26 de enero de 2016
CIRCULAR Nº 43.082

Señores
Directores Servicios de Sede
Directores de Gestión Regional y Red de Servicios de Salud
Directores Regionales de Sucursales
Directores Administrativos y Jefes de Servicio
de Hospitales y Clínicas
Jefes de Departamento, Sección y Oficina
Jefe de Sucursales y Agencias
Caja Costarricense de Seguro Social
Presente

Estimados señores:

Asunto: Reglamento de firmas digitales y firmas certificadas de la Caja Costarricense de Seguro Social.

Para lo correspondiente, me permito informarles que el Reglamento de firmas digitales y firmas digitales certificadas de la Caja Costarricense de Seguro Social, que en adelante se transcribe, aprobado en el artículo 51° de la sesión Nº8816, celebrada el 10 de diciembre del año 2015, fue publicado en "La Gaceta" Nº 15 del 22 de enero de 2016:

"REGLAMENTO DE FIRMAS DIGITALES Y FIRMAS DIGITALES CERTIFICADAS DE LA CAJA COSTARRICENSE DE SEGURO SOCIAL

Capítulo I
Disposiciones Generales

Artículo 1.- Objeto. El presente Reglamento tiene por objeto regular el uso de Firma Digital y Firma Digital Certificada como mecanismos de seguridad, autenticación e identidad digital, para la emisión de documentos electrónicos y digitales en la Caja, conforme con las disposiciones del presente Reglamento y lo dispuesto en la Ley número 8454 y la normativa que la complementa.

Artículo 2.- Alcance. El presente Reglamento se aplicará a los funcionarios o unidades internas de la Caja, conforme con los procesos telemáticos que se habiliten acorde con los programas y proyectos afines con los planes maestros de innovación, gobierno digital y modernización del Estado.

Artículo 3.- Definiciones. Para los efectos del presente Reglamento, se entenderán los siguientes conceptos:

AUTENTICACIÓN: Verificación de la identidad de un individuo que se realiza:

a. En el proceso de registro. Es el acto de evaluar las credenciales de la entidad final (por ejemplo, un suscriptor) como evidencia de que realmente es quien dice ser.

b. Durante el uso del Certificado Digital. Es el acto de comparar electrónicamente las credenciales y la identidad enviada (código de usuario y contraseña, certificado digital) con valores previamente establecidos para comprobar la identidad.

AUTORIDAD CERTIFICADORA: La persona jurídica pública o privada, nacional o extranjera, prestadora del servicio de creación, emisión y operación de certificados digitales.

AUTORIDAD CERTIFICADORA RAÍZ: El nodo superior auto certificante de la jerarquía nacional de certificadores registrados.

AUTORIDAD CERTIFICADORA REGISTRADA: La Autoridad Certificadora inscrita y autorizada por la Dirección de Certificadores de Firma Digital.

AUTORIDAD DE REGISTRO: Entidad delegada por la Autoridad Certificadora para la verificación de la identidad de los solicitantes y otras funciones dentro del proceso de expedición y manejo de certificados digitales. Representa el punto de contacto entre el usuario y la Autoridad Certificadora.

CERTIFICADO DIGITAL: Una estructura de datos creada y firmada digitalmente por una Autoridad Certificadora autorizada, para identificar y firmar digitalmente documentos electrónicos. Lo anterior, acorde con la Norma INTE/ISO 21188 versión vigente y las políticas que al efecto emita la Dirección de Certificadores de Firma Digital.

DOCUMENTO ELECTRÓNICO: Cualquier manifestación o conjunto de datos con carácter representativo o declarativo, creado, preservado, visualizado o transmitido por un medio electrónico o informático.

DOCUMENTO ELECTRONICO FIRMADO DIGITALMENTE: aquel documento electrónico, cualesquiera que sean su contenido, contexto y estructura, cuya estructura lógica tiene asociada una firma digital. En otras palabras, es un objeto conceptual que contiene tanto el documento electrónico como una firma digital, sin importar que estos dos elementos puedan encontrarse representados por conjuntos de datos diferentes (Conforme con la Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente)

FIRMA DIGITAL: Conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de autenticación y como medio para asegurar la integridad de los datos y el no repudio.

