Ministerio Secretaría General de la Presidencia

APRUEBA NORMA TÉCNICA SOBRE SEGURIDAD DE LA INFORMACIÓN PARA LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO

Vistos:

Considerando:

D e c r e t o

ARTÍCULO PRIMERO. - Apruébese la siguiente norma técnica sobre seguridad de la información para los órganos de la Administración del Estado.

''NORMA TÉCNICA SOBRE SEGURIDAD DE LA INFORMACIÓN PARA LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO"

TITULO I

Ámbito de aplicación

Artículo 1º.- La presente norma técnica establece los estándares mínimos obligatorios para la gestión de la seguridad de la información, por parte de los órganos de la Administración del Estado.

Los requisitos y procedimientos previstos en esta norma tienen por finalidad garantizar la confidencialidad, integridad, disponibilidad y factibilidad de autenticación de la información que gestionen los órganos de la Administración del Estado.

Artículo 2°. Las entidades implementarán la presente norma según el nivel de criticidad en que se encuentren clasificadas, de conformidad con los siguientes niveles:
Nivel 1. Nivel básico de seguridad
Nivel 2. Nivel avanzado de seguridad

Para efectos de dicha implementación, se deberán cumplir necesariamente las acciones indicadas en la presente norma y los controles definidos para cada uno de los niveles, los cuales serán determinados por medio de una Guía Técnica dictada conforme al título VII de la presente norma.

No obstante lo anterior, la entidad podrá elevar su nivel de seguridad en los procesos que estime necesarios o podrá incorporar controles adicionales al nivel básico establecido en la presente normativa.

Excepcionalmente, tratándose del nivel avanzado, las entidades podrán excluir fundadamente, mediante acto administrativo, ciertos controles de la implementación.

TITULO II

Definiciones

Artículo 3º.- Para efectos de la presente norma, acorde a las definiciones utilizadas en la NCh-ISO 27000 cuando corresponda, se entenderá por:

Activo de información: Datos o conocimiento que tiene valor para la entidad.

Amenaza de Seguridad: Causa potencial de un incidente de seguridad, que puede provocar daño a un activo de información o una entidad.

Autenticación: Proceso que provee una garantía de que una característica afirmada por algo es correcta.

Autenticidad: Propiedad de que algo es lo que afirma ser.

Dueño de un activo de información: Persona a quien se le asigna el deber de mantener actualizada la información del activo, su correcta operación y la aplicación de las políticas de seguridad de la entidad al mismo.

Confidencialidad: Propiedad de la información de no estar a disposición o no ser revelada a individuos, entidades o procesos no autorizados o no previstos legalmente.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada o habilitada legalmente.

Entidad: Órgano o servicio de la Administración del Estado, según lo dispuesto en el inciso segundo del artículo 1° de la Ley N°18.575.

Evento de Seguridad: Ocurrencia identificada en un sistema, servicio o red que indica una posible brecha de la seguridad, de las políticas, una falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad de la entidad.

Incidente de Seguridad: Uno o más eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones o actividades de una entidad o amenazar la seguridad de la información de la misma.

Infraestructura de información: Conjunto de servicios, tecnología y sistemas que soportan la operación de un proceso o actividad.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Gestión de Riesgos: Proceso que maneja la incertidumbre presente en las actividades u operaciones de una entidad. Se compone de la identificación, evaluación y tratamiento de riesgos.

Partes Interesadas: Conjunto de organismos o individuos, internos o externos respecto a una entidad, que pueden afectar o percibirse a sí mismos como afectados por una decisión o actividad de la entidad.

Políticas de Seguridad: Conjunto de normas, objetivos y lineamientos de una entidad, declaradas formalmente, con el fin de lograr los objetivos de seguridad de la misma.

Postura de riesgo de seguridad: Estado de seguridad de la infraestructura de información de la entidad que se basa en los recursos y capacidades existentes para manejar la defensa de la entidad y para reaccionar según las situaciones que ocurren.

Riesgo: Efecto de la incertidumbre sobre los objetivos de una entidad, habitualmente expresado en relación a las consecuencias de un evento y su probabilidad de ocurrencia.

