REPUBLICA DE CHILE
MINISTERIO DE BIENES NACIONALES
DIVISION PLANIFICACION Y PRESUPUESTO
FNB/EQE/GAC/HMA
Condución N°535956

APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE BIENES NACIONALES. DEJA SIN EFECTO RESOLUCIÓN EXENTA N° 1796 DE 2018 DEL MINISTERIO DE BIENES NACIONALES.-

SANTIAGO, 03 SEP 2019

EXENTA N° 1005 **/. VISTOS:**

Ministerio de Bienes Nacionales
Registro
V° B° Jefe

MINISTERIO DE HACIENDA
OFICINA DE PARTES
RECIBIDO

CONTRALORIA GENERAL
TOMA DE RAZON
RECEPCIÓN

DEPART. JURÍDICO		
DEP. T.R Y REGISTRO		
DEPART. CONTABIL.		
SUB. DEP. C. CENTRAL		
SUB. DEP. E. CUENTAS		
SUB. DEP. C.P.Y. BIENES NAC.		
DEPART. AUDITORIA		
DEPART. V.O.P.,U y T		
SUB. DEPT. MUNICIP.		

REFRENDACIÓN
REF. POR $
IMPUTAC.
ANOT. POR $
IMPUTAC.
DECUC. DTO.

Ministerio de Bienes Nacionales
Exento de Trámite de Toma de Razón

Estos antecedentes; la Ley N° 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado; el DFL N°. 29, de 2004, del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.834, Estatuto Administrativo; La Ley N° 19.880, que establece Bases de los Procedimientos Administrativos; La Ley N° 19.799, sobre Documentos Electrónicos, Firma Electrónica y los Servicios de Certificación de dicha Firma; el Decreto N° 181/2002, del Ministerio de Economía , que aprueba el Reglamento de la ley N° 19.799; el Decreto N° 83/2004 del Ministerio Secretaría General de la Presidencia; la Resolución Exenta N° 904, de 31 de mayo de 2011, que crea el Comité de Seguridad de Información del Ministerio de Bienes Nacionales; la Resolución Exenta N°862, de 08 de agosto 2018, que deroga parcialmente Resolución Exenta N° 904 de 2011 y aprueba normas para el funcionamiento del comité de Seguridad de la información del Ministerio de Bienes Nacionales; la Resolución Exenta N° 829, de 15 de julio de 2019, que designa Encargado de Seguridad de Información; y la Resolución N° 7 de 2019 de la Contraloría General de la República.

C O N S I D E R A N D O:

Que para el cumplimiento de sus funciones el Ministerio de Bienes Nacionales ha identificado la necesidad de gestionar adecuadamente la Seguridad de la Información, con el objetivo de mejorar los niveles de protección de los Activos de Información relevantes que dan sustento a sus procesos de provisión y de soporte.

Que para estos efectos se ha designado un Encargado de Seguridad de la Información y creado un Comité de Seguridad de la Información, que en función del marco legal y tecnológico vigente, ha propuesto al Jefe del Servicio una Política General de Seguridad de la Información.

Que la referida política declara el compromiso del Ministerio de Bienes Nacionales tendiente a asegurar la confidencialidad, integridad y disponibilidad de los Activos de Información institucionales, en las distintas actividades que realizan tanto el personal propio, así como las empresas externas que le prestan servicios, en el desempeño de sus funciones.

R E S U E L V O:

I.- Derógase la Resolución Ex. N° 1796 de 19 de diciembre de 2018.

II.- Apruébase la Política General de Seguridad de la Información para el Ministerio de Bienes Nacionales, cuyo texto es el siguiente:

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código: TIC-SI-POL

Versión: 4

Fecha: 26.08.2019

TABLA DE CONTENIDO

DESCRIPCIÓN GENERAL DE CAMBIOS

1 29.05.2012 Todas Se actualiza misión institucional y modifica presentación

2 19.05.2016 Todas Se actualiza declaración institucional, alcance, roles y responsabilidades, difusión. Se agrega aceptación.

