Ministerio Secretaría General de Gobierno

Gobierno de Chile

APRUEBA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y SU RESUMEN, DEL MINISTERIO SECRETARÍA GENERAL DE GOBIERNO.

RESOLUCIÓN EXENTA N° 272/2376

SANTIAGO, 27 DIC 2017

VISTO:

Lo dispuesto en el D.F.L. N° 1-19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que Fija texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la Ley N° 19.880, establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado; en la Ley N° 19.032, de 1991, que Reorganiza el Ministerio Secretaría General de Gobierno; en el D.F.L. N° 1 del Ministerio Secretaría General de Gobierno, de 1992, que modifica la Organización del Ministerio Secretaría General de Gobierno; en el D.L. N° 1.028, de 1975, que Precisa atribuciones y deberes de los Subsecretarios de Estado; en la Ley N° 19.233, de 1993, que tipifica figuras penales relativas a la informática; en la Ley N° 19.799, de 2002, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma; en la Resolución Exenta N°272/1244 del 03 de septiembre de 2015; en Decreto Supremo N° 83, de 2014, del 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; en la Resolución Exenta N° 272/1557, de 2016, que aprueba Política de seguridad de la información del Ministerio Secretaría General de Gobierno; y en la Resolución Nº 1.600 de 2008, de la Contraloría General de la República y sus modificaciones; y

CONSIDERANDO:

1.- La relevancia que tiene en el ámbito de la información contar con una Política de Seguridad de la Información.

2.- La necesidad de relevar su vigencia mediante la actualización de dicha Política General de Seguridad de la Información y su Resumen.

RESUELVO:

1.- APRUÉBASE la presente actualización de la Política General de Seguridad de la Información y su Resumen, los que se adjuntan y forma parte integrante de este acto.

2.- DÉJESE SIN EFECTO la Resolución Exenta N° 272/1557, del 26 de octubre de 2016, que aprobó en carácter de resumen, la Política de Seguridad de la Información, mediante el anexo denominado "Política General de Seguridad de la Información".

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

OMAR JARA ARAVENA
Subsecretario General de Gobierno

AVD/HGM/SLLM/

Adjunta:
- Política General de Seguridad de la Información (26 páginas); y
- Resumen Política General de Seguridad de la Información (14 páginas);

Distribución:
- Gabinete Señora Ministra Secretaria General de Gobierno;
- Gabinete Señor Subsecretario General de Gobierno;
- División de Administración y Finanzas;
- Secretaría de Comunicaciones;
-Unidad de Asesoría Jurídica;
- Unidad de Planificación y Control de Gestión; y
- Central de Documentación.

	Norma Chilena NCh-ISO 27001:2013	
International Organization for Standardization	**Medio de Verificación de Control**	• A.05.01.01 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN • A.05.01.02 REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Código	POL-03-2016	
Versión:	0.2.6	
ELABORADO POR	**REVISADO POR**	**AUTORIZADO POR**
Jefe de Unidad de Informática	Encargado de Seguridad de la Información	Subsecretario Ministerio Secretaría General de Gobierno
FECHA	FECHA	FECHA
10/10/2017		
FIRMA	FIRMA	FIRMA

MINISTERIO SECRETARÍA GENERAL DE GOBIERNO

Subsecretaría General de Gobierno

Gobierno de Chile

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

1. INTRODUCCIÓN

El presente Documento "Política General de Seguridad de la Información", tiene por objeto reflejar el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional considerando los parámetros de calidad que la norma ISO 27001:2013 nos aporta, y establece el marco de referencia sobre el cual el Ministerio Secretaría General de Gobierno (MSGG) implementa y mantiene actualizado el Sistema de Seguridad de la Información, fijando las directrices y normas correspondientes para proteger sus recursos informáticos, en especial la información corporativa.

