



20 de agosto de 2024  
**AI-Ad-017-2024**

Señor:  
Rafael Soto Quirós  
Gerente general pro t mpore

*Asunto: Servicio de advertencia sobre la validez jur dica de los documentos electr nicos firmados digitalmente*

Estimado se or:

La Auditor a en cumplimiento del Plan Anual de Trabajo, revisa la “*Directriz uso de la firma digital y gesti n electr nica de documentos*”<sup>1</sup>, con el fin de verificar si cumple con los est ndares requeridos y garantiza la accesibilidad y validez legal de los documentos a largo plazo, determin ndose lo siguiente:

### **Autenticidad e integridad de los documentos electr nicos**

#### **Condici n**

Se revisa una muestra<sup>2</sup> de documentos electr nicos<sup>3</sup> emitidos por varias dependencias de la Instituci n, con el fin de verificar si estos cumplen con la validez legal de acuerdo con la normativa, determin ndose que un 80% (48) presentan advertencias sobre la fecha oficial de la firma<sup>4</sup> por la omisi n de la marca o estampa de tiempo.

---

<sup>1</sup> Comunicada por la Gerencia mediante oficio G-1639-2023 (17/08/2023).

<sup>2</sup> Muestra de 60 documentos electr nicos.

<sup>3</sup> Ley 8454 de Certificados, Firmas Digitales y Documentos Electr nicos de Costa Rica, art culo 3 estipula como documento electr nico a “Cualquier manifestaci n con car cter representativo o declarativo, expresada o transmitida por un medio electr nico o inform tico, se tendr  por jur dicamente equivalente a los documentos que se otorguen, residan o transmitan por medios f sicos.

<sup>4</sup> Fecha en que una autoridad competente ubica la firma en el tiempo.



El ICT no cuenta con actividades de control para validar la validez legal de los documentos electrónicos recibidos y emitidos por terceros.

## Causa

La condición determinada se presenta porque:

1. La “*Directriz uso de la firma digital y gestión electrónica de documentos*” establece que los documentos digitales son válidos desde su suscripción digital, pero omite la utilización de la estampa de tiempo, la responsabilidad de los funcionarios con la misma y la verificación de la validez del documento electrónico.
2. No hay actividades de control -políticas, procedimientos o mecanismos- que proporcionen un marco para asegurar el correcto uso de la firma digital, el estampado de tiempo y la verificación de la validez del documento electrónico.

## Criterio

La ley de certificados, firmas digitales y documentos electrónicos<sup>5</sup>, artículo 6 - Gestión y conservación de documentos electrónicos establece que, 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.

La política de formatos oficiales de los documentos electrónicos firmados digitalmente<sup>6</sup>, establece lo siguiente:

### *“5.2.1 Firma digital certificada del documento electrónico*

*Cuando se firma digitalmente un documento electrónico, se deberá asegurar que el sistema o sistemas que implementan los mecanismos de firma digital certificada incluyan los atributos descritos a continuación (siempre respetando el estándar que corresponda):*

---

<sup>5</sup> Ley N° 8454

<sup>6</sup> Emitida por el Ministerio de Ciencia, Tecnología y Telecomunicaciones -MICITT-



Nombre del atributo	Descripción del atributo	Etapas de proceso posibles para la inclusión del atributo en el documento
Resumen hash encriptado (digest)	Mecanismo criptográfico que permite garantizar la integridad y autenticidad del documento.	Emisión
Certificado del firmante	Copia del certificado del firmante que permite verificar la autoría del documento.	Emisión
Tokens de estampado de tiempo	Solicitados a una TSA de la jerarquía del Sistema Nacional de Certificación Digital.	Emisión o Recepción
Ruta de certificación	Cadenas de certificados que ubiquen el certificado del firmante y de las estampas de tiempo en la jerarquía del Sistema Nacional de Certificación Digital.	Emisión o Recepción
Información de revocación	Respuestas de validez del certificado del firmante, de las estampas de tiempo y de todos los certificados de sus respectivas rutas de certificación.	Emisión o Recepción