3 22.10.2018 Todas Se actualiza de acuerdo a observaciones de red de expertos PMG SI, se agregan dominios de la norma.

4 25.07.2019 Objetivos y Roles y Responsabilidades Se actualiza la forma de clasificar la información en base a la norma NCh-ISO 27001:2013 y NCh-ISO 27002:2013.

Se actualiza el alcance y la declaración institucional.

Se agrega rol del encargado de ciberseguridad en la lista de roles y responsabilidades.

OBJETIVOS.-

El objetivo de la presente Política es entregar los lineamientos para la implementación de controles de seguridad de la información que permitan conservar, salvaguardar y proteger la información contenida y generada en los procesos del Ministerio de Bienes Nacionales, en adelante "el Ministerio", reduciendo los riesgos ante una eventual pérdida producto de la materialización de una o más amenazas asociadas a los Activos de Información, de manera de preservar su disponibilidad, integridad y confidencialidad.

En virtud de lo anterior, el Ministerio se compromete a lo siguiente:

Mantener un adecuado catastro de Activos de Información relevantes para los procesos de la institución, realizando una evaluación de riesgos de Seguridad de la Información.

Implementar y proponer controles en base a un marco normativo para dar cumplimiento a la Política General, políticas específicas y procedimientos referentes a la Seguridad de la Información.

Clasificar la información según su carácter de confidencialidad e implementar mecanismos de seguridad de acuerdo a los estándares NCh-ISO 27001:2013 y NCh-ISO 27002:2013, ambas idénticas a la normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013, respectivamente.

Llevar registro, gestionar y determinar la respuesta ante incidentes que afecten a los Activos de Información.

Ejecutar un plan permanente de capacitación, difusión y sensibilización de los funcionarios en temas relativos a la Seguridad de la Información.

Establecer los mecanismos de difusión de la presente política para el conocimiento de terceros que suscriban contratos o convenios con el Ministerio, en lo que respecta a sus derechos y obligaciones en materia de Seguridad de la Información, los cuales deberán quedar debidamente especificados en los respectivos instrumentos que les vinculan al Ministerio y en todo mecanismo de traspaso de información que exista entre las partes.

Asegurar la continuidad de sus procesos, determinando planes de contingencia ante desastres.

ALCANCE.-

La presente política se aplicará en todos los elementos que involucren a los Activos de Información que soportan los procesos de provisión de servicios estratégicos establecidos en el Formulario A1 vigente y compromete el actuar de la Autoridad de Gobierno, funcionarios, personal a honorarios y personal contratado por convenios de fondos de terceros sin distinción de nivel jerárquico ni tipo de servicio para los cuales fueron requeridas sus prestaciones, a estudiantes en prácticas académicas y a los proveedores que prestan servicios a la institución.

DEFINICIONES Y ABREVIATURAS.-

Activos de Información: Corresponden a todos aquellos elementos necesarios para que el Ministerio funcione y consiga sus objetivos estratégicos.

Estos Activos se pueden dividir en tres tipos relacionados:

Los de información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)

Los equipos/Sistemas/Infraestructura que soportan esta información.

Las personas que utilizan la información y tienen el conocimiento de los procesos institucionales.

Riesgo de Seguridad de la Información: Corresponde a una amenaza potencial que podría afectar a los Activos de Información vinculados a procesos de provisión de Productos Estratégicos. A su vez, amenaza es toda acción que aprovecha una vulnerabilidad o debilidad de un activo para atentar contra la seguridad.

Integridad: Propiedad de la información en virtud de la cual se garantiza que se encuentra completa, actualizada y es veraz, sin modificaciones inapropiadas o corrupción.

Confidencialidad: Propiedad de la información en virtud de la cual se garantiza que se encuentra protegida de personas/usuarios no autorizados.

Disponibilidad: Propiedad de la información en virtud de la cual se garantiza que se encuentre disponible cuando se necesite.