La siguiente definición permite orientar el uso de las tecnologías de información y comunicación (TIC), pues constituyen – a nuestro entender- uno de los principales instrumentos que apoyan la administración y gestión de las organizaciones, más aún –como es nuestro caso- se administran grandes volúmenes de información, los que aportan a la toma de decisiones y el desarrollo de nuestra institución. Tomando esta importancia pues aportan para cumplir objetivos globales o limitados en su alcance, pero requiriendo disponer de soluciones que aseguren la prestación de servicios eficaces y eficientes, tanto a destinatarios internos como externos a la organización.

Dado el alto impacto de una inadecuada administración de la información, se requiere disponer de los instrumentos para gestionar dentro de un marco de control y seguridad que procure el logro de los objetivos que se pretenden con su uso. Así mismo las posibilidades de interconectarse y de interoperar entre sistemas a través de redes, han abierto nuevos horizontes, a la vez que ha permitido la aparición de nuevas amenazas a los sistemas informatizados.

Lo anterior obliga a desarrollar la documentación, que permita disponer a los usuarios del MSGG los principales conceptos que se abordan en la Política General de Seguridad de la Información, por lo cual se ha elaborado un Resumen del presente documento.

Las directrices informáticas y particularmente las de seguridad de la información, constituyen las alarmas y compromisos compartidos en la organización, que le permiten actuar proactivamente ante situaciones que comprometen su integridad. Por tanto, deben constituir un proceso continuo y retroalimentado que observe el grado de consciencia respecto a métodos de acceso a la información, monitoreo de cumplimiento y renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.

2. *DECLARACIÓN INSTITUCIONAL*

El **Ministerio Secretaría General de Gobierno**, hace suyo e incorpora a su quehacer diario, un conjunto de políticas, normas y procedimientos tendientes a regular el uso, almacenamiento, acceso y distribución de sus activos informáticos.

Para llevar a cabo dicho compromiso, está implementando un Sistema de Seguridad de la Información (SGSI), el cual tiene como finalidad resguardar los activos informáticos, garantizando un alto nivel de continuidad operativa de sus procesos de negocio que contribuyan al cumplimiento de la misión y objetivos estratégicos de nuestro Servicio.

La información, directrices y alcances definidos en el presente documento, como también de aquellos relacionados al presente, como los que consignan normas y procedimientos de seguridad informática, son susceptibles de continuas mejoras mediante modificaciones que permitan mantenerlos vigentes de acuerdo a las condiciones requeridas por el Ministerio respecto a la seguridad de sus medios tecnológicos.

3. *ROLES Y RESPONSABILIDADES*

Cumpliendo con los objetivos de la norma ISO 27001:2013, se han definido los siguientes roles y responsabilidades en al ámbito de Seguridad de la Información:

3.1. Autoridad Superior del Servicio.

Subsecretario (a) General de Gobierno.
Responsable de aprobar la Política de Seguridad Informática y sus modificaciones, con la asistencia del Comité de Seguridad de la Información.

3.2. Comité de Seguridad de la Información.

El Comité de Seguridad de la Información, dispondrá y autorizará toda la documentación necesaria que permita y facilite el correcto funcionamiento del proceso de Seguridad de la Información, debiendo para lo mismo, reunirse en forma trimestral y/o en función de las contingencias que requieran su convocatoria. Dicha convocatoria será refrendada mediante la correspondiente Acta con las resoluciones pertinentes.

El Comité estará conformado por representantes de las diferentes áreas del Ministerio y/o los representantes que ellos designen para tales efectos.

Subsecretario Ministerio Secretaria General de Gobierno.
Jefe de la División de Administración y Finanzas.
Jefe de la División de Comunicación y Cultura.
Jefe de la División de Organizaciones Sociales.
Encargado de Seguridad y Confidencialidad de la Información, como Secretario Ejecutivo.

Esta instancia permite por esta vía difundir a las Jefaturas y funcionarios, las Políticas de Seguridad Informática, los procedimientos para implementarlas y las mejoras que se requieran en la materia.

Este Comité podrá autorizar la elaboración, revisión, actualización y publicación de Políticas específicas de Seguridad de la Información y formalizarlas mediante un Acta.