FIRMA DIGITAL CERTIFICADA: Firma digital emitida al amparo de un certificado digital, válido y vigente, expedido por la Autoridad Certificadora.

IDENTIDAD DIGITAL: Conjunto de rasgos unívocos que caracterizan a una persona física, en un medio de transmisión digital.

LEY número 8454: Ley de certificados, firmas digitales y documentos electrónicos.

MEDIO DE ALMACENAMIENTO: Medio físico donde residirá la información del certificado digital, residir en un dispositivo criptográfico seguro como una tarjeta inteligente o un token criptográfico u otro medio idóneo.

SUSCRIPTOR: Funcionario, persona física poseedor de un Certificado Digital emitido por la Autoridad Certificadora o bien un ente certificador, que funge como responsable de su debida custodia y adecuado uso, y con el cual podrá interactuar legítimamente con los sistemas de tecnología de información de la Caja y otros trámites electrónicamente realizados para los cuales se encuentre autorizado como usuario.

Capítulo II
De las firmas de documentos electrónicos

Artículo 4.- De la presunción de autoría y validez. Todos los documentos electrónicos asociados a una firma, se presumirán jurídicamente válidos en su emisión, integridad y autoría de quien lo emite. No obstante, el uso de medios electrónicos y digitales no dispensa el cumplimiento de requisitos y formalidades que el ordenamiento jurídico exija para cada acto o negocio jurídico en particular.

Artículo 5.- Implementación de Firmas Digitales. Las directrices, políticas y pautas técnicas acerca de los trámites en los que pueden ser utilizados éstos u otros medios electrónicos, serán definidas para cada tipo de proceso por parte de la Caja, previa coordinación técnica de la Dirección de Tecnologías de Información y Comunicaciones, conforme la verificación de infraestructura, sistemas, aplicaciones, medidas de seguridad y lineamientos emitidos al efecto.

Artículo 6. De las Firmas manuscritas y Firmas Digitales. Salvo disposición jurídica que obligue al uso de una firma específica, se continuarán utilizando los medios de firma manuscrita, firma digital y firma digital certificada en los registros electrónicos de la Caja, de forma que todo documento o mensaje electrónico y demás comunicaciones digitales internas o archivos asociados a una firma se presume válido en su autoría, alcances y responsabilidades, conforme con lo dispuesto por la Ley 8454 y su Reglamento.

Artículos 7.- De la Firma Digital Certificada. La firma digital certificada y los dispositivos criptográficos (tarjeta inteligente o cualquier otro medio de almacenamiento autorizado por el MICIT –Ministerio de Ciencia y Tecnología-) son de uso personalísimo, por lo que su emisión, entrega, uso y custodia son exclusivos del funcionario a quien se le asignen (suscriptor).

Es deber del funcionario salvaguardar el medio de almacenamiento en un lugar seguro y utilizarlo en forma personal para efectos de los trámites autorizados y conforme a los procedimientos establecidos, no revelando a nadie la clave de seguridad del certificado. Si en algún momento el Suscriptor sospecha que la seguridad del medio (o del certificado en sí) se ha visto comprometida por pérdida, sustracción, robo o deterioro, entre otros, debe reportarlo a la autoridad certificadora que emitió el certificado digital y a la Dirección de Tecnologías de la Información y Comunicaciones, para el respectivo control.

Artículo 8.- Período de vigencia del certificado digital. Los suscriptores deberán observar la vigencia de los certificados digitales reconocidos por los entes certificadores, por lo que vencido el certificado digital el funcionario deberá tramitar la renovación del mismo, conforme con la Ley 8454 y su Reglamento, el acuerdo de suscripción originario y las políticas institucionales que al efecto se emitan.

