

**ACTUALIZA POLÍTICA GENERAL DE
SEGURIDAD DE LA INFORMACIÓN Y
ESTABLECE RESPONSABLE
INSTITUCIONAL.**

Santiago, 30 DIC 2015

RESOLUCION EX. N° 01873 /

VISTO: lo dispuesto en el Título VI de la Ley N° 19.496 sobre normas de Protección de los Derechos de los Consumidores y fija sus funciones; el D.S N° 83 de 2004, Ministerio Secretaría General de la Presidencia, que Aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; la Norma Chilena Oficial NCH-ISO 27001 Of.2009, sobre sistema de gestión de la seguridad de la información; la Ley N°20.285, sobre acceso a la información pública; la Ley N°19.628 sobre Protección de la vida privada, la Guía Metodológica del Sistema de Seguridad de la Información; y la Resolución N° 1600, de 2008, de la Contraloría General de la República.

CONSIDERANDO:

1. Que es necesario adecuar la Política General de Seguridad de la Información aprobada por Resolución Exenta N° 1631, del 08 de noviembre de 2012, así como actualizar las responsabilidades, de acuerdo a los lineamientos y organización institucional.

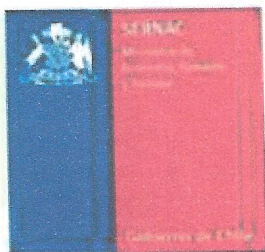
2. Las facultades que la ley confiere al Director Nacional.

RESUELVO:

1.- **ACTUALÍCESE** la "Política General de Seguridad de la Información", la que forma parte de esta Resolución y que es del tenor siguiente:

I. Declaración Institucional

El Servicio Nacional del Consumidor es la institución del Estado, responsable de vigilar que se respeten los derechos de los/as consumidores/as, y de implementar una política de protección de estos derechos, promoviendo con ello mercados más justos y eficientes, consumidores empoderados en su rol e impacto en dichos mercados y una institucionalidad acorde a las necesidades y desafíos, en un marco de excelencia e integrando a los distintos actores del sistema.



Define sus líneas estratégicas en cuanto a: informar, educar y proteger eficientemente a los consumidores ciudadanos, en un marco técnico de eficacia, eficiencia y transparencia de la acción institucional y de los mercados, y del rol responsable, activo y participativo de cada uno de sus actores, considerando para ello tanto los requisitos legales, como las necesidades de los/as ciudadanos/as.

Es en este sentido que la Dirección Nacional considera que los activos de información son esenciales para el desarrollo de sus procesos, comprometiéndose a iniciar y sentar las bases para el desarrollo paulatino de un sistema de Seguridad de la Información, que asegure preservar la confidencialidad, integridad y disponibilidad de estos activos, con la finalidad de asegurar la continuidad del negocio, dar cumplimiento a la normativa aplicable y a las definiciones estratégicas vigentes, mediante la implementación de un conjunto adecuado de controles que permitan gestionar los riesgos y garantizar la Seguridad de la Información, así como el mejoramiento continuo del sistema y el desarrollo de una cultura de seguridad institucional.

II. Objetivos de la Política y sistema de Seguridad de la Información

Para la implementación paulatina de un Sistema de Seguridad de la Información, se establecen los siguientes objetivos:

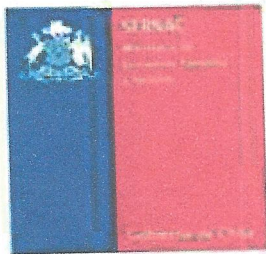
- Realizar un levantamiento y/o inventario de los activos de información relevantes asociados a los procesos, con la finalidad de evaluar su nivel de protección y criticidad.
- Realizar un análisis de riesgos sobre los activos de información que se definan institucionalmente como críticos, con el fin de implementar controles que permitan mitigar estos riesgos.
- Desarrollar de manera permanente actividades de capacitación, difusión y sensibilización a los funcionarios de la institución, sobre Seguridad de la Información.
- Complementar la presente Política General de Seguridad de la Información, con las políticas específicas, procedimientos, instructivos, etc. que permitan articular el sistema, integrándose tanto de manera metodológica como documental con los sistemas de gestión existentes en la institución.

III. Alcance de la Política de Seguridad de la Información

La presente política será de aplicación obligatoria a toda la Institución, sus procesos, funcionarios, proveedores y clientes tanto internos como externos y los incumplimientos que den origen a incidentes que afecten la seguridad de los activos de información, serán objeto de responsabilidad administrativa, en los términos establecidos en el párrafo V del DFL N°29 de 2005, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.834, sobre Estatuto Administrativo.

