BANCO HIPOTECARIO DE LA VIVIENDA
AUDITORÍA INTERNA

Informe Final TI-SI-001-2021

AUDITORÍA SOBRE EL SISTEMA DE EXPEDIENTE DIGITAL

27/01/2022

RESUMEN EJECUTIVO

La revisión estuvo enfocada en evaluar los controles generales existentes para el uso y administración del Sistema de Expediente Digital.

Como parte de las debilidades de control, se localizaron cuentas locales en ciertos servidores de datos utilizados para el Sistema de Expediente Digital que contaban con permisos de administrador local sobre esos equipos.

También se encontró la inexistencia de seguimientos sobre cualquiera de los cambios que se realicen sobre los permisos y privilegios lógicos de los usuarios del Sistema o de los grupos de trabajo creados.

Referente al proceso general de administración del Laserfiche, se logró determinar que el mismo es realizado en su totalidad por un funcionario del área de Sistemas y no por los dueños de este.

Adicionalmente se logró determinar que herramientas propias de control existentes en el aplicativo y relacionadas con auditorías de ciertos procesos y generación de reportes específicos, no está siendo utilizada por los dueños de la aplicación.

Por último, se localizó la carencia de normativa específica sobre el uso de la firma digital y la validez y vigencia de ciertos documentos utilizados en el expediente digital del bono de vivienda.

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

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 2021.

1.2 Objetivo

El objetivo principal de la auditoría es evaluar la suficiencia de los controles implementados por la Administración para la utilización del sistema de Expediente Digital.

1.3 Alcance

El estudio abarcó la documentación vigente con corte al 15 de Diciembre del 2021, suministrada en su mayoría por el Departamento de Tecnologías de Información.

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 s.

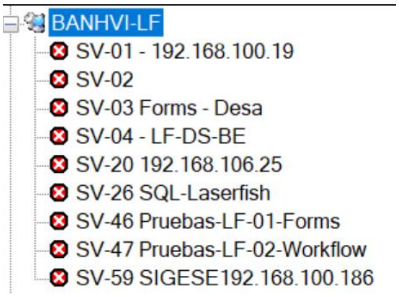
Los resultados de las pruebas ejecutadas y demás documentos que respaldan el trabajo realizado, se mantienen como papeles de trabajo en el expediente electrónico de la Auditoría Interna. Las deficiencias detectadas, tanto en aspectos de control interno como operativas, de la presente revisión, se detallan en la siguiente sección de Resultados de la Evaluación.

2. RESULTADOS DE LA EVALUACIÓN

2.1 Cuentas con permisos de Administrador

Como parte de la revisión, se procedió a valorar las cuentas definidas como administradoras locales en los servidores utilizados por el Sistema de Expediente Digital, mismos que se muestran en la siguiente imagen:

Imagen 1- Lista Servidores Laserfiche



Sobre este particular, se localizó que la cuenta denominada "*Laserfiche*" está definida con permisos de administrador local en los equipos SV-02, SV-03 y SV-20. Así mismo, también a la cuenta de "*soporte-lf*" se le asignaron privilegios de administrador en los servidores SV-0 y SV-03. Se recalca que estas dos cuentas no son utilizadas por el área de Soporte Técnico de TI para sus funciones normales, sino que son utilizas para efectuar procesos relacionados con el Sistema de Expediente Digital.

Seguidamente se muestran las pantallas con las referencias indicadas:

