BANCO HIPOTECARIO DE LA VIVIENDA
AUDITORÍA INTERNA

Informe Final
TI-ES-001-2023

AUDITORÍA ESPECIAL SOBRE LA FIRMA DIGITAL A NIVEL INSTITUCIONAL

06/09/2023

RESUMEN EJECUTIVO

La revisión estuvo enfocada en evaluar los controles implementados para el uso y administración de los documentos firmados digitalmente en el Banco.

Como parte de las actividades de control que pueden mejorarse, se localizaron debilidades de procesamiento en el sistema SIGECE que afectan directamente los documentos en PDF que fueron firmados digitalmente.

También se encontró como debilidad de control, la carencia en la definición de estándares para el uso de la firma digital en documentos oficiales del Banco.

Referente a los inconvenientes presentados con el SIGECE, se localizó la necesidad de efectuar una valoración sobre los repositorios actuales de documentos con firma digital que perdieron su integridad.

Por último, se ubicó la necesidad de implementar un control normativo que se enfoque en validar y controlar los archivos con formato PDF y que cuenten con firma digital.

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 6

2.1 CONVERSIÓN DE DOCUMENTOS CON FIRMA DIGITAL 6
2.2 ESTANDARIZACIÓN EN EL USO DE LA FIRMA DIGITAL 8
Imagen 1- Memorando GG-ME-1044-2022 9
Imagen 2- Oficio BANHVI-GG-OF-0176-2023 9
Imagen 3- Oficio BANHVI-DAD-OF-014-2023 10
Imagen 4- Oficio BANHVI-DAD-OF-023-2023 10
2.3 ACTUALIZACIÓN Y CONSERVACIÓN DE DOCUMENTOS FIRMADOS DIGITALMENTE 12
2.4 VALIDEZ Y CONTROLES GENERALES DE LA FIRMA DIGITAL 14
Imagen 3- Ejemplo de validación WEB de firma digital 15

3. CONCLUSIÓN 18

4. RECOMENDACIONES 19

4.1 CONVERSIÓN DE DOCUMENTOS CON FIRMA DIGITAL 20
4.2 ESTANDARIZACIÓN EN EL USO DE LA FIRMA DIGITAL 20
4.3 ACTUALIZACIÓN Y CONSERVACIÓN DE DOCUMENTOS FIRMADOS DIGITALMENTE 20
4.4 VALIDEZ Y CONTROLES GENERALES DE LA FIRMA DIGITAL 21

1. INTRODUCCIÓN

1.1 Justificación de la auditoría

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

1.2 Objetivo

Evaluar los controles implementados para el uso y administración de los documentos firmados digitalmente en el Banco.

1.3 Alcance

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

De acuerdo con las normas de auditoría vigentes se remitió el informe borrador según oficios BANHVI-AI-OF-073-2023 y BANHVI-AI-OF-074-2023, con los cuales se solicitaron las reuniones de cierre con las áreas correspondientes. Sobre este particular, se recibió correo electrónico del Departamento de Tecnologías de Información el día 14 de julio del 2023, donde indican no tener observaciones a los puntos relacionados con su área. Referente a la Dirección Administrativa, no se recibió ninguna respuesta, teniendo también como aceptados los resultados del estudio.

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.
- ✓ Ley de Certificados, Firmas Digitales y Documentos Electrónicos No. 8454 del 30 de agosto de 2005.
- ✓ Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N°33018 del 20 de marzo de 2016.
- ✓ Ley de Protección de la persona frente al tratamiento de sus datos personales No.8968 de 7 de julio de 2011.
- ✓ Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente del 20 de mayo de 2013
- ✓ Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE).
- ✓ Normas Generales de Auditoria para el Sector Publico
- ✓ 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, así como información solicitada directamente a los usuarios involucrados con el proceso.

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

2. RESULTADOS DE LA EVALUACIÓN

2.1 Conversión de documentos con firma digital

En vista de la puesta en vigencia de la directriz N°067-MICITT-H-MEIC publicada en la gaceta N°79 del 25 de abril del 2014, denominada "*Masificación de la implementación y el uso de la firma digital en el Sector Público Costarricense*", el Banco empezó a trabajar en su implementación a nivel institucional, esto según consta en el memorando GG-ME-0994-2015 del 9 de diciembre del 2015. Hoy en día la firma digital es utilizada en todas las unidades de la institución al momento de remitir oficios, memorandos o cualquier documento oficial, como medio de autenticación y validez de dichos documentos. Para este fin, se implementó hace unos meses el uso del sistema denominado SIGECE, el cual se utiliza como un repositorio para cargar y descargar la documentación que es enviada por las distintas unidades o departamento a otras áreas. Al revisar este proceso en la auditoría, se logró determinar que los documentos al momento de descargarse de mencionado sistema pierden sus propiedades como archivos PDF (Portable Document Format), pasando a convertirse todo el documento en una imagen.

