I. DISPOSICIONES GENERALES

De acuerdo a la normativa vigente establecida en la Ley N° 8454 y directrices emanadas del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT), se procede a normar el uso de la Firma Digital Certificada a lo interno de esta Dirección General; al ser esta una herramienta de identificación confiable y segura, ofreciendo una oportunidad fundamental para el incremento de la eficiencia, la eficacia, la transparencia y el acometimiento de los fines estatales.

Este lineamiento tiene como propósito garantizar la integridad y autenticidad de los documentos electrónicos que tendrán la misma validez y eficacia jurídica que la firma manuscrita. Igualmente, el detalle de las características que un documento electrónico firmado digitalmente debe tener para considerarse que cumple con el formato oficial nacional.

En ese sentido, la Ley N° 8454, publicada en la Gaceta No. 197 del 13 de octubre del 2005 establece en el artículo N° 8, que debe entenderse 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*".

Además, el artículo N° 9 indica que "*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*".

La DGSC, considerará como único mecanismo de Firma Digital el establecido en el marco de la Ley N° 8454 "Ley de certificados, firmas digitales y documentos electrónicos" y su Reglamento, definido y administrado por el MICITT, así como lo indicado en la Directriz N°067-MICITT-H-MEIC publicada en el Diario Oficial La Gaceta Nº 79 del 25 abril de 2014, emitida por la Dirección de Certificadores de Firma Digital del MICITT. Por tal motivo, en este contexto, en el uso de la Firma Digital Certificada, no se aceptarán para trámites oficiales, ni se permitirán mecanismos alternos auto gestionados que pudieran clasificarse como firmas electrónicas, incluyendo firmas digitales emitidas por otras empresas nacionales o internacionales, que no sea el reconocido por la Dirección de Certificadores de Firma Digital.

La DGSC, procurará mantener informados a sus funcionarios, sobre los mecanismos de Firma Digital, con el objetivo de 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 técnicamente reconocer, interpretar y validar las firmas digitales asociadas a estos documentos electrónicos, para lo que se les brindará la capacitación correspondiente.

Con miras a la reducción en el uso del papel y la mejora de la eficiencia y eficacia institucional en sus procesos, la Dirección General, dentro de sus posibilidades presupuestarias y operacionales, actualizará sus procesos internos de tal forma, que estén soportados en plataformas digitales que utilicen la capacidad de autenticación y de firma digital certificada de los funcionarios.

Cada funcionario, asumirá la responsabilidad correspondiente en el uso del Certificado de Firma Digital y las certificaciones de documentos electrónicos firmadas digitalmente se harán por medios electrónicos, según legislación nacional, salvo solicitud expresa del interesado que lo requiera en papel.

II. DEFINICIONES Y CONCEPTOS GENERALES

- **Firma Digital:**
  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.

- **Declaración de las Prácticas de Certificación (DPC):**
  Declaración de las prácticas que utiliza el certificador para la emisión de los certificados (define el equipo, las políticas y los procedimientos que el certificador utiliza para satisfacer los requerimientos especificados en las políticas del certificado que son soportados por él).

- **Documento electrónico:**
  Cualquier manifestación con carácter representativo o declarativo, expresado o transmitido, por un medio electrónico o informático.

- **Documento electrónico firmado digitalmente:**
  Aquel documento electrónico, cualesquiera que sea su contenido, contexto y estructura, que tiene lógicamente asociada una Firma Digital.

- **Autoridad Certificadora Emisora:**
  La persona jurídica pública o privada, nacional o extranjera, prestadora del servicio de creación, emisión y operación de certificados digitales.

- **El documento electrónico de archivo:**
  Registro de la información generada, recibida, almacenada y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital; es producida por una persona o entidad en razón de sus actividades y debe ser tratada conforme con los principios y procesos archivísticos.

- **Dirección de Certificadores de Firma Digital (DCFD):**
  La Dirección de Certificadores de Firma Digital es el ente encargado de administrar y supervisar el sistema de certificación, adscrita al Ministerio de Ciencia y Tecnología.

- **PIN de Activación**:
  Son requeridos para operar los módulos criptográficos y que necesitan ser protegidos, los cuales pueden ser una palabra de paso, una frase clave o información biométrica (huella digital); para el caso de la Certificado Digital, consiste en una clave numérica.

- **Firma Digital Certificada:**
  Una Firma Digital que haya sido emitida al amparo de un Certificado Digital válido y vigente, expedido por un Certificador registrado ante la DCFD.

