Ministerio Secretaría General de la Presidencia

APRUEBA NORMA TECNICA PARA LOS ORGANOS DE LA ADMINISTRACION DEL ESTADO SOBRE SEGURIDAD Y CONFIDENCIALIDAD DE LOS DOCUMENTOS ELECTRONICOS

Núm 83.- Santiago, 3 de junio de 2004.- Vistos: Lo dispuesto en el artículo 32° N° 8 de la Constitución Política de la República; el artículo 3° letra a) del DFL N° 7.912, de 1927; la ley N° 19.799, sobre documentos electrónicos, firma electrónica y la certificación de dicha firma; el decreto supremo N° 181, de 2002, del Ministerio de Economía, Fomento y Reconstrucción; y lo dispuesto en la resolución N° 520, de 1996, que fija el texto refundido, coordinado y sistematizado de la resolución N° 55, de 1992, ambas de la Contraloría General de la República.

Considerando:

1.- Que, el artículo 47 del DS. N° 181 de 2002, del Ministerio de Economía, Fomento y Reconstrucción, Reglamento de la ley N° 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, en adelante el Reglamento, creó el Comité de Normas para el Documento Electrónico.

2.- Que, el Comité, en su agenda de trabajo fijada en sesión de fecha 8 de enero de 2003, estableció la determinación de una norma técnica para la seguridad y confidencialidad del documento electrónico y los repositorios en que se almacenan, como una de sus tareas inmediatas.

3.- Que, para el desarrollo de la referida tarea, la Secretaría Técnica del Comité creó un grupo de trabajo sobre seguridad y confidencialidad del documento electrónico, en el que participaron representantes de los miembros del Comité de Normas para el Documento Electrónico, del Ministerio del Interior, de la Contraloría General de la República, del Instituto Nacional de Normalización, del Servicio de Impuestos Internos, del Servicio Nacional de Aduanas, de la Armada de Chile, del Banco Central de Chile, del Banco Estado, de Microsoft, de Orion 2000, de Neosecure, de Sinacofi, y de American Telecommunication, y que fue asesorado técnicamente por la Universidad de Chile a través de CLCERT.

4.- Que el trabajo se realizó de conformidad con la política gubernamental orientada a la incorporación de las Tecnologías de la Información y Comunicaciones en los órganos de la Administración del Estado, para mejorar los servicios e información ofrecidos a los ciudadanos y la eficiencia y la eficacia de la gestión pública, e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos.

Decreto:

Artículo primero.- Apruébase la siguiente norma técnica sobre seguridad y confidencialidad del documento electrónico para los órganos de la Administración del Estado.

"NORMA TECNICA SOBRE SEGURIDAD Y CONFIDENCIALIDAD DEL DOCUMENTO ELECTRONICO"

TITULO I

Ambito de aplicación

Artículo 1°.- La presente norma técnica establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los órganos de la Administración del Estado, y las demás cuya aplicación se recomienda para los mismos fines.

Las exigencias y recomendaciones previstas en esta norma, tienen por finalidad garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; facilitar la relación electrónica entre los órganos de la Administración del Estado y entre éstos y la ciudadanía y el sector privado en general; y salvaguardar el uso del documento electrónico de manera segura, confiable y en pleno respeto a la normativa vigente sobre confidencialidad de la información intercambiada.

Artículo 2°.- Las disposiciones de la presente norma técnica se aplicarán a los documentos electrónicos que se generen, intercambien, transporten y almacenen en o entre los diferentes organismos de la Administración del Estado y en las relaciones de éstos con los particulares, cuando éstas tengan lugar utilizando técnicas y medios electrónicos.

Artículo 3°.- Para los efectos de esta norma, los documentos electrónicos constituyen un activo para la entidad que los genera y obtiene. La información que contienen es resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella.

Artículo 4°.- Esta norma se cumplirá en dos etapas, de conformidad con los siguientes niveles:

Nivel 1. Nivel básico de seguridad para el documento electrónico.

