementación de un software que controle los cambios que se realizan en los permisos lógicos de las diferentes carpetas de trabajo definidas en la Intranet y que informe de forma automática a los dueños de las carpetas y a personal del Departamento de TI previamente definido, cada vez que se presente una modificación en los permisos previamente establecidos.

Nivel de Riegos: **Alto**

4.3 Verificación de permisos de usuario en las carpetas de red

Al Departamento de TI

Se debe elaborar la normativa interna necesaria enfocada a revisar de forma periódica la configuración sobre accesos vigentes en las carpetas de trabajo de la Intranet (G:) de las diferentes unidades del Banco, esto con el objetivo de valorar si los permisos lógicos establecidos son los correctos según los requerimientos originales de cada área o las solicitudes de cambios correspondientes. Como parte de esta nueva normativa, se debe involucrar a los dueños de cada unidad lógica, con la finalidad de que queden documentados los vistos buenos correspondientes una vez se hayan verificado los accesos.

Nivel de Riesgo: **Alto**

4.4 Bloqueo de usuarios de forma temporal

A la Dirección Administrativa

Se debe elaborar la normativa suficiente y necesaria enfocada a controlar las suspensiones de los funcionarios que por distintas razones (vacaciones, incapacidades,

permisos u otros) dejen de laborar temporalmente en la institución. La normativa que se defina debe estar ligada con las políticas y procedimientos que en su defecto ha creado para estos fines el Departamento de Tecnologías de Información. Una vez creada e implementada la política o el procedimiento correspondiente, se debe establecer un control que asegure su cumplimiento, evitando así contar con usuarios activos en el Active Directory que por su condición laboral deberían estar bloqueados.

Nivel de Riesgo: **Alto**

4.5 Control sobre los funcionarios desactivados

Al Departamento de TI

Es necesario implementar un control con el que se liguen las mesas de servicio con las desactivaciones de acceso a la red ya sea de forma temporal o permanente para los funcionarios que así se requieran, pudiendo ubicar no solo el origen del movimiento, sino el funcionario de Soporte Técnico que ejecutó la acción. Para esta actividad también se deben valorar de ser necesario las actualizaciones correspondientes en la normativa del Departamento de Tecnologías de Información, donde se contemple tanto el proceso de ejecución como el de revisiones posteriores por parte de los supervisores correspondientes.

Nivel de Riesgo: **Medio**

Estudio realizado por:

JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)

Firmado digitalmente por JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)
Fecha: 2023.02.14 12:16:00 -06'00'

MATI. Jorge Ramirez Bolaños
Auditor Encargado

MAURICIO GONZALEZ ZUMBADO (FIRMA)

Firmado digitalmente por MAURICIO GONZALEZ ZUMBADO (FIRMA)
Fecha: 2023.02.15 10:43:33 -06'00'

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