- **Mecanismo en Línea para Verificar el Estado del Certificado (OCSP):**
  Mecanismo mediante el cual se permite a las partes que confían consultar y obtener la información del estado de un Certificado sin requerir para ello el uso de una Lista de Revocación de Certificados (CRL).

- **La gestión de los documentos electrónicos con Firma Digital Certificada:**
  Es la gestión propia de los mismos y estará regulada por los mecanismos de Firma Digital certificada y deberán implementarse bajo la normativa interna de la DGSC, la Dirección General del Archivo Nacional y las regulaciones vigentes del MICITT, garantizando así la validez de las firmas digitales en el tiempo, potenciando la interoperabilidad en el intercambio de documentos electrónicos entre las Áreas e Instituciones, la apropiada conservación de los documentos electrónicos firmados digitalmente, y el valor legal de los medios electrónicos a través del tiempo.

- **Uso indebido**:

El uso indebido se considera como aquellas prácticas que se opongan a la normativa interna de la institución, a la legislación, políticas y reglamentación nacional vigente, según lo establecen los artículos del 26 al 32, de la Ley N° 8454 “Ley de Certificaciones, Firmas Digitales y Documentos Electrónicos”, del Ministerio de Ciencia, Tecnología y Telecomunicaciones.

III. CERTIFICADO DE FIRMA DIGITAL

- **Asignación del Certificado de Firma Digital:**
  Los elementos: Dispositivo y Certificado de Firma Digital serán autorizados por la jefatura correspondiente, a cada funcionario que requiera esta herramienta para ejercicio de sus funciones, de acuerdo con el marco de responsabilidades y sistemas institucionales establecidos.

- **Trámite y entrega del Certificado de Firma Digital:**
  El funcionario, realizará las diligencias necesarias para contar con la Firma Digital Certificada, previa autorización de su Jefatura.

- **Instalación del Certificado de Firma Digital**
  La jefatura inmediata, solicitará la instalación del Certificado de Firma Digital a la Unidad de Tecnologías de Información (TI).

- **Vigencia del Certificado de Firma**
  La vigencia del Certificado de Firma Digital, según establece la política de certificados emitida por la Dirección de Certificadores de Firma Digital del MICITT (a la fecha de este documento, la vigencia es de 4 años).

IV. USO DE FIRMA DIGITAL

Todo documento, mensaje o archivo digital asociado a una o varias firmas digitales, salvo prueba en contrario, será de la autoría y responsabilidad del o los firmantes.

La Firma Digital, 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 uso indebido de la Firma Digital asignada por la DGSC a un funcionario que incurra en incumplimiento en el ámbito de sus funciones y deberes, facultará a la jefatura a comunicar al funcionario subalterno, la cancelación del uso de la misma en actividades propias de sus funciones, sin perjuicio de la responsabilidad disciplinaria, civil y penal correspondiente. Lo anterior, de acuerdo con los artículos N°8, N°14 y N°29 de la Ley N°33018-MICIT y su Reforma N°34890-MICIT.

- **Derechos del personal de la DGSC que utilicen la Firma Digital.**

-Recibir un Certificado de Firma Digital para la ejecución de las actividades asignadas por la jefatura, cuando las actividades así lo ameriten, el costo, por primera vez, estará cubierto por el presupuesto de la DGSC, acorde con las disponibilidades presupuestarias. En caso de extravío, olvido de la clave o renovación, el costo deberá ser cubierto por el funcionario.

-Recibir el apoyo, la gestión y el mantenimiento por parte de la Unidad de Tecnologías de Información para un correcto funcionamiento del dispositivo y del Certificado de Firma Digital en la computadora que la DGSC le haya asignado o autorizado.

-Obtener el permiso de la jefatura, para realizar los trámites propios de obtención y renovación del certificado dentro de la jornada laboral.

- **Obligaciones del personal que utiliza el Certificado de Firma Digital en la gestión interna de la DGSC.**

-Asegurar el debido uso del Certificado de Firma Digital conforme al presente lineamiento, normativa interna de la Institución, legislación, políticas y reglamentación nacional vigente, incluyendo el acuerdo suscriptor con la Autoridad Certificadora Emisora.

-Vigilar por la veracidad y confiabilidad de la información que firma digitalmente.

-Suministrar a la Autoridad Certificadora la información veraz, completa y actualizada que éstos requieran para la prestación de sus servicios.