Nivel 2. Nivel avanzado de seguridad para el documento electrónico.

TITULO II

Definiciones

Artículo 5°.- Para los propósitos de esta norma, se entenderá por:

a) Autenticación: proceso de confirmación de la identidad del usuario que generó un documento electrónico y/o que utiliza un sistema informático.
b) Confidencialidad: aseguramiento de que el documento electrónico sea conocido sólo por quienes están autorizados para ello.
c) Contenido del documento electrónico: información, ideas y conceptos que un documento expresa.
d) Continuidad del negocio: continuidad de las operaciones de la institución.
e) Disponibilidad: aseguramiento de que los usuarios autorizados tengan acceso oportuno al documento electrónico y sus métodos de procesamiento.
f) Documento electrónico: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.
g) Documentos públicos: aquellos documentos que no son ni reservados ni secretos y cuyo conocimiento no está circunscrito.
h) Documentos reservados: aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter.
i) Documentos secretos: los documentos que tienen tal carácter de conformidad al artículo 13 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado y su Reglamento.
j) Ejecutivo: autoridad dentro de la institución.
k) Identificador formal de autenticación: mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos.
l) Incidentes de seguridad: situación adversa que amenaza o pone en riesgo un sistema informático.
m) Información: contenido de un documento electrónico.
n) Integridad: salvaguardia de la exactitud y totalidad de la información y de los métodos de procesamiento del documento electrónico, así como de las modificaciones realizadas por entes debidamente autorizados.
o) Negocio: función o servicio prestado por la organización.
p) Política de seguridad: conjunto de normas o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto.
q) Repositorio: estructura electrónica donde se almacenan documentos electrónicos.
r) Riesgos: amenazas de impactar y vulnerar la seguridad del documento electrónico y su posibilidad de ocurrencia.

s) Sistema informático: conjunto de uno o más computadores, software asociado, periféricos, terminales, usuarios, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.
t) Usuario: entidad o individuo que utiliza un sistema informático.

TITULO III

De la seguridad del documento electrónico en general

Artículo 6°.- La seguridad del documento electrónico se logra garantizando los siguientes atributos esenciales del documento:

a) Confidencialidad;
b) Integridad;
c) Factibilidad de autenticación, y
d) Disponibilidad.

Artículo 7°.- Los atributos esenciales que aportan seguridad al documento electrónico se obtienen y sostienen mediante la ejecución permanente de las siguientes acciones:

a) Desarrollar y documentar políticas de seguridad de uso, almacenamiento, acceso y distribución del documento electrónico y de los sistemas informáticos utilizados en su procesamiento;
b) Diseñar y documentar los procesos y procedimientos para poner en práctica las políticas de seguridad;
c) Implementar los procesos y procedimientos señalados precedentemente;
d) Monitorear el cumplimiento de los procedimientos establecidos y revisarlos de manera de evitar incidentes de seguridad;
e) Concientizar, capacitar y educar a los usuarios para operar los sistemas informáticos de acuerdo a las exigencias establecidas;
f) Definir y documentar los roles y responsabilidad de las entidades e individuos involucrados en cada una de las letras anteriores.

Artículo 8°.- Los órganos de la Administración regidos por esta norma deberán aplicar sus disposiciones para garantizar los atributos esenciales que confieren seguridad al documento electrónico, definidos en el artículo 6.

No obstante, la consecución y mantención de tales atributos por parte de cada órgano de la Administración del Estado estarán sujetas a la consideración de factores de riesgo y factores de costo/beneficio. Estos últimos podrán invocarse mediante una resolución fundada del jefe de servicio correspondiente, basada en un estudio de análisis de riesgo y/o costo/beneficio.

TITULO IV

Del nivel básico de seguridad del documento electrónico

Párrafo 1°

Normas generales

Artículo 9°.- Durante la primera etapa de aplicación de esta norma, los órganos de la Administración del Estado desarrollarán las políticas, procedimientos, acciones y medidas tendientes a obtención del Nivel Básico de Seguridad de los documentos electrónicos que se establecen en este Título.