Imagen 2- Usuarios Administrador Servidor SV-02

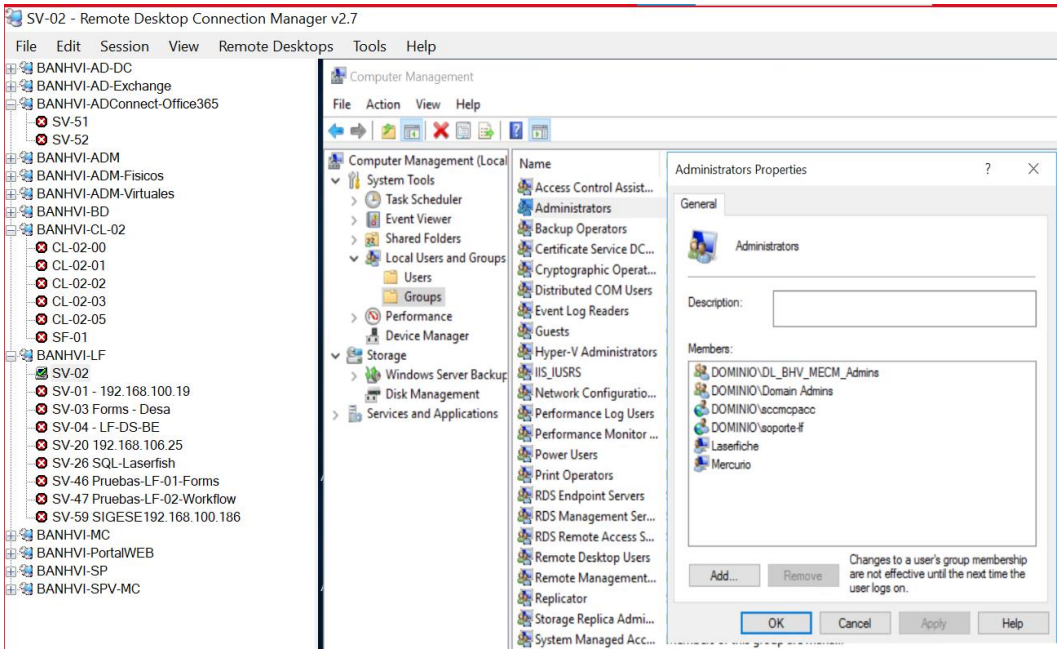


Imagen 3- Usuarios Administrador Servidor SV-03

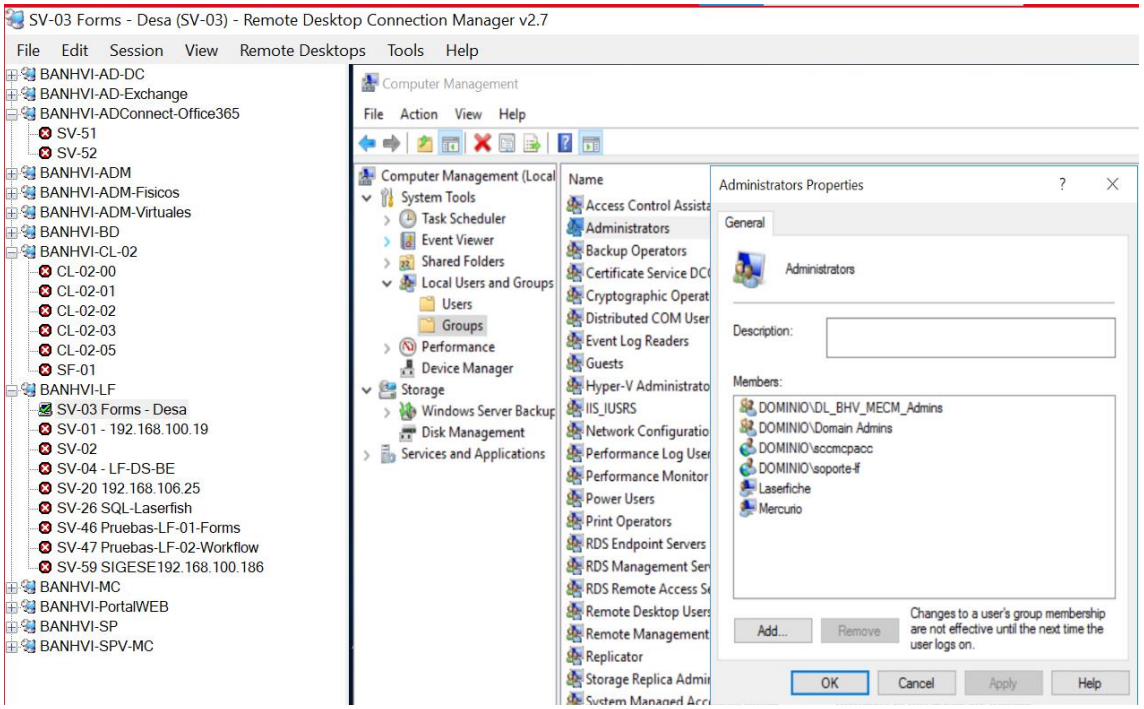
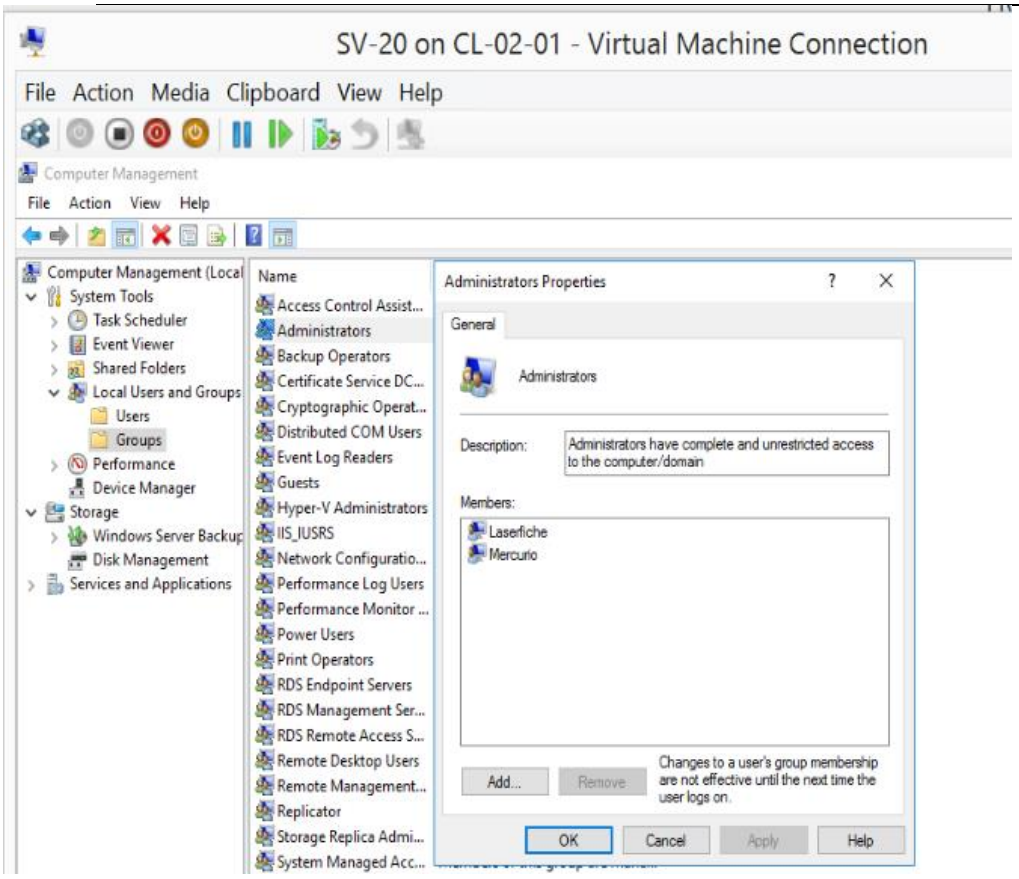