En los artículos 6, 8 y 9 de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos No. 8454 del 30 de agosto de 2005, se indica:

> *"Artículo 6º-**Gestión y conservación de documentos electrónicos.** Cuando legalmente se requiera que un documento sea conservado para futura referencia, se podrá optar por hacerlo en soporte electrónico, siempre que se apliquen las medidas de seguridad necesarias para garantizar su inalterabilidad, se posibilite su acceso o consulta posterior y se preserve, además, la información relativa a su origen y otras características básicas.*"
>
> *Artículo 8º-**Alcance del concepto**. Entiéndese por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico.*
> *Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado.*
>
> *Artículo 9º-**Valor equivalente**. Los documentos y las comunicaciones suscritos mediante firma digital tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita. Los documentos públicos electrónicos deberán llevar la firma digital certificada."* (Los subrayados son nuestros)

Así mismo, en la Norma Técnica Nacional NTN-004 de 16 de diciembre de 2001, Lineamientos para la digitalización de documentos textuales con la finalidad de sustituir el soporte original, se indica en sus definiciones lo siguiente:

> *"II.DEFINICIONES:*
>
> ***Firma Digital**: entiéndase por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico. Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado.*
>
> ***Integridad**: Propiedad de un documento electrónico que denota que su contenido y características de identificación han permanecido inalterables desde el momento de su emisión."* (El subrayado es de nuestra autoría)

Adicionalmente y referente al procesamiento de la información, en el proceso DSS06 del COBIT 5, en la práctica de gestión DSS06.02, se menciona:

> *"**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.)"*

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

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

Según el proceso de validación efectuado, así como por lo detallado por el personal técnico encargado del mantenimiento del SIGECE, la causa de que se estuvieran convirtiendo los archivos PDF a imágenes al momento de ser descargados, se debe

a problemas de configuración de la herramienta y que dicho proceso nunca había sido valorado desde que se puso a operar el sistema.

Un efecto directo de contar con esta situación es que tal como lo indica la normativa referida, no sería posible para los funcionarios responsables, la validación de que el documento original no haya sido alterado, así como las ratificaciones necesarias sobre la autenticidad de las firmas digitales estampadas en los documentos, perdiendo por defecto la trazabilidad e integridad de dichos archivos.

2.2 Estandarización en el uso de la firma digital

Como parte de la auditoría, se valoró la estandarización en el uso de la firma digital por las principales áreas del Banco, incluyendo a la Gerencia General, la Subgerencia de Operaciones, Subgerencia Financiera, el FONAVI, el FOSUVI, el Departamento de TI, el Departamento Financiero Contable, la Unidad de Riesgos, la Unidad de Planificación Institucional y la Dirección Administrativa. En este punto se logró determinar que la mayoría de las áreas utilizan la firma digital con toda la información general que brinda tal herramienta, esto sería el nombre de firmante, así como la fecha y hora en que se firmó. Sin embargo, esta situación no es aplicada siempre por la Gerencia General ni por la Dirección Administrativa, ya que en la mayoría de los documentos que se valoraron como parte de la muestra, en sus firmas digitales no se incluyeron ni la fecha ni la hora en que se ejecutó tal acción, siendo necesario tener el archivo original para poder validar las propiedades de la firma; actividad que en el Banco no está estandarizada.

Como ejemplo de las situaciones indicadas anteriormente, se muestran las siguientes imágenes:

1. La primera imagen, el memorado GG-ME-1044-2022 de la Gerencia General, tiene fecha del documento el 22 de agosto de 2022 y la firma digital no incluye la fecha ni hora en que fue firmado, sin embargo, al validar las propiedades de esta, se detalla que fue firmado el 27 de agosto de 2022, esto es cinco días después según la fecha del documento.
2. En la segunda imagen, el oficio BANHVI-GG-OF-0176-2023 del 21 de febrero de 2023 también de la Gerencia General, sí se incluye la fecha y hora en la firma digital, y se logra verificar que sí coinciden tanto la fecha del documento como la fecha de la firma.
3. En la tercera imagen, de la Dirección Administrativa, BANHVI-DAD-OF-014-2023, encontramos que la firma digital no incluye la información de fecha ni hora, y en el proceso de validación, se encuentra una diferencia de 7 días entre la fecha del documento y la fecha en que fue firmado.
4. En la cuarta imagen, el oficio BANHVI-DAD-OF-023-2023 de la Dirección Administrativa, se encuentra como fecha de la firma el 21 de marzo, pero el documento detalla que es del 14 de ese mes, esto es, 7 días de diferencia entre ambos datos.