Artículo 10°.- El Nivel Básico de Seguridad para el documento electrónico tiene por objeto:

a) Garantizar condiciones mínimas de seguridad y confidencialidad en los documentos electrónicos que se generan, envían, reciben, procesan y almacenan entre los órganos de la Administración del Estado;
b) Facilitar la adopción de requerimientos de seguridad más estrictos por parte de aquellos organismos y en aquellos tópicos que se estimen necesarios, y
c) Facilitar el Nivel avanzado de seguridad para el documento electrónico, en aquellos organismos cuyo desarrollo institucional lo requiera.

Párrafo 2°

Política de seguridad

Artículo 11.- Deberá establecerse una política que fije las directrices generales que orienten la materia de seguridad dentro de cada institución, que refleje claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional.

La política de seguridad deberá incluir, como mínimo, lo siguiente:

a) Una definición de seguridad del documento electrónico, sus objetivos globales, alcance e importancia.
b) La difusión de sus contenidos al interior de la organización.
c) Su reevaluación en forma periódica, a lo menos cada 3 años.

Las políticas de seguridad deberán documentarse y explicitar la periodicidad con que su cumplimiento será revisado.

Párrafo 3°

Seguridad organizacional

Artículo 12.- En cada organismo regido por esta norma deberá existir un encargado de seguridad, que actuará como asesor del Jefe de Servicio correspondiente en las materias relativas a seguridad de los documentos electrónicos.

Las funciones específicas que desempeñe internamente el encargado de seguridad serán establecidas en la resolución que lo designe. En todo caso, deberá tener, a lo menos, las siguientes funciones:

a) Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de su organización y el control de su implementación, y velar por su correcta aplicación.
b) Coordinar la respuesta a incidentes computacionales.
c) Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.

Párrafo 4°

Clasificación, control y etiquetado de bienes

Artículo 13.- Los documentos electrónicos y sistemas informáticos deberán clasificarse y etiquetarse para indicar la necesidad, prioridad y grado de protección.

La clasificación de un sistema informático debe corresponder a la clasificación más estricta aplicable al documento electrónico que almacene o procese, de conformidad con el decreto supremo 26 de 2001, del Ministerio Secretaría General de la Presidencia.

A cada sistema informático, deberá asignársele un responsable quien velará por su debida clasificación y etiquetado.

Artículo 14.- Todo documento electrónico deberá ser asignado, explícita o implícitamente, a un responsable. En este último caso, el encargado de seguridad deberá proponer quién será responsable por omisión, sea asignando tal responsabilidad al usuario que lo crea, sea atribuyéndosela al responsable por el sistema informático que lo generó, u otra modalidad.

Artículo 15.- Para cada clasificación, el encargado de seguridad deberá proponer los procedimientos de manipulación requeridos para cubrir las siguientes actividades de procesamiento de un documento electrónico:

a) Copiado;
b) Almacenamiento;
c) Transmisión por correo electrónico y sistemas protocolarizados de transmisión de dátos digitales;
d) Destrucción.

Artículo 16.- La salida desde un sistema de un documento electrónico que está clasificado como reservado o secreto, deberá tener una etiqueta apropiada de clasificación en la salida.

Para estos efectos, deberá considerarse, entre otros, los informes impresos, pantallas de computador, medios magnéticos (cintas, discos, CDs, cassettes), mensajes electrónicos y transferencia de archivos.

Párrafo 5°

Seguridad física y del ambiente

Artículo 17.- Los equipos deberán protegerse físicamente de las amenazas de riesgos del ambiente externo, pérdida o daño, incluyendo las instalaciones de apoyo tales como el suministro eléctrico y la infraestructura de cables.

En particular, la ubicación del equipamiento de la institución deberá minimizar el acceso innecesario a las áreas de trabajo y disminuir las posibilidades de amenazas de humo y fuego, humedad y agua, inestabilidad en el suministro eléctrico, hurto y robo.