3.3. Encargado de Seguridad de la Información.

El Encargado de Seguridad es el Jefe(a) de la Unidad de Informática, y será nombrado por el Jefe (a) Superior del Servicio mediante Resolución. El Encargado desarrollará las siguientes tareas y responsabilidades:

a) Tener a su cargo la implementación de las Políticas de Seguridad Informática y velar por su correcta aplicación, en coordinación con el Comité de Seguridad de la Información del Ministerio.
b) Proponer al Comité referido, la respuesta a incidentes que afecten los activos informáticos institucionales, como también mejoras a las políticas, normas y procedimientos de seguridad informática.
c) Establecer canales de comunicación con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan conocer las tendencias, normas y métodos de seguridad implementados.
d) Actuar como Secretario Ejecutivo del Comité de Seguridad de la Información.

3.4. Usuarios.

Son las personas que usan los activos de información y los sistemas para su procesamiento. Son responsables de conocer y cumplir a cabalidad la Política de Seguridad de la Información, además de tener la obligación de reportar incidentes de seguridad.

4. POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

El Ministerio Secretaría General de Gobierno, basa su accionar en la automatización constante de sus procesos estratégicos, por lo que ha incorporado en su quehacer diario, tecnologías tales como, Internet, Intranet, Correo Electrónico, Sistemas de Información y diversas arquitecturas de Redes de Datos, lo que ha llevado a la repartición a depender, en gran medida, de ellas para realizar sus actividades diarias, lo que conlleva al riesgo de pérdida de la confidencialidad, integridad y disponibilidad de su información corporativa estratégica. Por consiguiente, la política de seguridad, se elabora con el fin de que tenga aplicación a largo plazo y guíe el desarrollo de normas o criterios más específicos de los recursos tecnológicos, constituyéndose en una declaración formal de principios generales de la organización en materia de información y alta tecnología.

En este sentido, la política de seguridad y, especialmente, lo relacionado con la seguridad de la información, surge como una herramienta organizacional para motivar y educar a cada uno de los integrantes del MSGG sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la institución desarrollarse y mantener un lugar preferente en el ámbito de sus competencias.

Lo anterior significa que el proponer o identificar directrices informáticas institucionales, requiere de laparticipación todas las instancias decisionales y operativas que componen la institución, como también del compromiso para aplicar, renovar y actualizar dicha políticas en función del dinámico ambiente en que se desenvuelven las organizaciones o instituciones modernas, por cuanto las políticas informáticas deben estar en función del propósito del Ministerio, así como de los objetivos que se desea alcanzar en la institución desde la perspectiva de las directrices tecnológicas.

Definición.

La política de seguridad de la información comprende un conjunto de directrices, normas y procedimientos documentados que regulan la forma en que se deben dirigir, proteger y distribuir los recursos informáticos de la organización para llevar a cabo los objetivos de seguridad de la misma. Entre los recursos informáticos de mayor trascendencia encontramos los Servidores, Sistemas de Procesamiento y Datos, Espacios de información compartida, equipamiento computacional y servicios de comunicación de datos.

Objetivos de la Política

- Proveer a los usuarios, funcionarios y autoridades superiores del MSGG, de las directrices, normas y procedimientos que se deben cumplir y utilizar para proteger los elementos de hardware y software de la plataforma tecnológica de servidores y comunicación de la institución, así como la información que es procesada y almacenada en éstos.
- Proteger los activos de información Institucionales frente a amenazas, internas o externas, sean ellas deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información que estos recursos generan.
- Mantener las Directrices de Seguridad del MSGG actualizadas, a efectos de asegurar su vigencia y nivel de eficacia.
- Implementar acciones conducentes a optimizar y actualizar las tareas cotidianas, por la vía de "Protocolos" que permitan transmitir adecuadamente el proceder en cada situación.

Directrices Generales.