La presente política adopta su base de contenidos, a partir de las buenas prácticas definidas en el la Nch-ISO 27001 y de los requisitos legales, normativos y contractuales relativos a la seguridad de la información, que sean aplicables al Servicio, como el Decreto Supremo N° 83/2004 del Ministerio Secretaria General de la Presidencia, que aprueba la norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

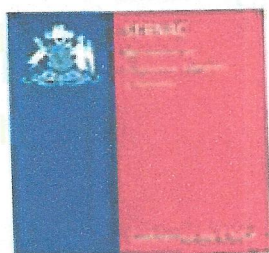




IV. Roles y Responsabilidades

La estructura de roles para la gestión del sistema, estará constituida de la siguiente manera:

Perfil	Cargo	Descripción de Funciones
Director/a Nacional	Director/a Nacional	<ul style="list-style-type: none"> - Generación de lineamientos y criterios generales. - Aprobación de políticas institucionales. - Evaluación del funcionamiento y efectividad del Sistema de Seguridad de la Información a intervalos planificados. - Asignación de recursos según las necesidades para la Gestión de Seguridad de la Información.
Comité de Seguridad de la Información	Integrado por los miembros del Comité de Riesgos (constituido mediante Resolución) más el Jefe/a de Soporte y Desarrollo Tecnológico y el Encargado Nacional de Seguridad de la Información	<ul style="list-style-type: none"> - Responsable de la implementación y mantención del Sistema de Seguridad de la Información. - Revisión periódica del Sistema de Seguridad de la Información, en particular de las responsabilidades del Encargado Nacional de Seguridad de la Información y Responsables de Dominios de Seguridad. - Monitorear el avance general de la implementación de Planes de Continuidad del Negocio. <p>Nota: corresponderá al Encargado Nacional de Seguridad de la Información, la coordinación de este Comité.</p>
Encargado/a Nacional de Seguridad de la Información	Encargado/a Nacional designado mediante la presente Resolución	<ul style="list-style-type: none"> - Asesorar al Director Nacional en materias relativas a la seguridad de los activos de información. - Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la institución y el control de su implementación y velar por su correcta aplicación. - Coordinar el análisis, levantamiento y documentación de los procesos de la Institución. - Coordinar la respuesta a incidentes que afecten a los activos de información institucionales. - 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. - Proponer la clasificación y procedimientos del caso para el procesamiento de activos de información. - Preparar instrucciones para la seguridad de los activos de información, respecto al uso seguro del correo electrónico, la asignación de identificadores, uso de redes y servicios en red. - Asesorar en la formulación de un plan de contingencia para asegurar la continuidad de operaciones críticas para el Servicio. - Coordinar el Comité de Seguridad de la Información, así como el respectivo Comité Operativo.

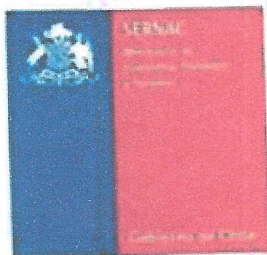


Perfil	Cargo	Descripción de Funciones
Aseguramiento del proceso	Auditoría Interna	<ul style="list-style-type: none"> Otorgar aseguramiento constante sobre el desarrollo del sistema de Seguridad de la Información. Retroalimentar sobre el cumplimiento de las recomendaciones y compromisos de los diferentes responsables que intervienen en el Sistema de Seguridad de la Información.
Funcionarios del SERNAC	Todos los Funcionarios del SERNAC	<ul style="list-style-type: none"> Dar cumplimiento a lo establecido en la presente Política y en las que la complementen y aplicarlo en su entorno laboral, a través de los procedimientos e instrucciones que determinen las áreas responsables, el encargado nacional y/o el Comité de Seguridad de la Información. Además, los funcionarios tienen la obligación de alertar de manera oportuna y adecuada a la jefatura directa, con copia al Comité de Seguridad de la Información, cualquier situación que atente contra lo establecido en esta política o pueda poner en riesgo la continuidad de los procesos. Corresponde también a los funcionarios implementar las medidas de prevención en su relacionamiento con sus respectivos clientes, especialmente en lo que diga relación con la confidencialidad de datos que se genere en virtud de dicha relación. Lo mismo para la debida reserva que deben tener los funcionarios/as respecto de los datos de que tomen conocimiento en el ejercicio de sus funciones. La referida obligación de reserva debe ser informada por el Servicio e incorporada en los contratos respectivos o en las políticas que correspondan.