Imagen 4- Usuarios Administrador Servidor SV-20



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."*

Además, en 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 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."

Según el proceso de evaluación, el motivo por el que a las cuentas indicadas se les haya otorgado permisos de administrador en los servidores SV-02, SV-03 y SV-20, se debe a que en su momento fue necesario como parte de la instalación y puesta en producción del Sistema, situación que no debería prevalecer a la fecha de la auditoría.

Uno de los posibles efectos que se pueden presentar por tener usuarios habilitados con permisos de Administración total sobre los servidores, es que se realicen modificaciones en la seguridad o la configuración general del equipo de manera no controlada, y tales cambios pueden comprometer la información contenida en esos equipos.

2.2 Monitoreo de modificaciones en permisos lógicos

Al evaluar varias secciones referentes a la funcionalidad del Sistema de Expediente Digital, se localizó que la herramienta cuenta con un apartado para administrar los permisos lógicos concedidos a cada uno de los usuarios, así como para controlar los privilegios asignados a los grupos de trabajo de los repositorios en los cuales se incluyen los diferentes usuarios, esto para una administración más controlada y expedita. Para la creación inicial de los permisos actuales, se elaboró en su momento una matriz de derechos y privilegios de acceso, que al final fueron incorporados al Sistema.

Al respecto de este tema, se encontró que no se están monitoreando los nuevos permisos o cualquier modificación que se realice sobre los privilegios lógicos existentes tanto de los usuarios del Sistema como de los grupos de trabajo del repositorio, así como tampoco la asignación de usuarios a cualquiera de los grupos de trabajo ya existentes.

En las siguientes imágenes se muestran unas pantallas de ejemplo sobre cómo se administran algunos de los ítems mencionados:

Imagen 5- Seguridad Directory Server

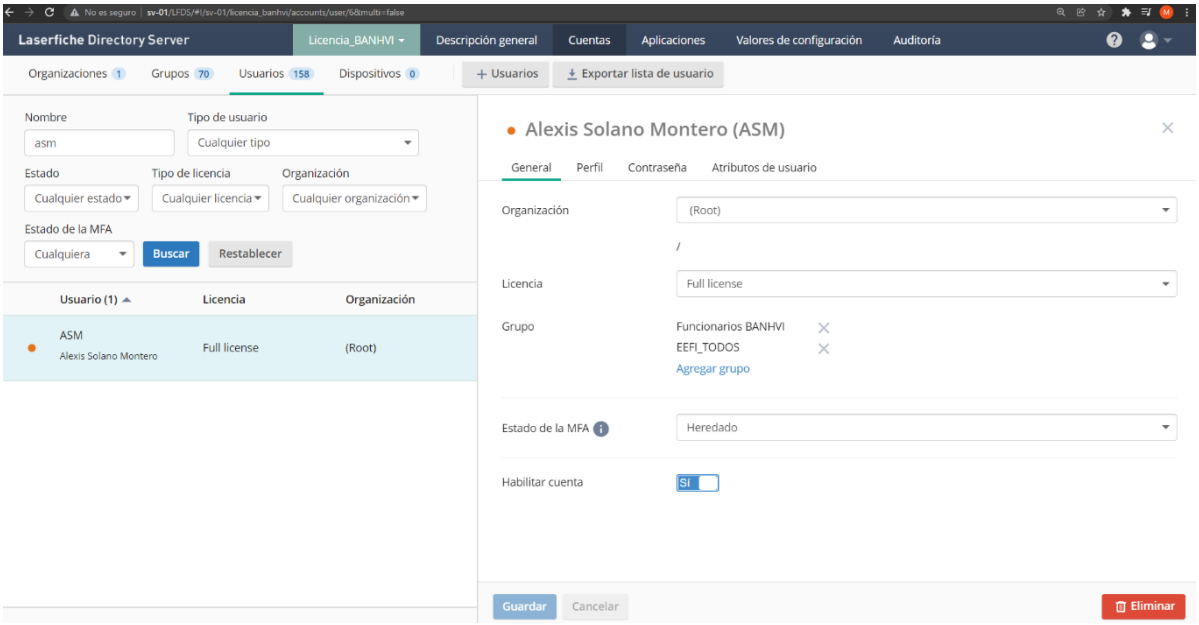


Imagen 6- Seguridad por Forms

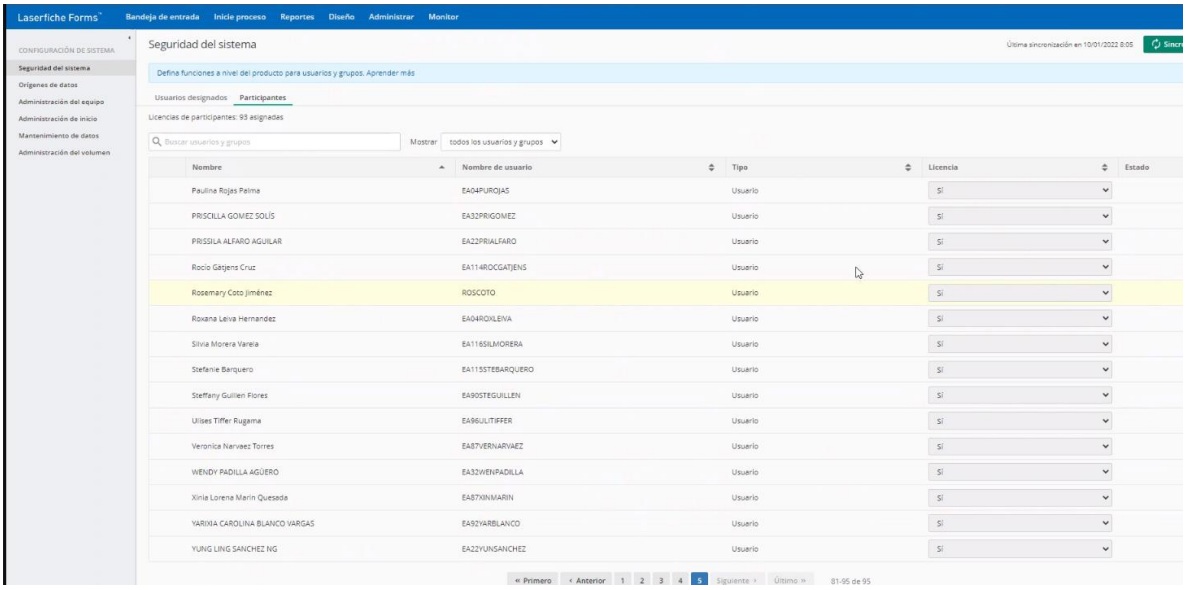
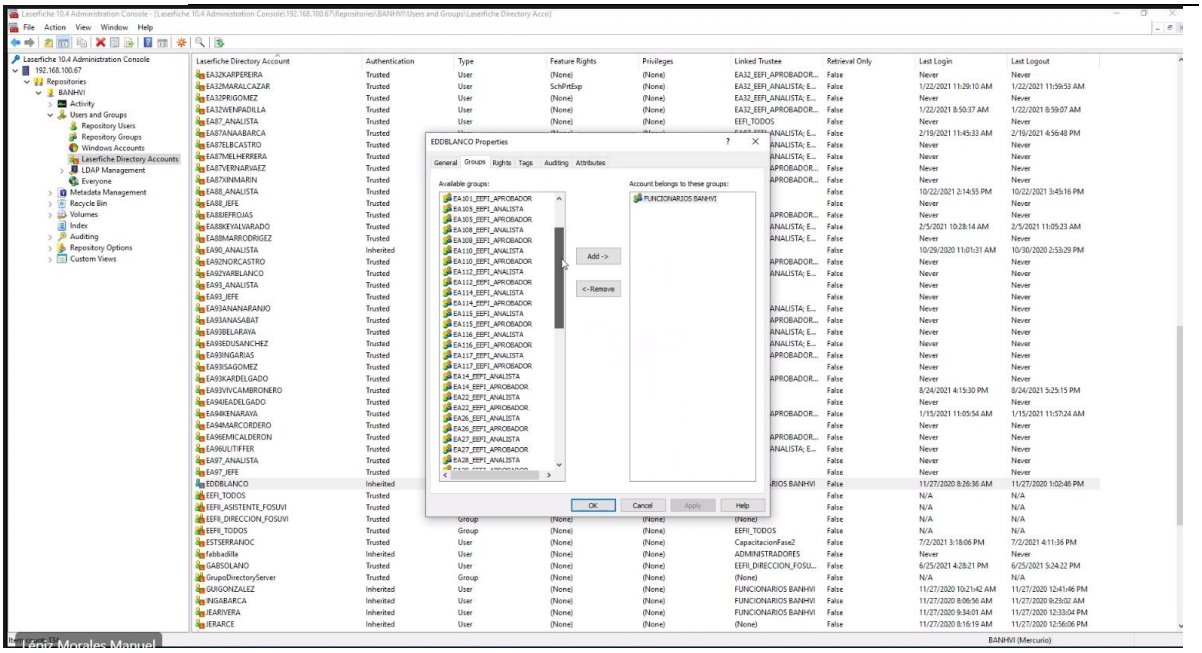