Imagen 1- Memorando GG-ME-1044-2022

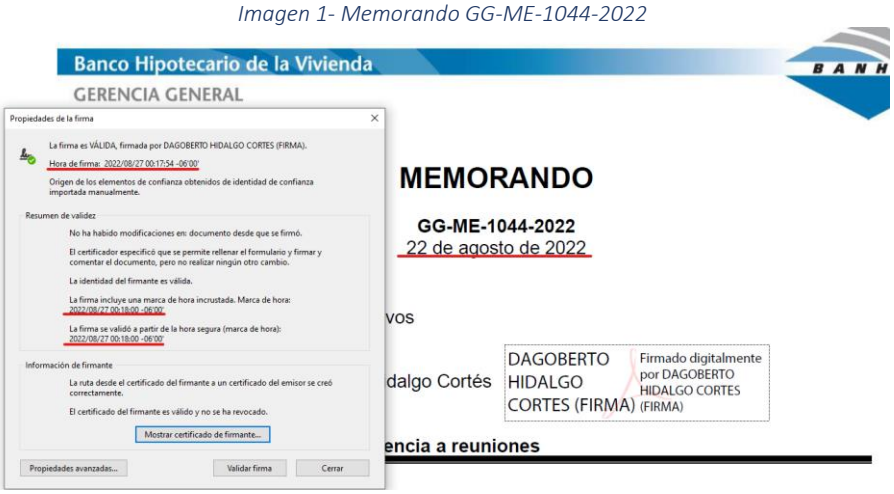


Imagen 2- Oficio BANHVI-GG-OF-0176-2023

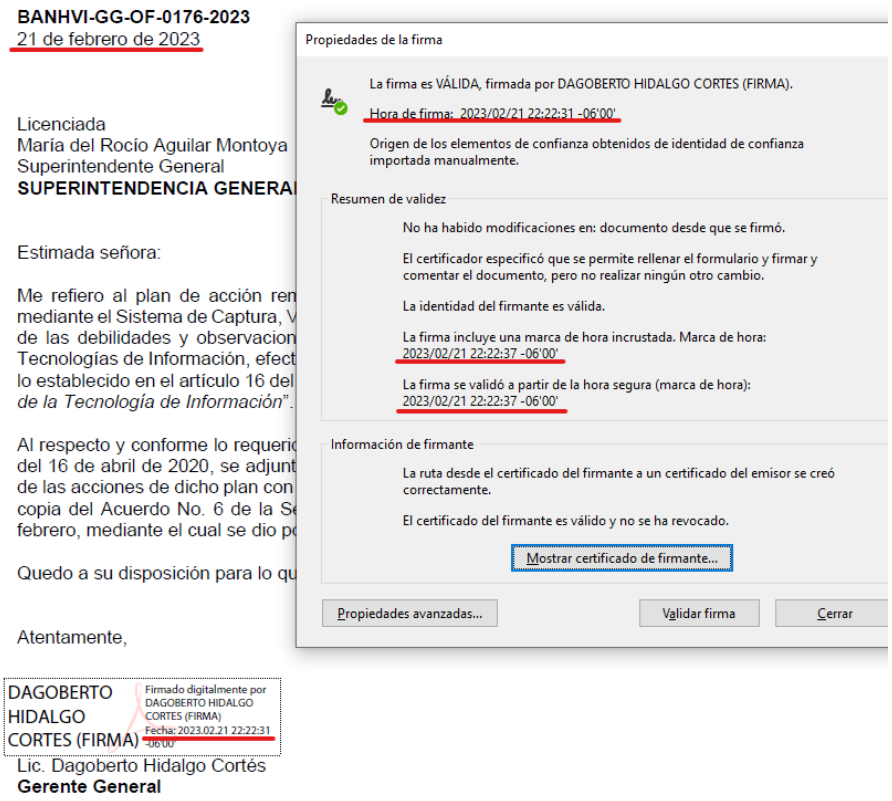
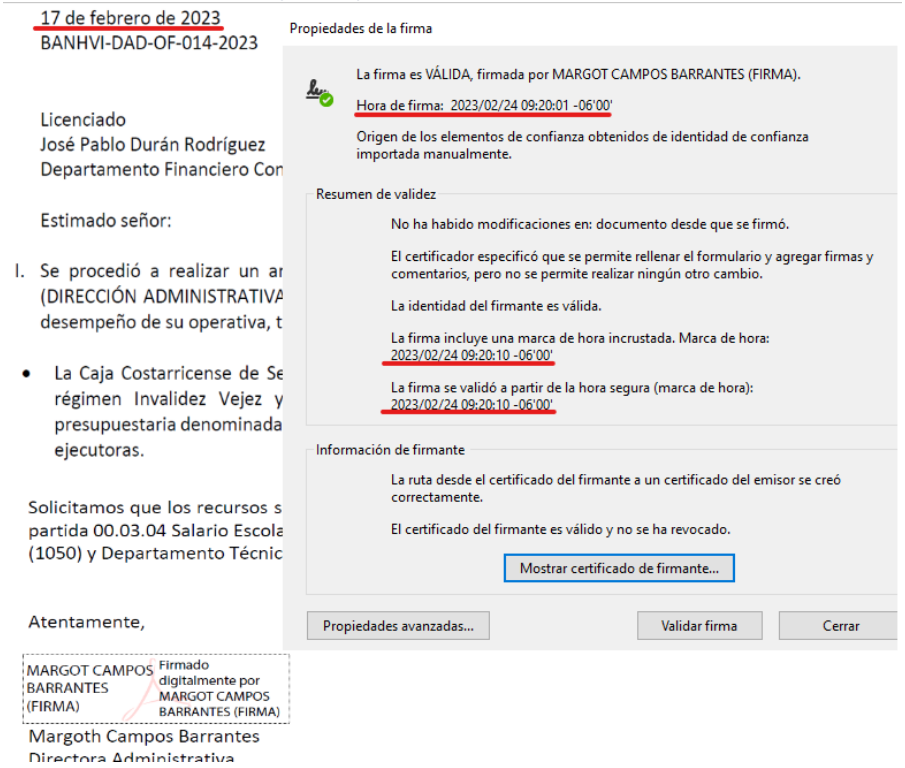