Artículo 9.- De la renovación del certificado digital. Para la renovación de los Certificados Digitales el Suscriptor requerirá únicamente que se mantengan las condiciones que originaron su emisión, podrá renovar por cuenta propia o a cargo de la Institución su certificado Digital; en este último caso deberá solicitar a la jefatura inmediata la aplicación del procedimiento que defina la Dirección de Tecnologías de Información y Comunicaciones para este fin.

Artículo 10.- Derechos del suscriptor de un Certificado Digital. El suscriptor de un Certificado Digital tiene los siguientes derechos:

- Ser informado sobre los medios a los que puede acudir para solicitar aclaraciones del mal funcionamiento de los Sistemas de Información.
- A la generación de un nuevo certificado cuando deje de funcionar el certificado digital, por causas ajenas al funcionario.
- Estar debidamente informado de todas sus obligaciones como suscriptor de un certificado digital.

Artículo 11.-Obligaciones de los funcionarios. Corresponde a todos los funcionarios institucionales participar en los procesos de modernización de las distintas plataformas de servicios, internos y externos, y de la aplicación de los Certificados Digitales so pena de que su inobservancia se constituya en falta sancionada conforme las disposiciones contenidas en el Reglamento Interior de Trabajo y la Normativa de Relaciones Laborales vigente, observar las siguientes obligaciones:

a. Resguardar estrictamente la confidencialidad de la clave, contraseña o mecanismo de identificación que se les haya asignado con ese carácter.
b. El usuario deberá informar inmediatamente a la Autoridad Certificadora y poner a su vez sobre aviso a la Dirección de Tecnologías Información y Comunicaciones, en caso de que dicha confidencialidad se vea o se sospeche que haya sido comprometida.
c. Abstenerse de prestar, ceder, escribir su número de identificación personal NIP (PIN, por sus siglas en inglés) y tomar todas las medidas razonables y oportunas para evitar que éste sea utilizado por terceras personas.
d. No transferir, compartir ni prestar el dispositivo criptográfico (tarjeta inteligente) a terceras personas.
e. No utilizar los certificados digitales para ningún propósito, cuando éstos han sido revocados o han expirado.
f. Solicitar la revocación del Certificado Digital ante el cambio de nombre, apellidos o nacionalidad de extranjero a nacional u otra información que haya sido objeto de verificación al momento de la emisión del certificado de firma digital.
g. Acatar los términos de los acuerdos de uso emitidos por cada autoridad de registro, por saber, las entidades que están aprobadas por el MICITT para fungir como Autoridades certificadoras; la lista oficial es actualizada por el Banco Central en su sitio web.
h. Acatar las recomendaciones y políticas técnicas y de seguridad que le señale el correspondiente certificador y emita la Dirección de Tecnologías de la Información y Comunicaciones sobre la materia.
i. Notificar inmediatamente ante órganos certificadores acreditados, en caso de extravío, sustracción o robo del certificado de firma digital u olvido de la clave, a fin de no interrumpir la continuidad de las labores que dependan de aquel. Para cubrir el costo por reposición se debe seguir el procedimiento "TIC-GFD-0001-Procedimiento para el otorgamiento de certificados de firma digital CCSS".
j. Las demás obligaciones que establezca la Ley número 8454, su Reglamento y los acuerdos de suscripción adoptados entre funcionarios y órganos certificadores.

Artículo 12.- De la revocación para los Certificados Digitales. Los Certificados Digitales podrán ser dejados sin efecto, cuando se presenten algunas de las causas siguientes:

- Cuando sea solicitado expresamente por el Suscriptor, por extravío, hurto o robo del certificado digital o se tenga la certeza de que se hayan presentado tales circunstancias.
- Por orden de la Dirección de Certificadores de Firma Digital, de conformidad con las competencias que le asisten conforme con la Ley 8454 y su Reglamento.