Imagen 7- Seguridad por Consola



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

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

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…"*

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"

Uno de los principales motivos por los que no se están controlando los cambios en los privilegios lógicos ni en los grupos de trabajo del repositorio, se debe a que el Sistema de Expediente Digital fue implementándose paulatinamente en las Entidades Autorizadas y para no atrasar el proceso, no fue valorado en ese momento la necesidad de implementar estos controles.

Al no contar con este tipo de controles se podrían otorgar más permisos lógicos de los correspondientes tanto a usuarios como a grupo de trabajo, que no fueron aprobados previamente por los dueños del Sistema y que pueden traer consigo implicaciones negativas sobre la seguridad de la información.

2.3 Administración del Sistema

En la auditoría se pudo comprobar que el proceso general de administración y control de la plataforma de Laserfiche, donde se incluyen temas como la seguridad del sistema, la creación y administración de usuarios y grupos, la asignación de privilegios lógicos a usuarios y grupos de trabajo, la creación y mantenimiento de los reportes, el monitoreo de las instancias, la administración de licencias disponibles, la elaboración de informes, el control de auditorías, entre otros; es ejecutada en su totalidad por el funcionario Manuel Lépiz Morales, el cual pertenece al área de Sistema del Departamento de TI y no por las áreas correspondientes.

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

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

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

"El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que las funciones incompatibles, se separen y distribuyan entre los diferentes puestos; así también, que las fases de autorización, aprobación, ejecución y registro de una transacción, y la custodia de Inventarios, estén

distribuidas entre las unidades de la institución, de modo tal que una sola persona o unidad no tenga el control por la totalidad de ese conjunto de labores." El subrayado es propio.

En el artículo 2.5.1 referente a la delegación de funciones del Manual de Normas de Control Interno N-2-2009-CO-DFOE de la Contraloría General de la República (CGR), encontramos el siguiente enunciado:

> *"El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que la delegación de funciones se realice de conformidad con el bloque de legalidad, y de que conlleve la exigencia de la responsabilidad correspondiente y la asignación de la autoridad necesaria para que los funcionarios respectivos puedan tomar las decisiones y emprender las acciones pertinentes."*

La razón por la que los procesos del Sistema de Expediente Digital antes detallados no hayan sido tomados por el negocio y se encuentren aún como parte de las actividades del área de Sistemas, esto a pesar de que desde Diciembre del 2020 se haya puesto en producción, se debe a que los dueños de la aplicación no han visto la necesidad operativa de controlar las actividades administrativas inmersas en el aplicativo.

Esta situación puede presentar problemas en la integridad y seguridad de la información que es administrada por el Sistema de Expediente Digital, esto al no ser controlada por los dueños del Sistema.

2.4 Auditoría y Reportes del Sistema

Como parte de la revisión se evaluaron los principales procesos de control inmersos en la herramienta de Laserfiche, encontrando que esta cuenta con insumos para parametrizar ciertos tipos de auditoría y de reporteo. En primera instancia se localiza el "*Audit Trail*" (imagen 8), el cual es una herramienta que se puede utilizar para auditar el repositorio donde se resguardan los documentos escaneados que conforman el expediente digital del bono de vivienda. También existe una opción de auditoría (imagen 9) en el Directory Server con la cual se pueden revisar temas como la asignación de licencias, los inicios de sesión, la creación y administración de usuarios internos y externos, la creación, eliminación o actualización de grupos, entre otros. Por último, existe toda una sección en la cual se pueden parametrizar diversos tipos de reportes (imagen 10), los cuales están relacionados con el proceso de los Formularios utilizados como parte del flujo del expediente digital; con tales reportes se podrían revisar por ejemplo tareas en proceso, procesos terminados, formularios con más de N días, tareas asignadas a las Entidades Autorizadas, tareas en proceso o terminadas en BAHNVI y otros.