Imagen 3- Oficio BANHVI-DAD-OF-014-2023



17 de febrero de 2023
BANHVI-DAD-OF-014-2023

Licenciado
José Pablo Durán Rodríguez
Departamento Financiero Con

Estimado señor:

I. Se procedió a realizar un ar
(DIRECCIÓN ADMINISTRATIVA
desempeño de su operativa, t

- La Caja Costarricense de Se
régimen Invalidez Vejez y
presupuestaria denominada
ejecutoras.

Solicitamos que los recursos s
partida 00.03.04 Salario Escola
(1050) y Departamento Técnic

Atentamente,

MARGOT CAMPOS BARRANTES (FIRMA)
Firmado digitalmente por MARGOT CAMPOS BARRANTES (FIRMA)

Margoth Campos Barrantes
Directora Administrativa

Propiedades de la firma

La firma es VÁLIDA, firmada por MARGOT CAMPOS BARRANTES (FIRMA).

Hora de firma: 2023/02/24 09:20:01 -06'00'

Origen de los elementos de confianza obtenidos de identidad de confianza importada manualmente.

Resumen de validez

No ha habido modificaciones en: documento desde que se firmó.

El certificador especificó que se permite rellenar el formulario y agregar firmas y comentarios, pero no se permite realizar ningún otro cambio.

La identidad del firmante es válida.

La firma incluye una marca de hora incrustada. Marca de hora: 2023/02/24 09:20:10 -06'00'

La firma se validó a partir de la hora segura (marca de hora): 2023/02/24 09:20:10 -06'00'

Información de firmante

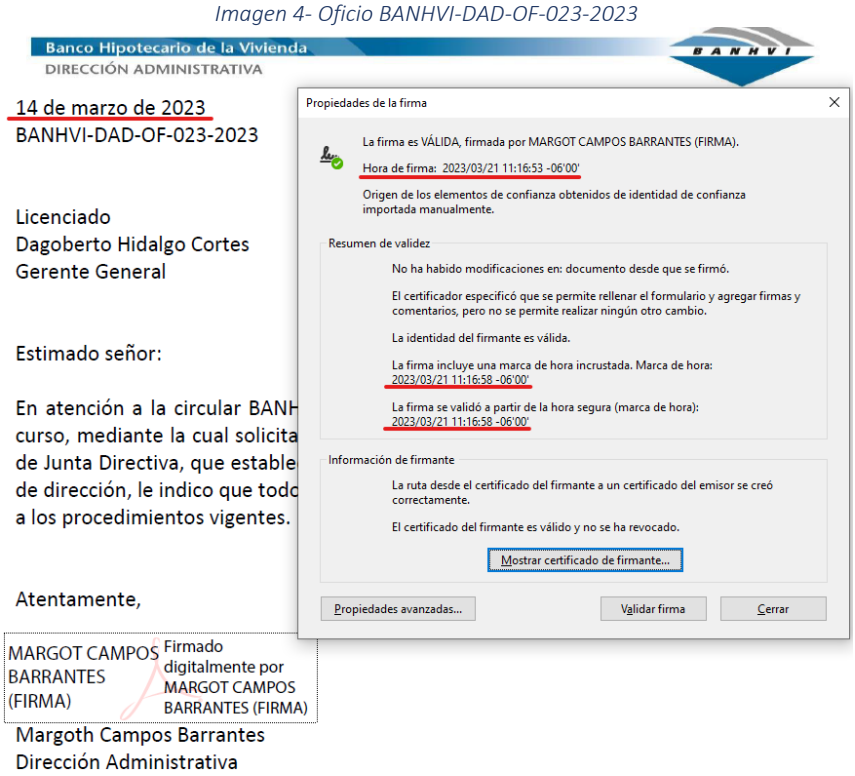
La ruta desde el certificado del firmante a un certificado del emisor se creó correctamente.