Artículo 18.- Para los efectos del artículo anterior, cada órgano deberá impartir y publicitar instrucciones relativas a los siguientes aspectos del ambiente externo:

a) Consumo de alimentos, bebidas y tabaco en las cercanías de sistemas informáticos.
b) Condiciones climatológicas y ambientales que pueden afectar sistemas informáticos o entornos cercanos.
c) Promoción de una práctica de escritorio limpio.

Artículo 19.- Respecto de los documentos electrónicos de la organización clasificados como reservados o secretos, se aplicarán las siguientes normas de seguridad ambiental:

a) Deberán almacenarse en áreas seguras, protegidos por un perímetro de seguridad definido, con barreras apropiadas de resguardo y controles de entrada. Estos deberán estar físicamente protegidos del acceso no autorizado, daño e interferencia. La protección provista deberá guardar relación con los riesgos identificados.
b) Deberán disponerse de manera que se minimicen las posibilidades de percances y descuidos durante su empleo.

Párrafo 6°

Seguridad del personal

Artículo 20.- El Jefe de Servicio deberá impartir instrucciones para la seguridad de los documentos electrónicos y los sistemas informáticos, respecto de las siguientes materias:

a) Uso de sistemas informáticos, con énfasis en prohibición de instalación de software no autorizado, documentos y archivos guardados en el computador.
b) Uso de la red interna, uso de Internet, uso del correo electrónico, acceso a servicios públicos, recursos compartidos, servicios de mensajería y comunicación remota, y otros.
c) Generación, transmisión, recepción, procesamiento y almacenamiento de documentos electrónicos.
d) Procedimientos para reportar incidentes de seguridad.

Artículo 21.- Las responsabilidades de seguridad aplicables al personal deberán ser explicitadas en la etapa de selección e incluirse expresamente en los decretos o resoluciones de nombramiento o en las contrataciones respectivas.

Párrafo 7°

Gestión de las operaciones y las comunicaciones

Artículo 22.- En todos los organismos sujetos a la presente norma, deberán explicitarse y difundirse los siguientes antecedentes e información:

a) Los contactos de apoyo ante dificultades técnicas u operacionales inesperadas de sistemas informáticos;
b) Las exigencias relativas al cumplimiento con las licencias de software y la prohibición del uso de software no autorizado;
c) Las buenas prácticas para protegerse de los riesgos asociados a la obtención de archivos y software a través de las redes de telecomunicaciones, o por otros medios, indicando qué medidas de protección se deberán aplicar.

Artículo 23.- Para los efectos de reducir el riesgo de negligencia o mal uso deliberado de los sistemas, deberán aplicarse políticas de segregación de funciones. Asimismo, deberán documentarse los procedimientos de operación de sistemas informáticos e incorporarse mecanismos periódicos de auditorías de la integridad de los registros de datos almacenados en documentos electrónicos.

Artículo 24.- En los órganos regidos por la presente norma, deberán realizarse copias de respaldo de la información y las aplicaciones críticas para la misión de la institución en forma periódica, en conformidad con las siguientes reglas:

a) La periodicidad con que se realizarán los respaldos de los computadores personales de la institución que estén asignados a usuarios, deberá explicitarse y no podrá ser menor a 1 respaldo anual;
b) La periodicidad con que se realizarán los respaldos de los sistemas informáticos y los equipos no contemplados en el punto anterior, utilizados en el procesamiento o almacenamiento de documentos electrónicos, deberá explicitarse y no podrá ser menor a 1 respaldo mensual;
c) Deberá garantizarse la disponibilidad de infraestructura adecuada de respaldo, para asegurar que éstos estén disponibles incluso después de un desastre o la falla de un dispositivo. Las configuraciones de respaldo para los sistemas individuales deberán ser probadas con regularidad, a lo menos cada 2 años, para asegurar que ellas satisfacen los requisitos estipulados en los planes de continuidad institucionales;
d) Deberá almacenarse en una ubicación remota, un nivel mínimo de información de respaldo, junto con registros exactos y completos de las copias de respaldo y los procedimientos documentados de restablecimiento. Esta instalación deberá estar emplazada a una distancia tal que escape de cualquier daño producto de un desastre en el sitio principal. En ámbitos críticos para la institución, se deberán almacenar al menos tres generaciones o ciclos de información de respaldo;
e) Los respaldos deberán cumplir con un nivel apropiado de protección física de los medios, consistente con las prácticas aplicadas en el sitio principal. Los controles asociados a los dispositivos del sitio de producción deberán extenderse para abarcar el sitio de respaldo.
f) Deberán consignarse plazos de retención de los respaldos de la institución, así como cualquier necesidad de realización de respaldos que estén permanentemente guardados, y
g) Deberán utilizarse medios y condiciones físicas de almacenamiento que garanticen una vida útil concordante con los plazos definidos en el punto precedente.

Artículo 25.- Las instituciones regidas por la presente norma deberán impartir instrucciones respecto al uso seguro del correo electrónico. Esas instrucciones deberán incluir al menos:

a) Una advertencia sobre la vulnerabilidad del correo electrónico a modificaciones o accesos no autorizados;
b) Una advertencia sobre los peligros asociados a la apertura de archivos adjuntos y/o a la ejecución de programas que se reciban vía correo electrónico;
c) La responsabilidad de no divulgar contraseñas de acceso al correo electrónico;
d) Una advertencia sobre la inconveniencia de almacenar contraseñas de acceso al correo electrónico en el mismo computador desde el cual se accede el correo electrónico;
e) Indicaciones sobre la elección de contraseñas seguras de acceso al correo electrónico;
f) Una recomendación sobre la conveniencia de que los usuarios tengan cuentas de correo electrónico distintas para efectos de su uso personal;
g) Un instructivo de cuándo no usar el correo electrónico;
h) Una prevención sobre la necesidad de comprobar el origen, despacho, entrega y aceptación mediante firma electrónica, e
i) Una precisión de las responsabilidades que corresponden a los usuarios en caso de comprometer a la institución, por ejemplo, con el envío de correos electrónicos difamatorios, uso para hostigamiento o acoso, compras no autorizadas, etc.

Artículo 26.- Los organismos sujetos a la presente norma, en la medida de sus posibilidades, deberán:

a) Instalar un antivirus que proteja frente a la posibilidad de obtener vía correo electrónico software malicioso;
b) Proveer mecanismos que mediante el uso de técnicas de cifrado, permitan proteger la confidencialidad e integridad de los documentos electrónicos;
c) Evitar el uso de cuentas de correo grupales;
d) Disponer controles adicionales para la verificación de mensajes que no se pueden autenticar;
e) Verificar que todos los equipos informáticos y medios digitales que sean usados en el almacenamiento y/o procesamiento de documentos electrónicos, de ser posible, sean reformateados previo a ser dados de baja.

Párrafo 8°

Control de acceso

Artículo 27.- El empleo de identificador formal de autenticación constituye un mecanismo básico para el uso de firma electrónica.

Los identificadores son un esquema de validación de la identidad del usuario para acceder a un sistema informático.

Un identificador temporal es aquel que se asigna a un usuario la primera vez que accede a un sistema, y que debe ser cambiado por éste en su primer acceso.

Artículo 28.- La asignación de los identificadores se deberá controlar mediante un proceso formal de gestión, en que el jefe directo del usuario peticionario será el responsable de la respectiva solicitud.