Sobre estas opciones del Sistema de Expediente Digital relacionadas con el Audit Trail, la Auditoría del Directory Server y los Reportes de los Formularios, se logró determinar que las mismas no están siendo utilizadas por los dueños o encargados de la aplicación,

dejando sin explotar varios de los insumos de control más relevantes que están disponibles en el aplicativo. Se muestran seguidamente unas pantallas de ejemplo:

Imagen 8- Pantalla Audit Trail

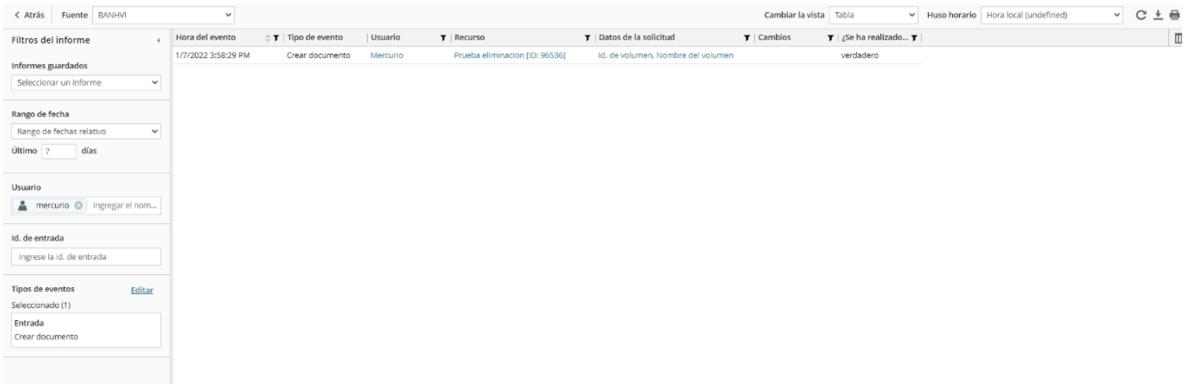


Imagen 9- Pantalla Auditoría Directory Server

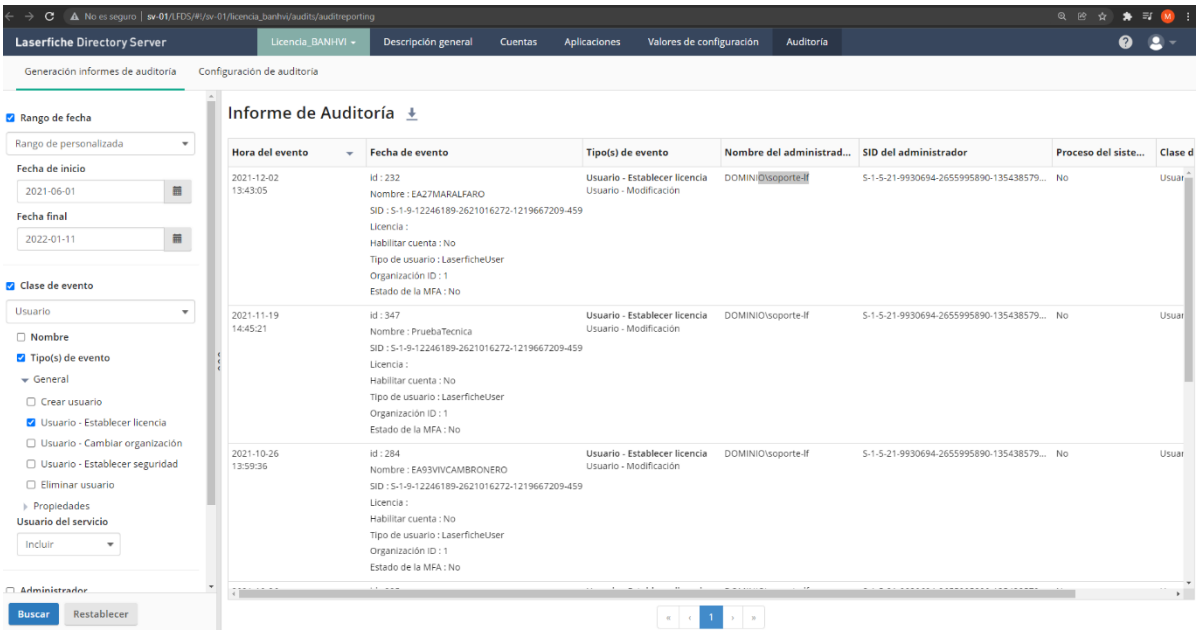
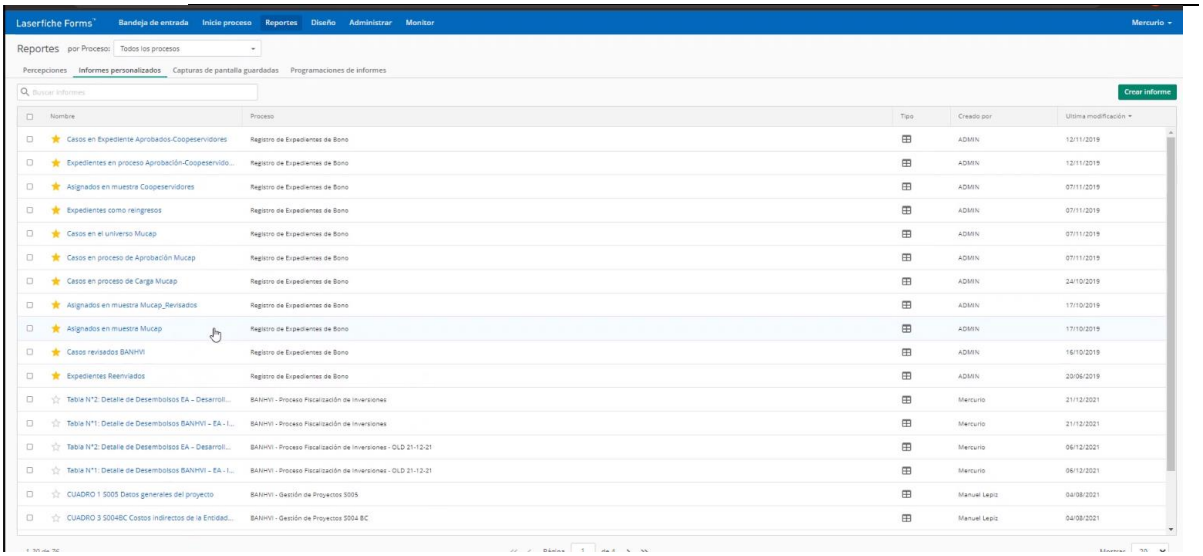