El certificado del firmante es válido y no se ha revocado.

Mostrar certificado de firmante...

Propiedades avanzadas... | Validar firma | Cerrar

Imagen 4- Oficio BANHVI-DAD-OF-023-2023



Banco Hipotecario de la Vivienda
DIRECCIÓN ADMINISTRATIVA

14 de marzo de 2023
BANHVI-DAD-OF-023-2023

Licenciado
Dagoberto Hidalgo Cortes
Gerente General

Estimado señor:

En atención a la circular BANH
curso, mediante la cual solicita
de Junta Directiva, que establec
de dirección, le indico que todo
a los procedimientos vigentes.

Atentamente,

MARGOT CAMPOS BARRANTES (FIRMA)
Firmado digitalmente por MARGOT CAMPOS BARRANTES (FIRMA)

Margoth Campos Barrantes
Dirección Administrativa

Propiedades de la firma

La firma es VÁLIDA, firmada por MARGOT CAMPOS BARRANTES (FIRMA).

Hora de firma: 2023/03/21 11:16:53 -06'00'

Origen de los elementos de confianza obtenidos de identidad de confianza importada manualmente.

Resumen de validez

No ha habido modificaciones en: documento desde que se firmó.

El certificador especificó que se permite rellenar el formulario y agregar firmas y comentarios, pero no se permite realizar ningún otro cambio.

La identidad del firmante es válida.

La firma incluye una marca de hora incrustada. Marca de hora: 2023/03/21 11:16:58 -06'00'

La firma se validó a partir de la hora segura (marca de hora): 2023/03/21 11:16:58 -06'00'

Información de firmante

La ruta desde el certificado del firmante a un certificado del emisor se creó correctamente.

El certificado del firmante es válido y no se ha revocado.

Mostrar certificado de firmante...

Propiedades avanzadas... | Validar firma | Cerrar

Según lo establece la Dirección de Gobernanza Digital del Ministerio de Ciencia, Tecnología y Telecomunicaciones, en el documento MICITT-DGD-OF-175-2020 del 10 de diciembre de 2020, relacionado con el criterio legal sobre la validez y eficacia en el tiempo de los actos suscritos con firma digital certificada, detalla:

> *"De acuerdo con el análisis realizado, y con base al ordenamiento jurídico vigente, esta Dirección concluye que:*
> *1.* ***Es responsabilidad de todo funcionario, a la hora de recibir un documento electrónico firmado con firma digital certificada, verificar que esta firma haya sido emitida por una autoridad certificadora autorizada en el país****, y que cumpla con todas las características que exige la normativa vigente de firma digital.*
> *2.* ***La responsabilidad de recibir un documento electrónico firmado con firma digital certificada es la misma responsabilidad que acarrea a todos los funcionarios que reciben documentos de manera física****, el que sea de manera digital no excluye dicha responsabilidad y la no verificación de estos requisitos podrá implicar responsabilidades por su no realización, como lo ha sido siempre dentro de los procesos tradicionales de documentos físicos." (*El destacado es nuestro)

En el punto 27 del artículo 2 sobre definiciones del Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N°33018 del 20 de marzo de 2016, se detalla:

> *"27) INTEGRIDAD: Propiedad de un documento electrónico que denota que su contenido y características de identificación han permanecido inalterables desde el momento de su emisión, o bien que -habiendo sido alterados posteriormente- lo fueron con el consentimiento de todas las partes legitimadas."*

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 acuerdo con lo que se pudo verificar en el análisis respectivo, el que no se utilice un estándar para la firma digital utilizada por la Gerencia General y la Dirección Administrativa, se debe a que no se ha establecido la normativa que regule y

establezca la forma en que deben ser implementadas tales firmas en los documentos oficiales emitidos por las distintas unidades de la institución.

Una consecuencia directa de esta situación es que ciertos oficios, memorandos o informes deben ser remitidos por las áreas antes de determinada fecha; situación que como se indicó no se podría verificar solo con ver el documento, sino que deben realizarse las validaciones antes detalladas, actividad que al no estar normada a nivel institucional, podría permitir que se envíe y reciban documentación oficial que cuente con fechas de entrega de forma extemporánea, dejando inválido tanto el documento como el proceso o las acciones que tengan relacionadas.