-Resguardar estrictamente la confidencialidad del PIN de activación del Certificado de Firma Digital, e informar inmediatamente a la Autoridad Certificadora en caso de que dicha confidencialidad se vea o se sospeche que haya sido comprometida.

-Acatar las recomendaciones técnicas y de seguridad que le señale la Autoridad Certificadora o la DGSC.

-En el contexto de la gestión interna de la DGSC, utilizar el Certificado de Firma Digital únicamente para los trámites autorizados por la jefatura o los que se haya definido de obligatoriedad dentro de la gestión documental de la DGSC.

-Utilizar el Certificado de Firma Digital única y exclusivamente en forma personal, no se podrá transferir ni poner a disposición de un tercero.

-Reportar de inmediato a la Autoridad Certificadora en caso de pérdida, sustracción, robo o deterioro, entre otros del Certificado Digital, para que se proceda a renovar y emitir un nuevo Certificado, el funcionario asumirá los costos correspondientes.

-Asumir por cuenta propia la reposición en caso de pérdida, sustracción, robo, deterioro u olvido, del dispositivo lector o el medio que se almacene del Certificado de Firma Digital o el Pin.

V. RESPONSABLES

a. Director General

- Brindar el apoyo necesario, para el uso e implementación de la Firma Digital.
- Aprobar el presente Lineamiento.
- Mantener actualizado el presente Lineamiento.

b. Directores y Jefaturas:

- Gestionar y mantener un registro actualizado de los trabajadores y trabajadoras, bajo su coordinación, que estén autorizados para firmar digitalmente dentro del ámbito de sus funciones, así como aquellos a quienes se les ha revocado el Certificado.

- Orientar y apoyar al trabajador y trabajadora en el adecuado uso de la firma digital en el ámbito de sus funciones, deberes y obligaciones.

- Seguir todas las normas, instructivos y manuales que se realicen para la firma y gestión de los documentos que se generan en sus distintas unidades y velar por la adecuada capacitación de cada colaborador en estos temas.

c. Unidad de Tecnologías de Información:

a. Establecer los estándares y velar por el cumplimiento de los mismos, en torno a la utilización de la Firma Digital en el uso de las aplicaciones de terceros que la Dirección General Servicio Civil actualmente usa.

b. Proporcionar y mantener la Infraestructura de Tecnologías de Información de la Dirección General Servicio Civil, relacionada con la implementación y la utilización de Firma Digital en la Institución.

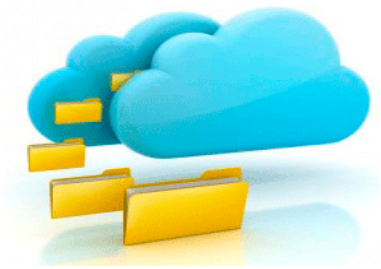
c. Asistir y apoyar en la instalación del Certificado de Firma Digital a los funcionarios de las respectivas dependencias de la DGSC.

d. Configurar los equipos de los funcionarios para que estos cumplan con la política de formatos oficiales emitida por la DCFD del MICITT, y así garantizar la validez a largo plazo de los documentos electrónicos firmados.

e. Brindar asesoría y soporte tecnológico en cuanto a la implementación y uso de Firma Digital en la Dirección General Servicio Civil, así como en los estándares y formatos definidos. Todo lo anterior, con base en las directrices, normativa interna aplicable y regulaciones emitidas por el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT.

f. Uniformar programas y sistemas informáticos en el proceso de gestión documental, con el fin de asegurar la compatibilidad de la información en las unidades administrativas.

g. Hacer investigaciones periódicas en el mercado sobre el avance de la tecnología, solicitar la adquisición de nuevos equipos de almacenamiento de información, y migrar los documentos producidos por medios automáticos a nuevos soportes, antes de que los actuales sean obsoletos y se corra riesgo de pérdida de información.



h. Tener el personal debidamente capacitado para efectuar la migración de los documentos producidos por medios automáticos a nuevos soportes, cuando su acceso se vea comprometido por la obsolescencia de los soportes en que se encuentren.

i. Se debe contar con los procedimientos para garantizar el funcionamiento permanente de los programas computacionales y del equipo de cómputo, para poder acceder a la información en el momento que se requiera por parte de los usuarios, asegurando así el mantenimiento adecuado.

j. Establecer en coordinación con los archivistas institucionales, una política institucional para la generación de respaldos periódicos de información que garantice la permanencia, la integridad, la autenticidad y la accesibilidad de la información en los documentos.

d. Seguridad del Sistema automatizado

- Establecer los mecanismos de seguridad para la transmisión y recepción de información con el fin de garantizar su privacidad, confidencialidad y autenticidad.