Incidente de seguridad: evento o situación que compromete de manera importante la disponibilidad, integridad y confidencialidad de la información.

ROLES Y RESPONSABILIDADES.-

El Ministerio contará con un Comité de Seguridad de la Información, "CSI", el cuál será responsable de la administración del Sistema de Gestión de Seguridad de la Información, "SGSI", según se describe a continuación:

Rol	Responsabilidad	Funciones y atribuciones
Jefe de Servicio	Liderar la implantación y mejora continua del SGSI	a. Demostrar liderazgo y compromiso con respecto al SGSI; b. Establecer una política de Seguridad de la Información; c. Asegurar que las responsabilidades y autoridades para los roles de SGSI sean asignados y comunicados; y , d. Responder, en coordinación con actores relevantes, ante incidentes de seguridad que afecten la continuidad operacional.
Comité de Seguridad de la Información	Coordinar la operación del SGSI	a. Actualizar las políticas de seguridad del SGSI; b. Validar, aprobar y difundir dichas políticas; c. Coordinar la implementación de los controles necesarios para materializar dichas políticas; d. Monitorear cambios significativos que pudieran afectar los riesgos de los Activos de Información; e. Monitorear incidentes de seguridad de información; y , f. Ponderar y establecer acciones adecuadas respecto de los incidentes detectados.
Encargado/a de Seguridad de Información	Coordinar la operación del SGSI	a. Encargarse del desarrollo inicial de las políticas de seguridad y el control de su implementación y velar por su correcta aplicación; b. Coordinar actividades para el CSI; c. Coordinar la debida respuesta y priorización al tratamiento de incidentes vinculados a los activos de información y la continuidad operacional; d. Monitorear el avance general de la implementación de las estrategias de control y tratamientos de riesgos; e. 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; f. Supervisar que las personas claves cuenten con las competencias y conocimientos necesarios para la operación del SGSI; y, g. Informar a el/la Jefe de Servicio sobre el desempeño del SGSI.
Encargado/a de ciberseguridad	Coordinar la implementación de Políticas y lineamientos relativos a	a. Alinear los esfuerzos de las distintas áreas, respecto a la protección de los sistemas tecnológicos y a la información contenida en ella, según los criterios de Ciberseguridad;

	materias de Ciberseguridad	b. Velar por el cumplimiento de la mitigación de riesgos que puedan afectar a la plataforma tecnológica, por parte de TI y Proveedores de Servicios; c. Gestionar al interior de la institución, todo requerimiento de información solicitado por el Equipo de Ciberseguridad del Ministerio del Interior y Seguridad Pública; d. Informar al Equipo de respuesta ante incidentes de seguridad informática (CSIRT, por sus siglas en inglés) sobre cualquier incidencia que pueda afectar a la plataforma tecnológica de la institución, sea que esta se encuentre expuesta a internet o que se encuentre en su red interna; y , e. Apoyar el proceso de Sensibilización en materias de Ciberseguridad al interior de la Institución.
Dueños de los procesos	Proteger sus Activos de Información	a. Definir y actualizar el inventario de los Activos de Información propios de sus procesos; b. Determinar las amenazas y riesgos que podrían afectar a sus activos, así como los controles que dichos procesos requieran para tratarlos; y, c. Comunicar oportunamente los incidentes relativos a la Seguridad de la Información que detecten.
Personal interno y externo	Uso responsable de los Activos de Información	a. Conocer y aplicar la normativa vigente, políticas y procedimientos de Seguridad de la Información; y, b. Comunicar oportunamente los incidentes relativos a la Seguridad de la Información.