Imagen 10- Pantalla Reportes



En el dominio de Entrega y Soporte del COBIT 5, en el proceso DS11 el punto 11.7 "*Chequeos de Exactitud, Suficiencia y Autorización*", dicta 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."*

En el 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."*

De igual forma el proceso AI3.2 del COBIT 5, detalla los siguientes controles con respecto a este tipo de actividades:

> *"**AI3.2 Protección y disponibilidad del recurso de infraestructura***
> *Implantar medidas de control interno, seguridad y auditabilidad durante la configuración, integración y mantenimiento del hardware y del software de la infraestructura para proteger los recursos y garantizar su disponibilidad e integridad. Se deben definir y comprender claramente las responsabilidades al utilizar componentes de infraestructura sensitivos por todos aquellos que*

desarrollan e integran los componentes de infraestructura. Se debe monitorear y evaluar su uso."

La causa por la que no se haya implementado el uso de las herramientas de auditoría y reportes del Sistema de Expediente Digital, se debe a que desde que se puso en producción la plataforma no fue definido clara y formalmente quiénes debían ser los responsables de administrar tales controles.

Como consecuencia de no tener habilitados los controles de auditoría o reportes detallados en este hallazgo se podrían estar presentado situaciones anómalas, dolosas o fuera de los parámetros previamente establecidos y permitidos, sin que los mismos puedan ser detectados a tiempo por los dueños del Sistema para su debida corrección o para tomar las medidas regulatorias correspondientes.

2.5 Normativa sobre la documentación del Expediente Digital

Referente a la documentación del bono individual de vivienda que las Entidades Autorizadas ingresan virtualmente utilizando el Sistema de Expediente Digital, se encontró que no está normado la forma en que deben administrarse el uso de las firmas digitales, así como la vigencia y validez de ciertos documentos. Como parte de los documentos electrónicos que pueden estar relacionados con este tema se encuentran el avalúo, estudios de otras propiedades, presupuestos, plano de construcción, estudio de trabajo social, informe de bienes e informe literal de propiedades, certificaciones de nacimiento y estado civil, entre otros. Es importante detallar que en la auditoría se localizó un documento borrador enfocado a normar estas situaciones, sin embargo, no estaba oficializado.

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."

De igual forma, 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.

La causa por la que no se encuentren normados los aspectos indicados de la documentación electrónica utilizada en el Sistema de Expediente Digital, se debe a que el uso de dicho Sistema para gestionar los bonos individuales es relativamente nuevo en la institución y se ha dado mayor relevancia a ponerlo en funcionamiento en todas las Entidades Autorizadas que en la parte normativa.

Como posibles efectos que esta carencia de formalidad puede generar es que se apruebe documentación que no cumple con los requisitos legales correspondiente o en su defecto, se presenten atrasos considerables en las diferentes etapas del flujo del bono de vivienda debido a la falta de certeza sobre cómo deben venir determinados documentos.