- Respecto a las condiciones en el uso del sistema, todos los usuarios deberán contar previamente con el certificado de Firma Digital, emitido por alguna Autoridad Certificadora Emisora autorizada y registrada ante la DCFD.

- Cada funcionario autorizado, deberá contar con una computadora con conexión a internet para el uso del sistema automatizado, con una plataforma web, compatible con los sistemas operativos y navegadores.

- A través del sistema, se deberá enviar notificación de los documentos enviados y recibidos en forma automática vía correo electrónico con su respectiva fecha y hora de recepción, misma que se conservará.

- La seguridad del sistema, deberá cubrir el área de autenticación de usuarios, autorización y control de acceso a usuarios, protección de la información y pistas de auditoría

- El sistema, deberá llevar registros confiables, la identificación del emisor, fecha y hora del envío y recibido.

- En el sistema, se conservarán los documentos enviados y recibidos con las debidas constancias en sus bitácoras de todos los mensajes y transacciones generadas, permitiendo el acceso e impresión de las mismas cuando sea necesario.

- El sistema contará con tres ambientes en cuanto a la producción, pruebas y respaldos que permitirán la continuidad, control y seguridad de la información que se gestione mediante los mismos.

- Los funcionarios de TI, velarán por el buen funcionamiento y mantenimiento de los servidores físicos y virtuales que albergan los documentos.

- Se deberá monitorear el rendimiento del sistema, actualización de programas y equipos, antivirus, mantenimiento de cuentas, seguridad informática y redes en el acceso local y remoto donde se pueda identificar problemas que puedan generar interrupciones en el funcionamiento del sistema.

- El ambiente de respaldos se actualizará diariamente con la información del ambiente de producción del sistema, donde se puedan detectar eventuales problemas del sistema.

- Se debe tener confidencialidad y probidad sin perjuicio a las medidas de seguridad implementadas en el sistema, donde todos los usuarios estarán obligados a conocerlas y guardarlas en todo el proceso, en acato a la legislación y normativa vigentes.

Área Administración de Servicios Institucionales:

- Establecer en coordinación con otras áreas de la Dirección General de Servicio Civil, en el marco de sus competencias y responsabilidades, los mecanismos, la normativa y los formatos de preservación documental a largo plazo, procesos de preservación entre formatos y herramientas para su gestión.

- Establecer y divulgar en conjunto con la Unidad de Tecnologías de Información, los estándares (informáticos o manuales) específicos para la gestión de los documentos cualquiera que sea su formato y según lo definido en las directrices y regulaciones emitidas por la Dirección General de Archivo Nacional y el Ministerio de Ciencia, Tecnología y Telecomunicaciones, MICITT.

- Asesorar a las dependencias de la DGSC, en la implementación de una adecuada gestión documental de los documentos firmados digitalmente, así como su preservación.

- Llevar el control de los funcionarios que han sido autorizados por la jefatura en el uso de la Firma Digital.

- Previa disponibilidad presupuestaria, realizar el trámite correspondiente para la adquisición de nuevos Certificados de Firma Digital cuando así lo amerite.

Gestión documental

- La gestión documental de electrónicos con Firma Digital Certificada, estará regulada según lo dispuesto en el Manual para el Funcionamiento del Proceso Archivístico Institucional, así como las políticas y los procedimientos institucionales para la creación, organización, utilización y conservación de los documentos en cualquier soporte, que este genere. Las mismas deben ser de acatamiento obligatorio para todos los miembros de la organización.

Procedimiento archivístico digital institucional

- De acuerdo con el Decreto No. 40554-C del Reglamento a la Ley del Sistema Nacional de Archivos N° 7202, artículo 87: "Medidas de Preservación de Documentos en Soporte Electrónico. Los archivos del Sistema, deben establecer los mecanismos y procedimientos necesarios para asegurar la autenticidad, integridad, inalterabilidad y disponibilidad de los documentos electrónicos de archivos…"

- Los procedimientos archivísticos, tienen como objetivo administrar el ciclo de vida de los documentos electrónicos que se gestionan dentro de las diferentes Áreas de la DGSC, en busca de la eficacia y eficiencia en este campo.