- **Documento de Política.** El presente documento es un marco, amparado en la Norma Internacional ISO 27001-2013 (en particular al Control A.05.01.01 Políticas de Seguridad de la Información), que define directrices globales de uso de los recursos tecnológicos de la Institución, por lo tanto, la Unidad de Informática, deberá, dentro de este marco, acorde con la normativa legal vigente que se consigna en el numeral 6 del presente documento, definir los protocolos y procedimientos que permitan el buen uso de los servicios e infraestructura informática, como son los Servicios Telemáticos (correo electrónico, Web, multimedia, etc.), el buen uso de la infraestructura de redes y del acceso a Internet, acceso a servidores con datos de carácter personal e institucional, e Incidencias de Seguridad.

  Las distintas unidades organizacionales, podrán definir sus propias normas y procedimientos para el uso de los recursos informáticos que estén bajo su control, las cuales deberán ser congruentes con estas políticas y, además, con las normas y procedimientos de uso general que establezca la Unidad de Informática.
- **Difusión del Documento de Política.** La Política de Seguridad de la Información del MSGG, sus directrices asociadas y sus actualizaciones deben darse a conocer a todos los funcionarios y

terceros que utilicen los recursos informáticos institucionales, en soporte papel y/o a través de las herramientas técnicas que provee la plataforma informática y de comunicaciones en operación.

- **Revisión y Actualización de la Política.** Debido a la propia evolución de las tecnologías informáticas, eventuales amenazas a la seguridad, y de los cambios a las normativas en el Estado; es responsabilidad de la Unidad de Informática mantener, revisar, reformular y difundir; si así se requiere, **anualmente** la **política, normas y procedimientos,** y sus directrices asociadas, a la vez de revisar su aplicación institucional. Así como mantener registro anual de los mismos.

- **Excepciones a la Política.** Todas las excepciones a la política de seguridad de la Información, deben ser analizadas y autorizadas por la Autoridad Superior del Ministerio. Cuando el MSGG requiera utilizar infraestructuras de redes de organismos externos (como el caso de CGR, Registro Civil, Ministerio de Hacienda, Ministerio del Interior, otros), las políticas, normas y procedimientos de estas instituciones serán de aplicación en la red del MSGG.

4.1. Organización de la Seguridad de la Información.

Objetivos

- Administrar la seguridad de la información dentro del MSGG y establecer un marco normativo para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades en estas materias.
- Garantizar la aplicación de medidas de seguridad adecuadas en el acceso de terceros a la información institucional.

Directrices

- **Responsable de la Seguridad de la Información.** La orientación, dirección, autoridad y cumplimiento de las actividades de seguridad de la información están centralizadas, para toda la Institución, en la Subsecretaria General de Gobierno, quien deberá, si así lo estima, delegar formalmente mediante acto administrativo, estas responsabilidades en las instancias que determine.
- **Acuerdos de Confidencialidad.** Todos los funcionarios y terceros que tengan acceso a información clasificada como sensible, deben firmar cláusulas de protección de la confidencialidad o no divulgación de dicha información.

- **Contratos con Terceros.** La Dirección de Administración y Finanzas del MSGG, debe considerar en los contratos con terceros relacionados con las áreas de Informática y Comunicaciones una cláusula que identifique la responsabilidad del resguardo de la información y además la verificación de los antecedentes personales de aquellas personas contratadas.
- **Contacto con autoridades y grupos de interés especial.** Se deben mantener contactos apropiados con autoridades y grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.
- **Generar y administrar los Protocolos** como acciones conducentes a optimizar y actualizar las tareas cotidianas,

4.2. Activos asociados a la Información.

Objetivo

- Garantizar que los activos asociados a la información tengan un apropiado nivel de protección.
- Garantizar que las modificaciones de los elementos o activos que componen la plataforma tecnológica institucional, cumplen con las normas de seguridad establecidas.