DECLARACIÓN INSTITUCIONAL.-

El Ministerio es el organismo del Estado que reconoce, catastra y gestiona eficiente y eficazmente el patrimonio fiscal; poniendo el territorio al servicio del desarrollo económico, social y cultural del país, con una mirada integral y en forma sustentable , mediante el diseño, implementación y evaluación de políticas, planes, normas y programas, contribuyendo al aprovechamiento armónico y sustentable del territorio y al desarrollo económico, social y cultural de su población, y apoyar el ejercicio del derecho de propiedad particular para los grupos de población vulnerables, al regularizar la pequeña propiedad raíz particular..

Para el logro de los objetivos estratégicos, el Ministerio busca integrar permanentemente nuevas Tecnologías de la Información y de las Comunicaciones, "TICs", para apoyar los procesos institucionales y el

quehacer de su personal y de toda persona ligada a la Institución en general. La incorporación de TICs, si bien presenta beneficios, ventajas y oportunidades, conlleva asimismo riesgos que pueden afectar la información y con ello comprometer la imagen y/o el cumplimiento de los objetivos del Ministerio.

En este contexto, el MBN entiende la necesidad de gestionar la Seguridad de la Información realizando, todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determina, basándose para ello en estándares definidos en la materia, con el fin de alcanzar los niveles adecuados de integridad, confidencialidad y disponibilidad de los Activos de Información determinados como críticos para la ejecución de los procesos institucionales, dando cumplimiento de esta forma al marco legal vigente.

Integridad: La información está completa, actualizada y es veraz, sin modificaciones inapropiadas o corrupción.

Confidencialidad: La información está protegida de personas/usuarios no autorizados.

Disponibilidad: Los usuarios internos y externos pueden acceder a la información cuando lo requieran para utilizarla de acuerdo al marco legal y normativo definido.

MARCO PARA LA GESTIÓN DE LA INFORMACIÓN.-

Para cumplir con los compromisos antes descritos, se realizarán las siguientes acciones:

Se implementará, de manera progresiva, un SGSI basado en la norma NCh-ISO 27001:2013, con sus dominios y controles. Para las orientaciones o directrices de la implementación, se utilizará la norma NCh-ISO 27002:2013.

El SGSI se deberá alinear con las directrices que establece la Política Nacional de Ciberseguridad.

El SGSI deberá integrar el modelo de seguridad con las metodologías y políticas existentes en el MBN.

DIFUSIÓN.-

La difusión de esta política se realizará mediante el envío de correos electrónicos a todos los funcionarios del MBN, junto con su publicación en la intranet institucional.

REVISIÓN.-

Toda política deberá ser revisada y evaluada al menos una vez al año o cuando se produzcan cambios en las normativas y leyes que regulan el accionar del Ministerio, o cuando el Jefe de Servicio así lo disponga.

Para su revisión se podrá tomar en cuenta la evaluación de los riesgos de Seguridad de Información, el resultado de auditorías internas o externas, cambios en tecnologías, modificaciones en la organización del Ministerio, así como la ocurrencia de incidentes de seguridad que afecten al SGSI.

PROCESOS DISCIPLINARIOS.-

El incumplimiento o violación a las Políticas y Procedimientos de Seguridad, debidamente acreditado, conllevará a un proceso disciplinario formal avalado por la norma vigente y Estatuto Administrativo según corresponda, a los funcionarios, personal a honorarios y personal contratado por convenios de fondos de terceros, o el término anticipado del contrato por incumplimiento de las obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa, sin prejuicio de las responsabilidades civiles y penales que deriven de tales infracciones.

Anótese, comuníquese, notifíquese y archívese.

(FDO.) ALEJANDRA BRAVO HIDALGO. Subsecretaria de Bienes Nacionales.

Lo que transcribo a Ud., para su conocimiento.

Saluda a Ud.,

ANDREA SALAS BORDALI
Jefe de División Administrativa

Distribución:

Gab. Subsecretaría de Bs. Nac.
Sec. Reg. Ministeriales de Bienes Nacionales
Jefes de Oficinas Provinciales.
Jefes de Divisiones.
Jefes de Departamentos.
Encargados de Unidades.
Unidad de Decretos.
Archivo Oficina de Partes.