Artículo 13 - Eficacia de trámites no habilitados con firma digital certificada. El funcionario que reciba cualquier gestión, reclamo o recurso planteado por usuarios, en trámites administrativos no habilitados con el proceso de Firma Digital Certificada, deberá solicitar en forma inmediata la colaboración del apoyo informático correspondiente por parte del Centro de Gestión Informática (CGI) de la Dirección de sede correspondiente, para la validación de los documentos presentados, a fin de poder definir si están firmados correctamente, y continuar con el trámite normal del proceso.

Capítulo III
De la Organización y distribución de Competencias

Artículo 14.- De la Dirección de Tecnologías de la Información y Comunicaciones.
Corresponderá a la Dirección de Tecnologías de la Información y Comunicaciones:

a. Ejecutar acciones y medidas como unidad rectora, fiscalizadora y evaluadora del tema.
b. Establecer los lineamientos técnicos de administración de la infraestructura y servicios para la Firma Digital y Firma Digital Certificada de los documentos transmitidos y almacenados electrónicamente por parte de los suscriptores.

c. Emitir los lineamientos técnicos y procedimientos internos sobre seguridad lógica y física de documentos electrónicos, respaldo de información, estándares de la infraestructura tecnológica de Certificados Digitales y aquellos propios de su competencia.
d. Establecer y mantener la comunicación y la coordinación necesarias con todas las demás dependencias de la Caja involucradas en el proceso y con los usuarios internos adscritos al servicio de Certificados de Firma digital.
e. Procurar, a través del monitoreo de la operación de los equipos donde reside la información relativa a las Firmas Digitales, el mantenimiento y evaluación de la confiabilidad y calidad de los procedimientos utilizados, la integridad, confidencialidad, seguridad y disponibilidad de los datos.
f. Confeccionar informes de Control Interno de anomalías detectadas, así como las acciones tomadas o por tomar para corregirlas o reducir su daño.

Artículo 15.- De las Gerencias. Corresponderá a cada Gerencia autorizar el cobro a cargo de la Caja Costarricense de Seguro Social por el otorgamiento de certificados digitales, a nombre del número de funcionarios que considere necesario, siempre en seguimiento al Procedimiento para el otorgamiento de Certificados de Firma Digital establecido por la Dirección de Tecnologías de Información y Comunicaciones.

Artículo 16.- De las Jefaturas Corresponderá a las Direcciones de Sede, Direcciones de Servicios de Salud y a las Direcciones de Sucursales, con base en las solicitudes de las jefaturas subordinadas, determinar los proyectos y listas de funcionarios que se presentarán ante los Gerentes para su aprobación en el otorgamiento de los certificados digitales.

Artículo 17.- Archivo electrónico. Todas las dependencias de la Caja manejarán un archivo digital de todos los documentos electrónicos que se envíen y reciban en el cumplimiento de sus funciones, con el objeto de garantizar el libre acceso a la información pública, conforme la Constitución Política lo señala. Dicho archivo se constituirá y administrará conforme los lineamientos emitidos por el Sistema de Archivos Nacionales y aquellos dictados en conjunto por la Gerencia Administrativa y el acompañamiento técnico de la Dirección de Tecnologías de Información y Comunicaciones.

Capítulo IV
Disposiciones Finales

Artículo 18.- Integración normativa. Los aspectos no regulados por este Reglamento se regularán conforme lo dispone la Ley número 8454 y Reglamento y demás normas legales y reglamentarias conexas.

Corresponderá a la Dirección de Tecnologías de Información y Comunicaciones emitir, dentro del plazo de seis meses a partir de la publicación, los lineamientos pertinentes para asegurar la implementación de la presente normativa y mantenerlos actualizados de conformidad con el marco jurídico y operativo nacional vigente.

Artículo 19.- Vigencia. Rige seis meses después de su publicación en el Diario Oficial La Gaceta".

Asimismo, **se acuerda** instruir a la Administración su implementación y divulgación a nivel institucional, una vez publicado en el Diario Oficial La Gaceta.

ACUERDO FIRME".

Atentamente,

(Original firmado)
Emma C. Zúñiga Valverde
Secretaria Junta Directiva