Directrices

- **Inventario de los Activos**. Debe existir un registro general de todos los activos asociados a la información institucional, los que deben ser revisados y actualizados en forma periódica por quien corresponda, de acuerdo a la reglamentación vigente en el MSGG.
- **Clasificación de la Información**. La información debe ser clasificada y etiquetada de acuerdo a su valor, requisitos legales y grado crítico para el MSGG.
- **Incorporación, desvinculación, traslado y baja de Activos Tecnológicos**. Debe existir un proceso y/o procedimiento general que permita cumplir con los controles de seguridad que establecen los diferentes dominios para estos elementos tecnológicos, tanto para la incorporación como la baja de los activos que conforman las plataformas tecnológicas del MSGG, como también para el movimiento de ellos entre usuarios.
- **Generar y administrar los Protocolos** como acciones conducentes a optimizar y actualizar las tareas cotidianas,

4.3. Seguridad de los Recursos Humanos.

Objetivo

- Definir las responsabilidades en materias de seguridad informática, a partir de la etapa de reclutamiento de personal y verificar su cumplimiento durante el desempeño del individuo como funcionario.

Directrices

- **Antes del Empleo**. Los antecedentes de todos los candidatos al empleo, contratistas y terceros deben ser adecuadamente investigados, especialmente a aquellos que tendrán acceso a información sensible para la Institución.
- **Durante el Empleo**. Se debe concientizar a los funcionarios y terceras personas sobre la importancia de la aplicación de medidas de seguridad y uso correcto de los medios de procesamiento de información para minimizar los posibles riesgos de seguridad.
- **Cese del Empleo**. Se debe procurar que los funcionarios, contratistas o terceras personas que terminen su vínculo con el MSGG o cambien de Unidad Organizacional Interna, no pongan en peligro la integridad de la información institucional.
- **Generar y administrar los Protocolos** como acciones conducentes a optimizar y actualizar las tareas cotidianas,

4.4. Seguridad Física y Ambiental

Objetivos

- Prevenir e impedir accesos no autorizados a la información, daños e interferencia a las instalaciones de almacenamiento, procesamiento de información y comunicaciones institucionales.
- Proteger el equipamiento de procesamiento de información crítica institucional, ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados, considerando además los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático institucional

Directrices

- **Áreas Seguras**. Las Áreas que contengan información sensible o crítica deben contar con perímetros de seguridad adecuados y medidas de protección ante amenazas externas y ambientales.
- **Controles Físicos de Entrada**. Las áreas que contengan información sensible o crítica deben contar con los controles de entrada apropiados, que permitan el acceso solo a personal autorizado.
- **Trabajo en Áreas Seguras**. La Unidad de Informática debe diseñar e implementar protocolos adecuados para la realización de trabajo en áreas seguras.
- **Seguridad de los Equipos Computacionales**. El personal de las distintas Unidades Organizacionales del MSGG debe procurar las medidas adecuadas para proteger los equipos computacionales y de comunicación frente a amenazas, riesgos del ambiente externo y accesos no autorizados.
- **Computadores y Dispositivos de Almacenamiento Particulares**. Los funcionarios no deben usar en el interior de las instalaciones del MSGG equipos computacionales, medios de almacenamiento, periféricos o software particulares, sin la debida autorización de los Jefes de Unidad.

  El MSGG es el responsable de proveer y gestionar a través de los organismos correspondientes, el equipamiento tecnológico adecuado para el cumplimiento de la función operativa y administrativa.
- **Red de Datos**. El cableado de datos y de energía, además de los dispositivos de telecomunicaciones, que llevan la información o dan soporte a los servicios de información deben protegerse contra intercepción o daño.
- **Mantenimiento Preventivo**. La Jefatura de la Unidad de Informática debe definir periódicamente y de acuerdo a una calendarización anual, el mantenimiento preventivo del equipamiento computacional y de comunicaciones institucional.
- **Reutilización / Eliminación de Medios de Almacenamiento**. La Jefatura de la Unidad de Informática debe definir e implementar un procedimiento y registro para la eliminación segura de los datos de los medios de almacenamiento computacionales antes de ser reutilizados o desechados.
- **Generar y administrar los Protocolos** como acciones conducentes a optimizar y actualizar las tareas cotidianas,