2.3 Actualización y conservación de documentos firmados digitalmente

En conformidad con lo indicado en el hallazgo 2.1 de este informe, por un error con el sistema SIGECE, los documentos en formato PDF que fueron cargados a manera de comunicación por las distintas áreas del Banco para posteriormente ser descargados por los destinarios con el objetivo de resguardarlos en sus repositorios, como se explicó dichos archivos fueron convertidos en formato de imagen. Esta situación genera que los documentos que cuentan con esa característica no sean válidos según el ordenamiento jurídico nacional, ya que no sería posible verificar la firma digital del funcionario que gestionó cada oficio, memorando o informe.

En el punto 3 de la Ley de Protección de la persona frente al tratamiento de sus datos personales No.8968 de 7 de julio de 2011, se indica lo siguiente:

> *"3.- **Exactitud***
>
> *Los datos de carácter personal deberán ser exactos. La persona responsable de la base de datos tomará las medidas necesarias para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados.*
>
> *Si los datos de carácter personal registrados resultan ser inexactos en todo o en parte, o incompletos, serán eliminados o sustituidos de oficio por la persona responsable de la base de datos, por los correspondientes datos rectificados, actualizados o complementados. Igualmente, serán eliminados si no media el consentimiento informado o está prohibida su recolección." (*El subrayado es nuestro)

La Ley de Certificados, Firmas Digitales y Documentos Electrónicos No. 8454 del 30 de agosto de 2005, indica en sus artículos 4, 5 y 11 lo siguiente:

*"Artículo 4- **Calificación jurídica y fuerza probatoria**. Los documentos electrónicos se calificarán como públicos o privados, y se les reconocerá fuerza probatoria en las mismas condiciones que a los documentos físicos.*

*Artículo 5- **En particular y excepciones**: En particular y sin que conlleve la exclusión de otros actos, contratos o negocios jurídicos, la utilización de documentos electrónicos es válida para lo siguiente:*

(…)
c) La tramitación, gestión y conservación de expedientes judiciales y administrativos; asimismo, la recepción, práctica y conservación de prueba, incluida la recibida por archivos y medios electrónicos. De igual manera, los órganos jurisdiccionales que requieran la actualización de certificaciones y, en general, de otras piezas, podrán proceder sobre simples impresiones de los documentos en línea efectuadas por la autoridad judicial o aceptar las impresiones de dichos documentos en línea, aportadas por la parte interesada y certificadas notarialmente.
(…)

*Artículo 11.-**Alcance**. Entiéndese por certificado digital el mecanismo electrónico o digital mediante el que se pueda garantizar, confirmar o validar técnicamente:*
a) La vinculación jurídica entre un documento, una firma digital y una persona.
b) La integridad, autenticidad y no alteración en general del documento, así como la firma digital asociada.
c) La autenticación o certificación del documento y la firma digital asociada, únicamente en el supuesto del ejercicio de potestades públicas certificadoras.
d) Las demás que establezca esta Ley y su Reglamento." El subrayado es propio." El subrayado es propio.

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)

Como causa principal de que existan documentos oficiales resguardados como imágenes, se encuentra el error de conversión presentando por el sistema SIGECE, pero

adicionalmente no se localizó una normativa que regule el proceso de conservación de archivos en los repositorios de las distintas unidades o departamentos del Banco.

Una posible consecuencia de esta situación es que es al momento de revisiones ejecutadas por órganos internos o externos, los archivos que se presenten como imagen no sean aceptados como documentos oficiales ya que no sería posible realizar la vinculación entre el documento, la firma y la persona física que lo firmó.

2.4 Validez y controles generales de la firma digital

Como parte de la evaluación de la normativa nacional con relación a la administración y control de la firma digital en las instituciones del estado, se logró determinar que las firmas digitales que se adjuntan a los documentos oficiales del Banco no cuentan con un proceso establecido para determinar su ejecución, validez, administración, preservación, revocación, entre otros.

En este sentido, el Banco Central de Costa Rica ha puesto a disposición del público en general un sistema en línea con el cual se puede validar las principales características de un archivo firmado digitalmente, específicamente en la dirección: https://www.centraldirecto.fi.cr/spa/Bccr.Firma.Fva.ValidadorDocumentoPublico.CD.SPA/#/inicio

Seguidamente se muestra un ejemplo de un documento revisado con dicho sistema, donde se resalta que la garantía de validez en el tiempo no es correcta, siendo necesario hacer las modificaciones correspondientes:

Imagen 3- Ejemplo de validación WEB de firma digital

SELECCIONE EL DOCUMENTO A VALIDAR | RESULTADO DE LA VALIDACIÓN DE LA FIRMA DIGITAL

Nombre del documento: BANHVI-GG-OF-0176-2023 SUGEF Informe avance plan de acción AE de TI al 31-01-2023.pdf

Formato: Pdf

Tamaño: 164 KB

Resumen:

✓ **Garantía de integridad y autenticidad**

✗ **Garantía de validez en el tiempo**

Firmantes:

Firmante	Fecha oficial de la firma	Garantía de integridad y autenticidad	Garantía de validez en el tiempo
DAGOBERTO HIDALGO CORTES Cédula: 07-0129-0954	21/02/2023 10:22:37 p.m.	✓	✗

Detalle de la Firma Digital:

Firma Digital 1

✓ La firma es válida hoy 24/04/2023 03:52:50 p.m.