Por su parte, considerando los dominios en materia de Seguridad de la Información, se establecen las siguientes responsabilidades por Dominio:

Dominio	Nombre de Dominio	Cargo
1	Política de Seguridad	Director/a Nacional
2	Organización de la Seguridad de la Información	Subdirector/a de Gestión y Territorio
3	Gestión de Activos	Encargado/a de Seguridad de la Información
4	Seguridad de Recursos Humanos	Jefatura del Dpto. de Gestión y Desarrollo de Personas
5	Seguridad Física y Ambiental	Jefatura del Dpto. de Administración y Finanzas
6	Gestión de comunicaciones y Operaciones	Jefatura del Dpto. de Soporte y Desarrollo Tecnológico.
7	Control de Acceso	Jefatura del Dpto. de Soporte y Desarrollo Tecnológico
8	Adquisición, Desarrollo y Mantenimiento de Sistemas	Jefatura del Dpto. de Soporte y Desarrollo Tecnológico





Dominio	Nombre de Dominio	Cargo
9	Gestión de Incidentes	Encargado/a de Seguridad de la Información
10	Gestión de Continuidad del Negocio	Subdirector/a de Gestión y Territorio
11	Cumplimiento	Encargado/a de Seguridad de la Información

V. Monitoreo y Revisión.

Con el fin de asegurar su vigencia, actualización y mejora continua, la presente Política será revisada al menos una vez por año, por parte del Comité de Seguridad de la Información, proponiendo a la Dirección Nacional, las mejoras a implementar.

VI. Relación con otras Políticas Institucionales.

La presente Política se aplicará de manera complementaria con las demás políticas internas y gubernamentales definidas para el Servicio, así como otros documentos pertinentes de Sernac. Toda la documentación que forme parte del Sistema de Seguridad de la Información, se desarrollará bajo los criterios, formatos y metodologías existentes en el marco del Sistema de Gestión de la Calidad Institucional, siendo de carácter complementario, el desarrollo del presente sistema.

VII. Definiciones y Normativa vigente.

Las definiciones relacionadas con la Seguridad de la Información, se encontrarán disponibles en la Documentación Técnica y Legal del Sistema, ubicada en el Sistema de Control Documental ISOtools o equivalente vigente.

2.- **CONSTITÚYASE** el Comité de Seguridad de la Información en conformidad al punto IV de la presente política.

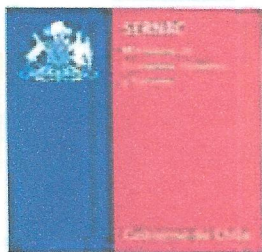
3.- **DESÍGNASE** como responsables de los dominios de seguridad, a los funcionarios que cumplan los cargos señalados en el punto IV de la presente política.

4.- **CONSTITÚYASE** el comité operativo de seguridad de la información, conformado por los responsables de dominios y el Encargado Nacional de Seguridad de la Información.

5.- **DESÍGNASE** como Encargado Nacional de Seguridad de la Información al Jefe/a de la Unidad de Soporte e Infraestructura del Departamento de Soporte y Desarrollo Tecnológico. En su ausencia, asumirá este rol el Jefe/a del Departamento.

6.- **ESTABLÉZCANSE** como funciones del Encargado/a Nacional de Seguridad de la Información, las señaladas para éste en el punto IV de la presente política.





7.- **DÉJASE** sin efecto lo establecido en la Resoluciones Exentas N° 910 y N° 911, ambas del 29-07-2011 y Resoluciones Exentas N° 1630 y N° 1631, ambas del 08-11-2012, y todas las anteriores que se hayan dictado en materia de Políticas de Seguridad de la Información, de este Servicio Nacional del Consumidor.

8.- **PUBLÍQUESE Y COMUNÍQUESE** la presente Política de Seguridad de la Información, a todos los funcionarios por los diversos medios institucionales (correo electrónico, intranet, web institucional, entre otros que se estimen pertinentes).

ANÓTESE Y COMUNÍQUESE.


ERNESTO MUÑOZ LAMARTINE
Director Nacional
Servicio Nacional del Consumidor

SERVICIO NACIONAL DEL CONSUMIDOR
DIRECTOR NACIONAL

SERVICIO NACIONAL DEL CONSUMIDOR
SUPERVISOR
EML/AMB/SG/amb
Distribución:
Todos los Departamentos y DRs