Para los efectos del referido control, en cada institución se impartirán instrucciones sobre la forma de asignación de identificadores que se aplicará. Dichas instrucciones deberán incluir a lo menos, lo siguiente:

a) La obligación de mantener en forma confidencial de los identificadores que se asignen;
b) La obligación de no registrar los identificadores en papel;
c) La prohibición de almacenar identificadores en un computador de manera desprotegida;
d) El deber de no compartir los identificadores de usuarios individuales;
e) El mandato de no incluir el identificador en cualquier proceso de inicio de sesión automatizado, por ejemplo, almacenado en una macro;
f) La indicación de cambiar los identificadores cuando hayan indicios de un posible compromiso del identificador o del sistema;
g) La recomendación de elegir identificadores que tengan una longitud mínima de ocho caracteres; sean fáciles de recordar; contengan letras, mayúsculas, dígitos, y caracteres de puntuación; no estén basados en cosas obvias o de fácil deducción a partir de datos relacionados con la persona, por ejemplo, nombres, números telefónicos, cédula de identidad, fecha de nacimiento; estén libres de caracteres idénticos consecutivos o grupos completamente numéricos o alfabéticos; y no sean palabras de diccionario o nombres comunes;
h) La indicación de cambiar los identificadores a intervalos regulares. Las contraseñas de accesos privilegiados se deberán cambiar más frecuentemente que los identificadores normales;
i) Normas para evitar el reciclaje de identificadores viejos, y
j) La indicación de cambiar el identificador temporal al iniciar la primera sesión.

Los sistemas informáticos deberán configurarse de manera que los usuarios se vean compelidos a cumplir con las obligaciones detalladas en los puntos anteriores.

Artículo 29.- Se deberá entregar a los usuarios identificadores temporales de una manera segura. Específicamente, se deberá evitar el uso de terceras partes o mensajes de correo electrónico no protegido (texto en claro) para comunicar el identificador.

Los usuarios deberán dar un acuso recibo de recepción del identificador.

Artículo 30.- En caso que los usuarios necesiten acceder a múltiples servicios o plataformas y sea necesario que mantengan múltiples identificadores, deberán ser notificados de que éstos deben ser distintos. Asimismo, se incentivará y facilitará el uso de certificados de firma electrónica.

Artículo 31.- Para reducir el riesgo de acceso no autorizado a documentos electrónicos o sistemas informáticos, se deberá promover buenas prácticas, como las de pantalla limpia.

En particular, se incentivará a los usuarios o configurar los sistemas de manera que se dé cumplimiento a los siguientes estándares:

a) Cerrar las sesiones activas en el computador cuando se finaliza la labor, a menos que éstas se puedan asegurar mediante un sistema apropiado de control de acceso, por ejemplo, con protector de pantalla con una contraseña protegida;
b) Cerrar las sesiones de los computadores principales cuando la sesión finaliza, lo que no significa, necesariamente, apagar el terminal o los equipos, y
c) Asegurar los terminales o equipos frente al uso no autorizado, mediante una contraseña de traba o de un control equivalente, por ejemplo, una contraseña de acceso cuando no se use.

Artículo 32.- Se deberá controlar el acceso a los servicios de red internos y externos mediante el uso de identificadores o certificados digitales.

Para tal efecto, los órganos de la Administración del Estado sujetos a la presente normativa deberán ajustarse a las siguientes exigencias:

a) Restringir la instalación de equipamiento personal que dificulte el control de acceso a documentos electrónicos y sistemas informáticos, de manera acorde a las políticas de seguridad de la institución, y
b) Mantener un catastro del equipamiento que permita la reproducción, distribución o transmisión masiva de información, y de las personas con privilegios de acceso a ellos.

Artículo 33.- Las instituciones regidas por la presente norma impartirán instrucciones relativas al uso de redes y servicios en red que, al menos, especifiquen lo siguiente:

a) Las redes y servicios de red a las que el acceso está permitido;
b) Los procedimientos de autorización para determinar quién tiene permitido acceder a las distintas redes y servicios de red, y
c) Los controles de gestión y procedimientos para proteger el acceso a las conexiones de la red y servicios de red.

Párrafo 9º

Desarrollo y mantenimiento de sistemas

Artículo 34.- Aquellos organismos que requieran precaver que la seguridad esté incorporada en los sistemas en la etapa de diseño, se entenderán como organismos complejos y para tal efecto, deberán adoptar las indicaciones contenidas en la sección correspondiente del Título V de esta norma, sobre "Nivel Avanzado de Seguridad para el Documento Electrónico".