4.5. Operaciones y Comunicaciones.

Objetivo

- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Directrices

- **Seguridad de la Red**. Las Redes de Datos deben contar con las medidas de seguridad adecuadas que permitan proteger la información en tránsito y disponibilidad de los servicios de red.
- **Acceso Remoto**. El acceso remoto a través de Internet a sistemas computacionales del MSGG debe ser otorgado únicamente a aquellos funcionarios o terceras personas que tengan una necesidad justificada. Dicha situación debe ser autorizada y monitoreada por la Jefatura de la Unidad de Informática.
- **Redes Inalámbricas**. Las redes inalámbricas utilizadas por el MSGG deben ser autorizadas por la Jefatura de la Unidad de Informática, la que informara a la autoridad que corresponda.
- **Protección contra Código Malicioso**. Se debe implementar controles de seguridad adecuados que permitan la detección, prevención y recuperación de la información ante código malicioso.
- **Copias de Seguridad**. La Jefatura de la Unidad de Informática será la responsable de establecer los procesos y procedimientos adecuados para respaldar periódicamente toda la información sensible o crítica del MSGG, residente en la plataforma tecnológica Institucional.
- **Gestión de Medios Removibles**. La Jefatura de la Unidad de Informática debe establecer procedimientos de seguridad para proteger los datos almacenados en medios removibles, ante divulgación no autorizada, modificación, eliminación y destrucción.
- **Seguridad de Dispositivos Móviles**. La Jefatura de la Unidad de Informática debe establecer los procedimientos de seguridad adecuados para proteger la información contenida en los equipos móviles.
- **Correo Electrónico**. Se debe proveer de un correo electrónico corporativo que permita a los funcionarios la comunicación electrónica entre las distintas entidades públicas o privadas, el que debe contar con las medidas de seguridad apropiadas.
- **Acceso a Internet**. El acceso a Internet en equipos institucionales, debe ser autorizado por la Jefatura de la Unidad de Informática, la que informará a la autoridad que corresponda.
- **Auditoría Informática**. Se debe generar y mantener registros de las actividades y eventos de seguridad de la información, en los diferentes sistemas informáticos institucionales durante un período definido.

- **Nombre de Dominios**. La autorización e inscripción de dominios a nombre del MSGG, es responsabilidad de la Jefatura de la Unidad de Informática, quien coordinará dicha acción con el Ministerio del Interior.
- **Generar y administrar los Protocolos** como acciones conducentes a optimizar y actualizar las tareas cotidianas.

4.6. Sistemas de Información.

Objetivos

- Asegurar la implementación de controles de seguridad, validación y auditoría de datos en el desarrollo de los sistemas de información
- Definir y documentar la metodología, normas y procedimientos que se aplicarán durante el ciclo de vida de los sistemas y aplicaciones y en la infraestructura base en la cual operan.

Directrices

- **Jefe Técnico de Proyecto**. La Jefatura de la Unidad de Informática debe nombrar formalmente un Jefe Técnico de Proyecto para los diferentes sistemas de información, con las debidas competencias, quienes entre sus principales funciones deben llevar un control completo y documentado de cada sistema informático a su cargo y base de datos correspondiente.
- **Adquisición de Sistemas de información**. Todo sistema de información adquirido a nombre del MSGG debe ser gestionado por la autoridad que corresponda, considerando los aspectos técnicos dados a conocer por la Jefatura de la Unidad de Informática.
- **Desarrollo de Sistemas de Información**. La Jefatura de la Unidad de Informática debe definir un lenguaje de programación estándar y robusto, que permita el desarrollo de sistemas de información y aplicaciones computacionales en forma segura, modular e integrable con los sistemas existentes al interior de la institución.
- **Ambientes de desarrollo, prueba y producción**. Se debe separar los ambientes de desarrollo, prueba y producción, para reducir los riesgos o cambios en el sistema operativo del servidor y/o proyecto de desarrollo de sistema.
- **Desarrollo de Bases de Datos**. La Jefatura de la Unidad de Informática debe definir un sistema de gestión de base de datos estándar que permita la administración de los datos de manera segura, auditable, clara y ordenada.