Autoría del firmante garantizada

Nombre: DAGOBERTO HIDALGO CORTES

Identificación: 07-0129-0954

Resumen:

✓ Garantía de integridad y autenticidad

⚠ La firma es válida hasta el 09/08/2024 02:01:29 p.m. cuando vence el certificado del firmante.

Detalle:

⚠ **Jerarquía de confianza:** El documento fue firmado con un certificado oficial pero los certificados de la jerarquía no están contenidos en el documento.

✓ **Integridad:** El contenido del documento no ha sido modificado después de realizada la firma.

✓ **Vigencia:** El certificado digital estaba vigente al momento de la firma.

✓ **Tipo de certificado:** El tipo de certificado utilizado es válido para firmar.

⚠ **Revocación:** El certificado no estaba revocado en el momento de la firma, pero la información necesaria para la validación de la revocación no está contenida en el documento.

⚠ **Fecha oficial de la firma:** El documento cuenta con una estampa de tiempo en el momento de la firma. Pero no incluye información de revocación o los certificados de la jerarquía correspondiente.

- **Fecha de la estampa de tiempo:** 21/02/2023 10:22:37 p.m.

El documento denominado Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente de la Dirección de Certificadores de Firma Digital del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) del 20 de mayo de 2013, detalla en sus puntos 4.1, 4.4 y 4.5 lo siguiente:

> *"4.1 Resumen*
> *La Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente establece el conjunto de reglas generales para el procesamiento de documentos electrónicos firmados digitalmente, tanto para la realización de la firma digital como para la verificación de su validez en cualquier momento en el tiempo."*
>
> *4.4 Cumplimiento*
> *Las entidades públicas, empresas privadas o particulares que deseen implementar soluciones con mecanismos de firma digital, tanto para soluciones internas, interinstitucionales, o para los servicios ofrecidos a sus clientes o administrados, deberán cumplir con los lineamientos establecidas en esta política para generar y procesar documentos mediante el uso de formatos oficiales, según el conjunto de responsabilidades que les corresponda (firma digital y/o validación de la firma digital).*
>
> *4.5 Vigencia*
> *La "Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente" rige a partir de su publicación.*
> *Se establece un periodo transitorio de 24 meses naturales a partir de su publicación para que las entidades públicas, empresas privadas o particulares que utilizan documentos electrónicos firmados digitalmente en sistemas informáticos a la medida o mediante soluciones ofimáticas ya instaladas, utilicen el formato oficial como soporte electrónico estandarizado cuando sea necesario el uso de firmas digitales."* Lo subrayado es de nuestra autoría.

En la Ley de Certificados, Firmas Digitales y Documentos Electrónicos No. 8454 del 30 de agosto de 2005, se indica en su artículo 10 lo siguiente:

> *"Artículo 10.-**Presunción de autoría y responsabilidad**. Todo documento, mensaje electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.*
> *No obstante, **esta presunción no dispensa el cumplimiento de las formalidades adicionales de autenticación, certificación o registro** que, desde el punto de vista jurídico, exija la ley para un acto o negocio determinado."* El destacado es propio.

Así mismo y según lo establece la Dirección de Gobernanza Digital del Ministerio de Ciencia, Tecnología y Telecomunicaciones, en el MICITT-DGD-OF-175-2020 del 10 de diciembre de 2020:

> *"De acuerdo con el análisis realizado, y con base al ordenamiento jurídico vigente, esta Dirección concluye que:*
> *1. Es responsabilidad de todo funcionario, a la hora de recibir un documento electrónico firmado con firma digital certificada, verificar que esta firma haya sido emitida por una autoridad certificadora autorizada en el país, y que cumpla con todas las características que exige la normativa vigente de firma digital."* El subrayado es nuestro.

Según se logró determinar, esta situación se presenta debido a que en el Banco no se ha establecido una Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente, tal como lo detalla el MICITT como parte de sus regulaciones.

Un efecto de no contar con la normativa que haga referencia a los procesos de ejecución, revisión, revocación, administración, conservación u otros, se podrían dar por aceptados documentos firmados digitalmente que, desde el punto de vista de legalidad, no cuentan con las características suficientes para ser aceptados como información oficial del Banco, haciendo por defecto ilegal el comunicado que en ellos se realice.