3. CONCLUSIÓN

En la revisión sobre el Sistema de Expediente Digital, la Auditoría Interna corroboró la implementación de controles generales para su uso y administración.

No obstante, se localizaron algunos aspectos específicos sobre el uso y administración de la herramienta que pueden ser mejorados con el desarrollo e implementación de controles adicionales tanto a nivel normativo como operativo, para lo cual la Administración activa cuenta con los recursos humanos y tecnológicos suficientes y competentes.

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 Cuentas con Permiso de Administrador

Al Departamento de TI

Se deben eliminar los permisos de Administrador Local para las cuentas "*Laserfiche* y *soporte-lf*" que se encuentran en los servidores SV-02, SV-03 y SV-20, según corresponda. En caso de que para el uso del Sistema de Expedientes Digitales se necesiten ciertos accesos con permisos superiores, debe valorarse la creación de un usuario enfocado a suplir los requerimientos técnicos del sistema, pero sin que cuente con todos los permisos disponibles concedidos a una cuenta de Administrador.

Nivel de riesgo: **Alto**

4.2 Monitoreo de modificaciones en permisos lógicos

A la Dirección FOSUVI

4.2.1 Se debe implementar un control de seguimiento sobre cualquier nuevo acceso o modificación que se realice en los privilegios lógicos del Sistema de Expedientes Digitales tanto de forma individual (cada usuario) como para los grupos de trabajo del repositorio del sistema. El control además de guardar un historial sobre los cambios o modificaciones debe enviar un aviso de forma inmediata (vía correo electrónico) tan pronto se ejecute la acción, esto al menos al funcionario que funja como dueño del Sistema, al encargado del área de Soporte Técnico y a la Dirección del FOSUVI.

Nivel de Riegos: **Alto**

4.2.2 Sobre el control de seguimiento en línea de los cambios en los permisos lógicos, se deben normar las acciones que los responsables del Sistema tienen que ejecutar con la finalidad de determinar que los cambios realizados en las cuentas de usuario o en los grupos de trabajo del repositorio hayan sido generados por necesidad o requerimiento de su área.

Nivel de Riegos: **Alto**

4.3 Administración del Sistema

Al Departamento de TI

Se deben efectuar las gestiones necesarias para que se eliminen como parte de las funciones operativas del funcionario Manuel Lépiz Morales, todos los aspectos referentes a la administración y ciertos mantenimientos del Sistema de Expediente Digital y que son propios del Negocio y no del área de Sistemas. Para esto el área de

Sistemas debe valorar en conjunto con los dueños del Sistema (FOSUVI) y el área de Soporte Técnico de TI, todas las actividades ejecutadas por el señor Lépiz que podrían causar conflictos de interés o debilidades en el control interno de administración de la herramienta. Una vez identificados los procesos correspondientes, deben ser cedidos a las áreas que correspondan (Soporte o FOSUVI) y seguidamente eliminar los privilegios de Administrador al señor Lépiz. De ser necesaria su colaboración, debe crearse otro tipo de usuario habilitando los accesos solo a las funciones requeridas.

Nivel de Riesgo: **Alto**

4.4 Auditoría y Reportes del Sistema

A la Dirección FOSUVI

4.4.1 Como parte de las funciones de control del Sistema de Expediente Digital, la Dirección FOSUVI debe asumir la administración y uso de las herramientas del Audit Trail enfocada hacia los repositorios, la opción de auditoría contemplada en el Directory Server y la sección de reportería enfocada hacia los Formularios. Para esta actividad debe solicitar la capacitación que sea necesaria y definir los distintos usuarios que se harían responsables de cada actividad.

Nivel de Riesgo: **Alto**

4.4.2 Debe elaborarse la normativa correspondiente, ya sea a nivel de política, procedimientos, instructivos, etc., donde se establezcan las actividades operativas que la Dirección FOSUVI debe ejecutar una vez que se implemente el uso de las herramientas de control relacionadas con auditoría y reportes del Sistema de Expediente Digital.

Nivel de Riesgo: **Alto**

4.5 Normativa sobre la documentación del Expediente Digital

A la Dirección FOSUVI

Es necesario continuar con el proceso de normar y formalizar todo lo relacionado a la documentación electrónica que es utilizada para la revisión y aprobación de los bonos de vivienda individuales y que ahora son gestionados por medio del Sistema de Expediente Digital, con esto se pueden evitar ambigüedades o problemas legales en las diferentes etapas de los flujos correspondientes.

Nivel de Riesgo: **Alto**

Estudio realizado por:

JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)

Firmado digitalmente por JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)
Fecha: 2022.01.27 15:50:24 -06'00'

MATI. Jorge Ramirez Bolaños
Auditor Encargado

Firmado digitalmente por GUSTAVO FLORES OVIEDO (FIRMA)
Fecha: 2022.01.27 18:30:19 -06'00'

Aprobado MBA Gustavo Flores Oviedo
Auditor Interno