*Dicha inclusión permitirá garantizar, a través del tiempo, la validez de la firma digital certificada que se plasme en un documento electrónico, lo cual es imprescindible para temas de gestión documental.”*

*“5.2.2 Verificación de la validez de la firma digital en el documento electrónico. Para verificar la validez de un documento electrónico firmado digitalmente en el formato oficial, es imperativo que se realicen las siguientes validaciones de los diferentes atributos que el documento contiene:*

Nombre del atributo	Descripción de la actividad de validación
Resumen hash encriptado (digest)	Verificar que hash encriptado corresponda con el documento electrónico
Certificado del firmante	Verificar que la firma del documento corresponde con el certificado del firmante
Tokens de estampado de tiempo	Verificar que los tokens de estampado de tiempo son de fechas previas a la fecha de vencimiento de los certificados



Nombre del atributo	Descripción de la actividad de validación
	del firmante o de las rutas de certificación e información de revocación según corresponda, y así garantizar que todos los certificados y cadenas eran vigentes y válidas cuando se usaron.
Rutas de certificación	Verificar que todos los certificados del documento correspondan a certificados de la jerarquía del Sistema Nacional de Certificación Digital.
Información de revocación	Verificar que todos los certificados del documento eran válidos (vigentes y no revocados) en el momento de su inclusión en el documento.

*Consideraciones para la verificación de la firma digital certificada:*

- *La firma digital certificada es un algoritmo matemático que se le agrega al documento electrónico cuando es firmado digitalmente.*
- *Los documentos electrónicos firmados digitalmente son una manifestación expresa de la voluntad del firmante representado por un medio electrónico o informático.*
- *La representación gráfica de una firma digital certificada, una impresión o captura de imagen de un documento electrónico firmado digitalmente, por sí solo, no cuenta con validez.*
- *La firma digital certificada se valida solamente de manera digital y deberá cumplir con la normativa vigente, lo cual incluye la Ley, reglamento y políticas.”*

*“5.2.3 Consideraciones adicionales para la inclusión de los atributos.*

*Tal y como se desprende de la presente política y de los estándares a los que hace referencia, los atributos “Resumen hash encriptado (digest)” y “Certificado del firmante” solo pueden agregarse en presencia de cada uno de los firmantes titulares de los certificados que realizan un ejercicio de firma sobre el documento electrónico. Los restantes atributos, “Tokens de estampado de tiempo”, “Rutas de certificación” e “Información de revocación”, pueden agregarse posterior al ejercicio de firmado del/de los firmantes del documento al momento de la recepción del mismo. Esto último es cierto siempre y cuando los certificados de los firmantes, y los certificados de la jerarquía, no hayan vencido ni tampoco*



*hayan sido revocados y de acuerdo con el inciso 4.4 de esta Política acerca del cumplimiento.*

*El escenario descrito es una medida existente para atender el riesgo de que, al tratar de hacer una firma digital certificada en formato oficial, los servicios de respuesta en línea o los repositorios de información de revocación no estén disponibles; con el objetivo de que dicha eventualidad no limite la creación de firmas digitales certificadas en documentos electrónicos, a los que posteriormente pueden incluirse todos los atributos adicionales que permiten la verificación de la validez de la firma digital certificada del documento electrónico a largo plazo. para el uso adecuado del documento electrónico que asegure el cumplimiento de las normativas legales y las mejores prácticas en la gestión documental.”*

La directriz<sup>7</sup> “Masificación de la implementación y el uso de la firma digital en el sector público costarricense”, estipula lo siguiente:

*Artículo 6°—En todo momento, los mecanismos de firma digital certificada deberán implementarse respetando la normativa vigente al respecto, garantizando así la validez de las firmas digitales en el tiempo, potenciando la interoperabilidad en el intercambio de documentos electrónicos entre instituciones, la apropiada conservación de los documentos electrónicos firmados digitalmente, y el valor legal de la interacción entre el ciudadano y la institución por medios electrónicos a través del tiempo.*