Párrafo 10

Gestión de la continuidad del negocio

Artículo 35.- El encargado de seguridad deberá formular un plan de contingencia para asegurar la continuidad de operaciones críticas para la institución. Este plan deberá, como mínimo, disponer la efectiva gestión de las relaciones públicas, la eficiente coordinación con las autoridades apropiadas, como policía, bomberos, autoridades directivas, etc., y mecanismos eficaces para convocar a quienes sean los responsables de los documentos electrónicos y sistemas informáticos afectados.

TITULO V

Del nivel avanzado de seguridad del documento electrónico

Artículo 36.- Durante la segunda etapa de aplicación de esta norma, los órganos de la Administración del Estado deberán desarrollar las políticas, procedimientos, acciones y medidas tendientes a obtención del Nivel Avanzado de Seguridad de los documentos electrónicos que se establecen en este Título.

Artículo 37.- El Nivel Avanzado de seguridad para el documento electrónico exige el cumplimiento de las exigencias y condiciones reguladas en el Título IV para el Nivel Básico de seguridad, y las previstas en la Norma NCh2777, que se entiende parte integrante del presente decreto, con los ajustes que se establecen en este artículo.

a) **Política de Seguridad:**

Se aplicarán las disposiciones contenidas en el capítulo 3 de la norma NCh2777, con la siguiente adecuación:

- Las instituciones deberán tener las políticas de seguridad descritas en la sección 3.1 para los repositorios de documentos electrónicos. En particular, estas políticas deberán contener lo siguiente:

  i. Indicaciones respecto de los sistemas informáticos, con énfasis en el procedimiento de autorización de instalación o modificación de software y archivos de configuración de los sistemas;
  ii. Indicaciones de uso de la red;
  iii. Procedimientos de respuesta a incidentes de seguridad;
  iv. Procedimientos de delegación de autoridad para ejecutar acciones de emergencia en los sistemas y los procedimientos correspondientes.

b) **Seguridad organizacional:**

Se aplicará la sección 4.1 del capítulo 4 de la norma NCh2777, con excepción de sus puntos 4.1.5 y 4.1.7 que se adoptarán como recomendaciones, y las secciones 4.2 y 4.3 de dicho capítulo.

c) **Clasificación y control de bienes:**

Se aplicará la sección 5.1 del capítulo 5 de la norma NCh2777, en lo referido a bienes relacionados con el Documento Electrónico. Asimismo, se aplicará el punto 5.2.1 de la sección 5.2.

El punto 5.1.2 de dicha sección se aplicará con las siguientes adecuaciones:

- Los procedimientos de etiquetado y manipulación de la información se entienden referidos al Documento Electrónico.
- Se excluyen las normas contenidas en las letras (c) y (d).

d) **Seguridad del personal:**

Se aplicarán las secciones 6.1 y 6.3 del capítulo 6 de la norma NCh2777. La sección 6.2 se adoptará como recomendación.

e) **Seguridad física y del ambiente:**

Se aplicarán las secciones 7.1 y 7.2 del capítulo 7 de la norma NCh2777, para repositorios de documentos electrónicos, con las siguientes adecuaciones:

- Para la sección 7.1:

  i. Los controles físicos de entrada en el perímetro de seguridad deberán utilizar el carné de identidad como identificación válida en el caso de los chilenos, y el pasaporte en el caso de los extranjeros.
  ii. Todo ingreso de visitas al perímetro de seguridad deberá ser autorizado por escrito, quedando constancia del propósito y duración de ella. Los visitantes serán acompañados en todo momento por alguna persona autorizada de la organización hasta que abandonen el recinto.