- Los documentos institucionales, reflejan las actividades, tareas o funciones de la Dirección General, y tienen como misión, informar sobre el desarrollo de una actividad donde se evidencian sus actividades propias. Así la información se fija en un soporte sin importar si es papel o electrónico.

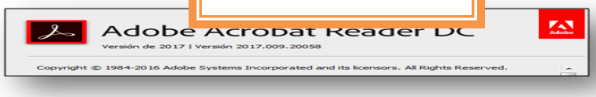
- Actualmente, para la Dirección General de Servicio Civil, es importante normalizar la producción de documentos electrónicos en las diferentes áreas administrativas y técnicas, con el fin de mejorar la gestión y transparencia administrativa, y que se consoliden los procedimientos en la elaboración de los mismos. Es así, como se debe contar con una plataforma digital que tenga la capacidad de implementar mecanismos de autenticación, y firmado de documentos y trámites electrónicos utilizando la firma digital de los funcionarios.

- Los documentos electrónicos oficiales de la DGSC, deberán ser formatos PDF, y firmados por medio de la herramienta ofimática, de descarga gratuita, Adobe Acrobat

Reader DC en su última versión, compatible con el equipo que utiliza el funcionario, donde se seguirán los pasos según anexo del "Manual de Firma Digital"

Versión 2012

Versión 2017



- Cada Área de la DGSC, deberá utilizar el mismo sistema para cumplir con la normalización, control y mantenimiento de los documentos, el cual contará con los siguientes instrumentos:

  - Un sistema integrado de código de referencia único documental acorde con la reorganización institucional de las Áreas y Unidades.

  - Sistema integrado de conservación y eliminación documental, como las tablas de plazos, entre otros que se requieran.

  - Un sistema integrado de gestión, que permita identificar la trazabilidad de los documentos en forma única y eficiente dentro de la DGSC.

  - Un Manual de usuario y procedimientos, para la gestión documental, el cual contará con los diferentes perfiles:

    - **Administrador**: Quien tiene el control total sobre el sitio en cuanto a la configuración y contenidos.
    - **Colaborador**: Quien podrá crear nuevo contenido y modificar el existente.
    - **Contribuidor**: Quien podrá crear contenido y modificar siempre que sea de su propiedad
    - **Consumidor (usuario)**: Quién podrá visualizar y descargar copia del contenido pero no puede modificarlo.

- **Operacionalización del proceso:**

  - Dentro de la operacionalidad del proceso se deberán tomar en cuenta los siguientes aspectos:

    - Estructura
    - Acceso
    - Consultas
    - Ingreso de Documentos
    - Documentos institucionales
    - Conservación
    - Seguridad del sistema

Los archivos de gestión digitales de cada Área y/o Unidad que están en las carpetas compartidas, harán sus respectivos respaldos, así como el Archivo Central y la Unidad de Tecnología de Información respaldarán también lo contenido en dichas carpetas. La Institución, se encargará de dotar de los recursos necesarios para el almacenamiento, custodia y recuperación de la información.

Esta estructura permitirá recibir, gestionar y conservar los documentos de archivo de acuerdo con las funciones de cada una, y en razón de lo establecido en la Ley N° 7202, Ley del Sistema Nacional de Archivos y su Reglamento, y se dispondrá dentro de la plataforma Institucional.

El acceso a los documentos electrónicos, se realizará por medio del sistema establecido, y queda garantizada de acuerdo con las normas y principios del acceso a la documentación de la Administración Pública, y a las restricciones establecidas por ley, principalmente en cuanto a la protección de datos de carácter personal e información susceptible.

La consulta de documentos y expedientes se llevará a cabo por medio del sistema establecido.

La transferencia de los documentos de archivo de gestión de cada área o unidad, se llevará a cabo diariamente al sistema establecido de carpetas compartidas, garantizándose la disponibilidad e integridad de los mismos.

Los documentos de los archivos de gestión transferidos serán los siguientes:

- Resoluciones
- Informes técnicos
- Dictámenes
- Oficios
- Circulares
- Criterios jurídicos
- Certificaciones
- Correos electrónicos
- Convenios
- Publicaciones oficiales en La Gaceta

La conservación de los documentos que administre el sistema, siguen lo establecido en el Decreto N°40555-C del 29 de junio de 2017 -Reglamento de Organización y Servicios del Archivo Nacional-; así como de instrumentos de vigencia legal, como por ejemplo: las Tablas de Plazos Documental aprobadas; normativa interna como el Oficio Circular N° SD-OC-008-2017 de fecha 22 de junio de 2017, sobre la transparencia y acceso a la información pública (Decreto Ejecutivo N°40200-MP-MEIC-MC, publicado en el Alcance N°122 - La Gaceta N° 104 del 02 junio 2017).