Sistema de Gestión de Seguridad de la Información: Conjunto de políticas, normas y procedimientos necesarios para desarrollar las funciones de seguridad de una manera sistemática, estructurada y alineada con los objetivos estratégicos y necesidades de la entidad.

Trazabilidad: Serie de procedimientos que permiten seguir el proceso de evolución de un producto en cada una de sus etapas.

TITULO III

De la gestión de seguridad de los activos de información en los órganos de administración del estado

Artículo 4°.- El Jefe Superior de Servicio, o su equivalente, es el responsable final por la seguridad de la información de la entidad y deberá velar por el cumplimiento de las medidas de seguridad de los activos de información y de la infraestructura de información de ella. En particular, deberá garantizar la ejecución de las siguientes acciones:

a) Desarrollar y documentar políticas de seguridad de la información compatibles con los objetivos estratégicos de la entidad;
b) Diseñar y documentar los procesos y procedimientos para poner en práctica las políticas de seguridad;
c) Considerar la asignación de recursos para implementar los procesos y procedimientos señalados precedentemente;
d) Monitorear el cumplimiento de las políticas, procesos y procedimientos establecidos y revisarlos de manera de mitigar los riesgos de seguridad;
e) Concientizar, capacitar y educar a los usuarios para operar los sistemas informáticos de acuerdo a las exigencias establecidas;
f) Evaluar periódicamente el desempeño y efectividad de las políticas, procesos y procedimientos de seguridad;
g) Mejorar de forma continua las políticas, procesos y procedimientos de seguridad;
h) Definir y documentar los roles y responsabilidad de las entidades e individuos involucrados en los literales previos.

Artículo 5º.- La entidad deberá elaborar y documentar una política de seguridad de la información, que establezca las directrices generales y de alto nivel a seguir por la institución, con el objetivo de implementar medidas de seguridad en concordancia con sus objetivos estratégicos.
A partir de los lineamientos dispuestos en la política de seguridad de la información, se elaborarán e implementarán otras medidas, tales como políticas específicas, procedimientos, normas y planes de seguridad.
La política de seguridad de la información deberá incluir, al menos, lo siguiente:

a) El compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional;
b) Una definición de seguridad de la información, incluyendo sus objetivos globales, alcance e importancia al interior de la entidad;
c) Establecimiento de un sistema de gestión de seguridad de la información de la entidad, alineado con lo establecido en el Artículo 4°, y el marco de trabajo que será utilizado;

d) Los mecanismos de difusión de sus contenidos al interior de la organización;
e) Su evaluación en forma periódica, a lo menos cada 3 años, o cada vez que se produzca un cambio importante en las condiciones de seguridad de la entidad, o en las definiciones de procesos y servicios estratégicos.

Artículo 6º.- La entidad deberá contar con una estructura apropiada de gobierno de seguridad, además procurará contar con personal capacitado para cumplir los objetivos del sistema de gestión de seguridad de la información.

Para ello, la entidad deberá contar con un Encargado de Seguridad, que reportará directamente al Jefe Superior del Servicio, o su equivalente, en materia de seguridad de la información, con independencia de las demás jefaturas de la Institución.

Las funciones específicas que deberá desempeñar internamente el Encargado de Seguridad serán establecidas en la resolución o acto administrativo correspondiente que lo designe. En todo caso deberá cumplir, a lo menos, con las siguientes funciones:

a) Tener a su cargo el desarrollo de las políticas de seguridad al interior de la organización, el control de su implementación, velar por su correcta aplicación, así como por su revisión y actualización de acuerdo con las necesidades de la institución y la periodicidad de revisión definida en las disposiciones de la Política;
b) Coordinar la respuesta a incidentes de seguridad de la información;
c) Mantener un registro de los incidentes de seguridad y promover acciones que impidan o reduzcan la probabilidad de ocurrencia de éstos;
d) Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes;
e) Mantener actualizado un Inventario de Activos de información de la entidad, identificando y clasificando los activos de información de la misma.

Artículo 7°.- La entidad deberá conformar un comité asesor en seguridad de la información, integrado por colaboradores directos del Jefe Superior del Servicio y representativos de áreas en las que se identifiquen riesgos de seguridad para la institución, incluyendo al Encargado de Seguridad.