- Para la sección 7.2:

  Se deberá velar para que los equipos computacionales en los que se almacenen documentos electrónicos y sistemas informáticos que los procesen, tengan un adecuado suministro de energía eléctrica, incluyendo no sólo el flujo de energía suministrado, sino también la "tierra eléctrica" de las instalaciones.
  La sección 7.3 se adoptará como recomendación.

f) **Gestión de las operaciones y comunicaciones:**

Se aplicarán las normas del capítulo 8 de la norma NCh2777, en su integridad.

g) **Control de acceso:**

Se aplicarán las normas del capítulo 9 de la norma NCh2777, con excepción de sus secciones 9.5, 9.6, 9.7 y 9.8 que se adoptarán como recomendaciones, y con los siguientes ajustes:

- Los registros de privilegios asignados, a los que hace referencia la sección 9.2.2, deberán tener un carácter histórico, es decir, no sólo se deben registrar los privilegios en aplicación. El período de conservación de estos registros será al menos el que las leyes vigentes indiquen para los documentos electrónicos a los que se pudo tener acceso con dichos privilegios.
- Las estipulaciones de la sección 9.4 deberán formalizarse en una política de uso correspondiente, de acuerdo a lo expresado en la sección "Política de Seguridad".

h) **Desarrollo y mantenimiento de sistemas:**

Se aplicarán únicamente las normas de la sección 10.3 del capítulo 10 de la norma NCh2777, con la siguiente adecuación:

- En las secciones referidas a firma electrónica, se adoptará lo establecido por la ley 19.799, sobre documentos electrónicos, firma electrónica y los servicios de certificación para dicha firma.

i) **Gestión de la continuidad del negocio:** Se aplicarán las estipulaciones del capítulo 11 de la norma NCh2777, en su integridad.

Artículo Segundo.- La presente norma deberá ser implementada por los diferentes órganos de la Administración del Estado dentro de los siguientes plazos:

- El Nivel 1, a más tardar en el año 2004.
- El Nivel 2, a más tardar en el año 2009.

Con la finalidad de lograr la debida implementación de esta norma en los plazos señalados, los servicios públicos deberán contemplar acciones adecuadas en sus respectivos planes de desarrollo informático. Los niveles de cumplimiento de la presente norma por parte de los servicios públicos se determinarán mediante la aplicación de un instrumento de evaluación que elaborará el Comité de Normas.

Artículo Tercero.- Créase el Subcomité de Gestión de Seguridad y Confidencialidad del Documento Electrónico como organismo asesor del Comité de Normas para el Documento Electrónico.

El Subcomité será coordinado por el Ministerio del Interior y tendrá entre sus funciones, proponer el Nivel de cumplimiento de la presente norma técnica por parte de los órganos de la Administración del Estado y el cronograma de implementación de la Norma en su nivel 2 por parte de los diferentes órganos de la Administración del Estado.

Artículo Cuarto.- Los Subsecretarios y Jefes de Servicio deberán designar, dentro del plazo de 30 días contados desde la fecha de total tramitación del presente decreto, un Encargado de Seguridad, para que desarrolle e implemente las políticas de seguridad en forma conjunta con el Comité de Gestión de Seguridad y Confidencialidad. En aquellos órganos en que no se designe dentro de plazo, actuará como Encargado de Seguridad el Auditor Interno de cada servicio.

Artículo Quinto.- El Comité de Normas para el Documento Electrónico podrá iniciar, de oficio o a petición de parte, un procedimiento de normalización con el objeto de sugerir al Presidente de la República la actualización de la norma técnica fijada por este decreto. En dicho procedimiento se tendrán en consideración los planteamientos del sector público y privado y de las Universidades.".

Anótese, tómese razón y publíquese.- RICARDO LAGOS ESCOBAR, Presidente de la República.- Francisco Huenchumilla Jaramillo, Ministro Secretario General de la Presidencia.- José Miguel Insulza Salinas, Ministro del Interior.

Lo que transcribo a Ud. para su conocimiento.- Saluda Atte. a Ud., Rodrigo Egaña Baraona, Subsecretario General de la Presidencia.