Los documentos externos que ingresen a las diferentes Áreas, en soporte papel y que sean digitalizados, deberán incluirse dentro del sistema establecido, y se conservará el original en soporte papel, teniendo claro que la copia digitalizada no cuenta con el valor legal, según la legislación vigente en esta materia.

Los documentos producidos y conservados digitales que cumplan con la Ley N° 7202 del Sistema Nacional de Archivo, y la Ley N° 8454 de Certificados y Documentos Electrónicos, serán gestionados como originales, y se conservarán en el sistema establecido, y no deben ser impresos, ya que la versión impresa carece de valor legal según la legislación vigente.

- **Funcionarios (Profesionales, secretarias, técnicos) que utilizan Firma Digital:**

  - Los funcionarios son responsables del documento electrónico que contiene una Firma Digital Certificada.

  - Cumplir con las formalidades de autenticación, certificación o registro, que desde el punto de vista jurídico exija la ley ante un acto determinado.

  - Utilizar la Firma Digital Certificada de forma adecuada acorde con el ámbito de sus funciones.

  - Gestionar con diligencia el acceso para contar con los dispositivos, sistemas y credenciales para la Firma Digital.

  - Mantener en vigencia su certificado de Firma Digital para el oportuno cumplimiento de sus deberes.

  - Custodiar y establecer medidas de seguridad para resguardar su Certificado Digital.

VI. ASPECTOS TÉCNICOS

- En todo momento, los mecanismos de Firma Digital Certificada, deberán implementarse respetando la normativa nacional vigente respectiva, garantizando así la validez de las firmas digitales en el tiempo, potencializando la posibilidad del intercambio de documentos electrónicos entre instituciones, la apropiada conservación de los documentos electrónicos firmados digitalmente, y el valor legal de los medios electrónicos a través del tiempo.

- La DGSC, deberá dentro de sus posibilidades técnicas y presupuestarias, modernizar y ajustar los sistemas de información que tenga en operación, para incorporar mecanismos de autenticación mediante Firma Digital Certificada, así como mecanismos de firma de documentos.

- Todo nuevo desarrollo, funcionalidad o implementación de sistemas de información de la DGSC, deberá incorporar:

  - Mecanismos de autenticación mediante Firma Digital Certificada, es decir, cuando un funcionario se autentique utilizando Firma Digital Certificada, se reconocerá la autenticidad plena y el valor de su relación con la institución por el canal electrónico.

- Mecanismos de firma de documentos y transacciones electrónicas mediante Firma Digital Certificada cuando el trámite así lo requiera dentro de sus posibilidades técnicas y presupuestarias.

VII. ASPECTOS SEGURIDAD DE INFORMACIÓN

- Se deberá respetar las disposiciones para la seguridad física y lógica de la información del "*Documento Integral de Seguridad de la Información de la DGSC*", emitido en octubre del 2016, por parte de la Unidad de Tecnologías de Información:

  - Sobre los recursos: **B) Riesgos**: "con la finalidad de mitigar el impacto que pueda tener la materialización de los riesgos, no solo en software, hardware e infraestructura, sino también el recurso humano con que cuenta la DGSC, la Unidad de TI deberá elaborar un plan de riesgos y un seguimiento mensual e informar a las autoridades.

  - Seguridad física: **C)** "El Acceso a las computadoras personales será responsabilidad de cada funcionario".

  - Seguridad lógica: **A) punto 8**: "*Es obligación absoluta del usuario de la cuenta del dominio proteger la contraseña y asegurarse del* ***ser único*** *que conozca dicha información*"

B) Sobre la seguridad de la Información: "Todos los funcionarios de la DGSC, están en la obligación irrenunciable de proteger la información utilizada, transmitida y/o contenida en la infraestructura tecnológica de la DGSC".

C) Acceso a los equipos, punto 12: "Los usuarios deben respaldar de manera periódica la información sensible que se encuentre en sus computadoras personales"

H) Sobre el uso del correo institucional, punto 3: "Revisar el correo electrónico es de carácter obligatorio y se considera un medio oficial de comunicación institucional"

Punto 11: "Es obligación cada usuario del servicio institucional del correo, el resguardar su información".