El comité, a lo menos, deberá:

a) Desarrollar procesos de alineamiento de seguridad de la información con los objetivos estratégicos de la entidad;
b) Validar las propuestas de alto nivel que le presente a revisión el Encargado de Seguridad;
c) Realizar seguimiento de la ejecución de los procesos de seguridad;
d) Revisar el cumplimiento de las políticas de seguridad mediante el sistema de gestión de seguridad de la Institución.

Artículo 8°.- La entidad deberá realizar una gestión de riesgos previo a elaborar e implementar el sistema de gestión de seguridad de la información, de forma al menos anual, una vez implementado éste. Para ello deberá realizar acciones dirigidas a evaluar y tratar dichos riesgos, considerando, a lo menos:

a) Establecer y mantener criterios de evaluación y aceptación de los riesgos de seguridad de la entidad;
b) Asegurar que las evaluaciones de riesgo produzcan resultados consistentes, válidos y comparables;
c) Identificar los riesgos de seguridad asociados a la pérdida de confidencialidad, integridad y disponibilidad de los activos de información identificados en el Inventario de Activos de información;
d) Analizar los riesgos respecto de sus posibles consecuencias, probabilidad de ocurrencia, determinando niveles de riesgo;
e) Determinar y aplicar controles de seguridad que sean apropiados para el tratamiento los riesgos de seguridad identificados;
f) Generar una Declaración de Aplicabilidad, aprobada por el Jefe Superior del Servicio, que contenga, a lo menos, las justificaciones técnicas, estratégicas y/o de costo/beneficio de las inclusiones y particularmente respecto de las exclusiones de los controles establecidos en la Guía Técnica, según lo prescrito en el inciso tercero del artículo 2°;
g) Monitorear, revisar y verificar que las medidas de mitigación de riesgos son efectivas, y se mantienen en dicha condición en el tiempo.

Las acciones realizadas en el proceso de gestión de riesgos deben quedar documentadas y revisarse con una periodicidad que permita una mejora continua del sistema de gestión de seguridad de la información.

Ministerio Secretaría General de la Presidencia

TITULO IV

De los dominios o ámbitos de control de seguridad para el nivel básico de seguridad

Artículo 9º.- Los dominios o ámbitos de control que abarcan el nivel básico de seguridad son, al menos, los siguientes:

a. Seguridad en relación con las personas

La entidad procurará asegurar que el personal interno y externo comprenda y cumpla las funciones y responsabilidades de seguridad que le hayan sido asignadas, incluso una vez terminado su relación con la entidad.

b. Administración de activos

La entidad deberá identificar los activos de información, definir las responsabilidades de protección de los mismos y asegurar que reciban el nivel de protección adecuado para prevenir una brecha de confidencialidad, integridad o disponibilidad de la información.

c. Control de Acceso

La entidad deberá proteger el acceso a la información e infraestructuras, y prevenir el acceso no autorizado a ellas.

d. Seguridad Física y del Ambiente

La entidad deberá proteger el acceso físico a la información e infraestructuras, y prevenir el acceso no autorizado, el compromiso físico de los activos, evitando o mitigando las brechas de confidencialidad, integridad o disponibilidad de la información.

e. Seguridad en las Operaciones

La entidad deberá asegurar la operación correcta y segura de su infraestructura de información.

f. Seguridad de las Comunicaciones

La entidad deberá asegurar la protección de la información en tránsito y en reposo, tanto en redes como en infraestructuras y sistemas.

g. Adquisición, desarrollo y mantenimiento de sistemas

La entidad deberá asegurar que la seguridad de la información sea parte integral del ciclo de vida de los sistemas.

h. Seguridad en la relación con proveedores

La entidad deberá asegurar la protección de los activos de información a los que tengan acceso proveedores.

i. Gestión de incidentes

La entidad deberá asegurar un enfoque consistente y eficaz en la gestión de incidentes de seguridad.

j. La seguridad como factor habilitante para continuidad de las operaciones

La entidad deberá incorporar la seguridad de la información en sus procesos de continuidad del negocio.

k. Cumplimiento

La entidad deberá cumplir con todos los requisitos legales, regulatorios y contractuales pertinentes.

Artículo 10º.- La implementación específica de controles para cada uno de estos dominios será especificada en la Guía Técnica descrita en el título VII de la presente norma.