- **Documentación de Sistemas de Información y Base de Datos**. Todo sistema de información desarrollado por personal interno o externo, debe ser debidamente documentado, considerando el ciclo de vida de un sistema y la metodología estándar definida por la Unidad de Informática.
- **Análisis y requerimientos de seguridad**. La Jefatura de la Unidad de Informática es la responsable de que todo sistema de información institucional desarrollado en forma interna o externa cuente con los controles de seguridad adecuados, que permitan el funcionamiento correcto de éstos.
- **Mantenimiento y soporte de sistemas de información**. La Jefatura de la Unidad de Informática administrará cada uno de los sistemas de información y bases de datos institucionales correspondientes.
- **Uso de medidas Criptográficas.** La Jefatura de la Unidad de Informática debe proveer las herramientas adecuadas para la protección de la información que se considera en riesgo y para la cual otros controles no proveen una protección adecuada, lo anterior con la finalidad de proteger la confidencialidad, autenticidad y la integridad de la información.
- **Intranet Institucional**. La administración de los aspectos comunicacionales de la Intranet Institucional, es de responsabilidad de la autoridad designada por la Jefatura del Servicio y la Jefatura de la Unidad de Informática es la encargada de administrar los sistemas de información y servicios brindados a través de ella.
- **Portal Institucional**. La gestión de la labor institucional comunicacional a través de Internet, es de responsabilidad de la autoridad designada por la Jefatura del Servicio, destacando entre sus principales funciones el poner en marcha, desarrollar y administrar el portal institucional.
- **Generar y administrar los Protocolos** como acciones conducentes a optimizar y actualizar las tareas cotidianas,

4.7. Control de Acceso a la Información.

Objetivos

- Controlar el acceso lógico a los sistemas de información y bases de datos, implementando las medidas de seguridad en los accesos de usuarios.
- Controlar la seguridad en la conexión entre la red institucional y otras redes públicas o privadas.
- Controlar a los funcionarios y terceras personas respecto a la utilización de sus cuentas de accesos a los sistemas y equipamiento informático institucional (administración de claves).

Directrices

- **Control de Acceso**. Todo sistema de información, debe estar regulado por un sistema de control de acceso autorizado por la Jefatura de la Unidad de Informática.
- **Registro de Usuarios.** La Jefatura de la Unidad de Informática debe definir un procedimiento formal para la asignación de acceso y perfiles a los sistemas de información institucional o extra institucional.
- **Gestión de Privilegios.** La Jefatura de la Unidad de Informática debe restringir y controlar la asignación de privilegios de las cuentas de usuarios a los diferentes sistemas de información.
- **Cese de Cuentas.** La Jefatura de la Unidad de Informática debe proceder de forma inmediata a cancelar el acceso a los sistemas informáticos o áreas seguras cuando existan causales para ello.
- **Uso de Contraseñas.** Los usuarios de los sistemas informáticos institucionales, deben seguir buenas prácticas en la selección y uso de contraseñas, las que serán definidas, previamente, por la Unidad de Informática.
- **Equipos Desatendidos.** Los funcionarios que utilicen sistemas de información o computadores que contengan información sensible, no deben dejarlos desatendidos, sin los controles de seguridad adecuados.
- **Generar y administrar los Protocolos** como acciones conducentes a optimizar y actualizar las tareas cotidianas,

4.8. Incidentes de Seguridad de la Información.

Objetivo

- Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas informáticos sean comunicados de una manera que permita se realice una acción correctiva oportuna.
- Por lo anterior la Unidad de Informática, cuenta con una Política de Gestión de Incidentes de Seguridad, la cual define los procedimientos y responsabilidades para el manejo de un incidente de seguridad. Documento que estará en constante actualización.