*“Artículo 8°—Las instituciones del sector público costarricense deberán realizar campañas y actividades de educación para sus funcionarios, que les permita aprender a utilizar los mecanismos de firma digital, así como reconocer la equivalencia jurídica y la eficacia probatoria de los documentos electrónicos firmados digitalmente con respecto a los documentos en papel con firmas autógrafas, tal como la Ley N° 8454 lo establece. Para el caso de aquellos funcionarios responsables de la recepción y/o trámite de los documentos electrónicos, deberán también*

---

<sup>7</sup> N° 067-MICITT-H-MEIC del 25/04/2014



*capacitarlos técnicamente para poder reconocer, interpretar y validar las firmas digitales asociadas a éstos documentos electrónicos.”*

## Efectos

La condición determinada puede materializarse en los riesgos siguientes:

- **Cumplimiento normativo**
  - **Valor probatorio:** La posibilidad de que se pierda el valor probatorio y veracidad del documento electrónico.
  - **Autoría y responsabilidad:** Pérdida de la presunción de autoría y responsabilidad del documento digital.
  - **Vinculación:** imposibilidad de vinculación entre el documento, una firma y la persona.
  - **Integridad:** La presunción de la integridad, autenticidad y no alteración en general del documento, así como de la firma digital asociada.

## Conclusión

La “*Directriz uso de la firma digital y gestión electrónica de documentos*” no cumple con la accesibilidad y la validez legal de los documentos, porque es omisa en la utilización de la estampa de tiempo que es un elemento esencial para preservar la integridad, la autenticidad y la validez legal que los documentos electrónicos deben mantener a lo largo del tiempo.

## Valor agregado de la Auditoría

El valor agregado que la Auditoría está aportando con este preventivo es en lo siguiente:

1. Contribuir con el cumplimiento del objetivo estratégico “Optimizar los procesos”.
2. Fortalecer los objetivos del sistema de control interno:
  - a. Exigir confiabilidad y oportunidad de la información.
  - b. Cumplir con el ordenamiento jurídico y técnico.
3. Que se administren los riesgos identificados y se fortalezcan los controles para minimizarlos.
4. Mejorar el marco legal institucional con el fin de cumplir las normativas legales y técnicas.



5. Asegurar la validez legal de los documentos electrónicos y su correcta conservación a largo plazo.

La Ley Orgánica, artículo 32, establece que la Gerencia es el responsable del eficiente y correcto funcionamiento administrativo de la Institución y debe ejercer las funciones inherentes a su condición de administrador general y jefe superior del Instituto, vigilando la organización, funcionamiento y coordinación de todas sus dependencias y la observación de las leyes, reglamentos y resoluciones de la Junta Directiva, razón por la cual, se comunica lo determinado sobre la validez de los documentos electrónicos, con el propósito que se tomen las acciones pertinentes para que se subsanen las causas identificadas y administrar al menos los riesgos determinados en este servicio preventivo.

Se solicita a la Gerencia, informar a esta Auditoría Interna dentro de los próximos diez días hábiles, sobre las acciones tomadas en relación con este servicio preventivo, a efecto de determinar lo procedente.

El presente servicio se realiza con fundamento en las competencias conferidas a la Auditoría Interna en la Ley Orgánica del ICT, artículos 33 y 35, la Ley General de Control Interno, artículo 22, inciso d), las “Normas para el Ejercicio de la Auditoría Interna en el Sector Público”, norma 1.1.4 y en atención del Plan Anual de Trabajo.

Atentamente,

Karen Barquero Murillo  
**Ejecutivo de turismo 3**

Romel Álvarez Navarro  
**Auditor interno**

- C. Sra. Karen Hernández Bonilla  
Jefe Departamento de Tecnologías Información y Comunicación  
Sr. Juan Carlos Quirós Espinoza  
Jefe Departamento Administrativo  
Sra. Teresita Calvo Acevedo  
Encargada Archivo central  
Consecutivo

RAN/kbm