TITULO V

De los niveles de seguridad

Artículo 11º.- La entidad deberá desarrollar y mantener un sistema de gestión de seguridad de la información que se oriente a alcanzar el nivel de seguridad apropiado para la entidad.

Artículo 12º.- El sistema de gestión de seguridad de la información deberá tender a cumplir, como mínimo, el nivel básico de seguridad de la información.

Artículo 13º.- El nivel de seguridad se aplica para toda la entidad. La entidad puede elevar el nivel de seguridad de algún proceso específico en caso de ser considerado necesario.

Artículo 14º.- El Nivel Básico de Seguridad consiste en el estricto cumplimiento de las disposiciones de la presente norma y de los controles del nivel básico establecidos en la Guía Técnica.

Artículo 15º.- El Nivel Avanzado de Seguridad consiste en el estricto cumplimiento de las disposiciones de la presente norma, de los controles del nivel básico establecidos en la Guía Técnica y de los controles del nivel avanzado incluidos en la Declaración de

Aplicabilidad de la entidad. Para cumplir el nivel avanzado de seguridad deberá cumplirse, a lo menos, con algún control asignado a dicho nivel.

TITULO VI

De la mejora continua de la seguridad de la información

Artículo 16º.- El jefe de servicio deberá asegurar que las medidas de gestión de la seguridad de la información son apropiadas y suficientes para cumplir los objetivos de la entidad, a través de la definición y establecimiento de métricas para evaluar y medir periódicamente la efectividad del sistema de gestión de seguridad.

Artículo 17º.- La entidad deberá programar, ejecutar y documentar auditorías independientes, con alcances definidos, con el fin de evaluar el desempeño y la efectividad del sistema de gestión de seguridad de la información y de los controles de seguridad implementados.

Artículo 18º.- Los resultados obtenidos durante la evaluación del desempeño y efectividad del sistema, deberán comunicarse y reportarse al jefe de servicio, o su equivalente, para revisar y evaluar la necesidad de acción respecto a los mismos.

Artículo 19º.- En el caso de detectar algún incumplimiento o deficiencia del sistema, la entidad deberá tomar las medidas correctivas necesarias para resolverlo, incluyendo, si es necesario, realizar cambios sobre el sistema de gestión de seguridad de la información.

TITULO VII
Guía Técnica

Artículo 20º.- El Ministerio Secretaría General de la Presidencia publicará una Guía Técnica en un plazo de 120 días desde la total tramitación del presente decreto, la que será aprobada mediante resolución exenta, en la cual se detallarán los controles de seguridad correspondientes a cada nivel.
La Guía Técnica se entenderá parte integrante de la presente norma y su cumplimiento será obligatorio de acuerdo al nivel de seguridad de cada entidad.

ARTÍCULO SEGUNDO. – Déjese sin efecto el Decreto Nº 83 de 2005 del Ministerio Secretaría General de la Presidencia.

DISPOSICIONES TRANSITORIAS

ARTÍCULO PRIMERO. – Para efectos de mantener actualizada la normativa, mientras no se defina otra instancia para dichos efectos, se crea la Mesa Técnica de Gestión de la Seguridad de la Información, de carácter interministerial, y cuyo objetivo será mantener actualizadas la presente norma y su correspondiente Guía Técnica, de forma compatible con esfuerzos y estándares internacionales en la materia. El Comité sesionará trimestralmente y estará conformado, a lo menos, por representantes del Ministerio del Interior y Seguridad Pública, del Ministerio de Defensa Nacional, del Ministerio de Hacienda, del Ministerio de Economía, Fomento y Turismo, del Ministerio de Transportes y Telecomunicaciones y del Ministerio Secretaría General de la Presidencia, quien presidirá las sesiones. Sin perjuicio de lo anterior, el Comité podrá sesionar en forma extraordinaria a requerimiento de los integrantes de la Mesa y con aprobación del Ministerio Secretaría General de la Presidencia.

ARTÍCULO SEGUNDO. – Las disposiciones de los artículos 8°, 16°, 17° y 18° de la presente norma comenzarán a regir a contar de 1 año desde su publicación, sin perjuicio de que su implementación podrá ser efectuada desde la fecha de su publicación de forma voluntaria por razones de buen servicio.