3. CONCLUSIÓN

De acuerdo con el avance tecnológico que se ha tenido en los últimos años, el uso de la firma digital tanto a nivel institucional como nacional se ha vuelto un requisito para poder determinar la autoría de un documento, siendo además utilizada para poder confirmar que dicho documento no ha sido alterado desde que fue firmado por su remitente.

En la revisión realizada sobre este particular, la Auditoría Interna pudo localizar algunos aspectos que pueden ser mejorados con el desarrollo e implementación de ciertos controles tanto a nivel normativo como operativo, mismos que forman parte del ciclo normal en la implementación de herramientas y tecnologías que el Banco ha tenido que adoptar según las crecientes demandas implantadas por el entorno en que participa, ya sean regulatorias, tecnológicas u operativas.

La finalidad de este informe es que la Administración Activa pueda identificar y mejorar puntos específicos en el uso de estas tecnologías, lo cual por consiguiente produciría una mejora general en el control interno relacionado con dicho proceso. Para esto, se detallan en la siguiente sección de este informe recomendaciones específicas orientadas a dicho fin.

4. RECOMENDACIONES

En relación con los informes de la Auditoría Interna dirigidos a los titulares subordinados, la Ley General de Control Interno No. 8292 en su artículo 36 establece:

*"Artículo 36. —**Informes dirigidos a los titulares subordinados**. Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*

a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.

b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.

c) *El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda."*

4.1 Conversión de documentos con firma digital

Al Departamento de TI

Es necesario realizar las modificaciones necesarias en el sistema de SIGECE para que se subsanen las debilidades de control relacionadas con la conversión de archivos PDF a imágenes al momento en que son descargados. Como parte de la documentación de este trabajo, se debe incluir las razones por las que se produjo el error, así como las actividades ejecutadas para la solución; esto con el fin de que sea parte de los conocimientos adquiridos para posibles futuras correcciones.
Nivel de Riesgo: **Alto**

4.2 Estandarización en el uso de la firma digital

A la Dirección Administrativa

4.2.1 Con el fin de estandarizar el uso de la firma digital en todos los documentos oficiales de la institución, es necesario que se elabore e implemente la normativa necesaria, la cual regule toda la información y los componentes obligatorios que debe poseer la firma digital al momento de utilizarse en los documentos oficiales de la institución. En caso de ser necesario, se debe validar con el Departamento de TI las características técnicas que previamente tienen que ser definidas y habilitadas en todos los equipos que vayan a utilizar dicha tecnología.
Nivel de Riesgo: **Medio**

4.2.2 Es necesario instaurar como parte del proceso de revisión de los documentos firmados digitalmente, la validación de las fechas de envío de los oficios versus las fechas en que son firmados digitalmente los documentos, esto con el objetivo de determinar si los oficios o memorandos se encuentran dentro de los plazos permitidos, cuando esta situación sea aplicable al documento que se remite y recibe.
Nivel de Riesgo: **Medio**

4.3 Actualización y conservación de documentos firmados digitalmente

A la Dirección Administrativa

4.3.1 Se deben girar las instrucciones correspondientes para que todas las unidades y áreas del Banco realicen un inventario de los archivos con formato PDF que hayan sido descargados desde el SIGECE y que estén resguardados en sus repositorios, con la finalidad de remplazar todos aquellos que fueron copiados

como una imagen y no como el documento original (PDF), cuando los mismos cuenten con las firmas digitales de su emisor.
Nivel de Riesgo: **Medio**

4.3.2 Se debe elaborar la normativa correspondiente que defina la metodología para el resguardo de los archivos firmados digitalmente que se copian en los repositorios de la Intranet creados para cada área o unidad del Banco. Dicho procedimiento además de indicar la forma en que deben guardarse tales documentos, debe detallar las características que deben poseer para que sea considerado como válido desde el punto de vista de legalidad.
Nivel de Riesgo: **Medio**

4.4 Validez y controles generales de la firma digital

A la Dirección Administrativa

Es necesario que se instaure en el Banco una política que gestione todo el proceso de administración y control de los documentos que son firmados digitalmente. Para esto, se recomienda que se utilice el documento denominado "*Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente*" elaborar por el MICITT para estos fines y en el cual se establecen todos los rubros operativos y técnicos que deben ser acatados para este tipo de procesos.
Nivel de Riesgo: **Alto**

Estudio realizado por:

JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)

Firmado digitalmente por JORGE ANTONIO RAMIREZ BOLAÑOS (FIRMA)
Fecha: 2023.09.06 13:10:05 -06'00'

MATI. Jorge Ramírez Bolaños
Auditor Encargado

Firmado digitalmente por GUSTAVO FLORES OVIEDO (FIRMA)
Fecha: 2023.09.06 14:29:51 -06'00'

Aprobado MBA. Gustavo Flores Oviedo
Auditor Interno