Directrices

- **Reporte de eventos de seguridad**. La Jefatura de la Unidad de Informática debe establecer un procedimiento formal de comunicación y respuesta a incidentes.
- **Documentar Eventos de Seguridad**. La Jefatura de la Unidad de Informática debe definir un procedimiento que permita documentar y evaluar los incidentes de seguridad ocurridos al interior del MSGG.
- **Pruebas de Vulnerabilidades**. La Jefatura de la Unidad de Informática y otras instancias designadas por la Jefatura del Servicio, realizará pruebas para detectar debilidades y/o fallas de seguridad en los sistemas informáticos institucionales.
- **Almacenamiento de evidencia digital.** La Jefatura de la Unidad de Informática debe establecer procedimientos formales para el almacenamiento de evidencia digital ante un incidente de seguridad.
- **Generar y administrar los Protocolos** como acciones conducentes a optimizar y actualizar las tareas cotidianas,

4.9. Continuidad Operativa.

Objetivo

- Minimizar los efectos o trastornos ante fallas importantes o desastres en los sistemas informáticos, que puedan afectar la disponibilidad del servicio informático institucional y asegurar su reanudación oportuna.

Directriz

- **Plan de Continuidad Operativa**. La Jefatura de la Unidad de Informática debe desarrollar, implementar y mantener los planes de continuidad operativa ante situaciones que impidan el normal funcionamiento de los servicios informáticos institucionales críticos.
- **Generar y administrar los Protocolos** como acciones conducentes a optimizar y actualizar las tareas cotidianas,

4.10. Cumplimiento.

Objetivos

- Cumplir con las disposiciones legales y normativas internas a fin de evitar sanciones administrativas al Ministerio y/o al funcionario.
- Garantizar que los sistemas informáticos cumplan con la política, normas y procedimientos de seguridad del MSGG.

Directrices

- **Disposiciones Legales y Normativas Internas.** Los funcionarios y terceras personas deben velar por el cumplimiento de las disposiciones legales y normativa interna que dice relación con el uso y aplicabilidad de las tecnologías informáticas y de comunicación al interior del MSGG.
- **Procedimiento de Auditoría.** Anualmente, se deberá aplicar un procedimiento de auditoría interna, que permita visualizar el nivel de cumplimiento y efectividad de las directrices, normas y procedimientos de seguridad informática establecidas.
- **Medidas Disciplinarias**. El incumplimiento de las políticas, normas o procedimientos de seguridad informática, constituirá falta administrativa, que será sancionada de acuerdo a la normativa vigente.
- **Documentos de Seguridad Informática**. Toda la documentación referente a la Seguridad Informática Institucional, inclusive las políticas, normas y procedimientos de seguridad, son de uso interno.
- **Generar y administrar los Protocolos** como acciones conducentes a optimizar y actualizar las tareas cotidianas,

5. *ALCANCE DE LA POLITICA DE SEGURIDAD DE LA INFORMACION.*

- Estas directrices son aplicables a todos los recursos institucionales y a la totalidad de sus procesos relacionados con la utilización de las tecnologías informáticas y de comunicaciones, ya sean internos o externos vinculados al MSGG a través de contratos o acuerdos con terceros.

6. *MARCO LEGAL PARA LA POLITICA DE SEGURIDAD DE LA INFORMACION.*

Normativa legal vigente y aplicable:

- ✓ Ley 19.223, Delitos Informáticos
- ✓ Ley 17.336, Propiedad Intelectual
- ✓ Ley 19.927, Que modifica Código Penal, Código de Procedimiento Penal y Código de Procesal Penal en materias de delitos de Pornografía Infantil.
- ✓ Ley 19.628, Protección de la vida privada.
- ✓ Ley 19.799, Documentación Electrónica, Firma Electrónica y servicios de certificación de dicha firma.
- ✓ Ley 19.927, Pornografía Infantil.
- ✓ Ley 20.285, Acceso a Información Pública
- ✓ Ley 19.880, Procedimientos Administrativos que rigen los actos de los órganos de la administración del estado.
- ✓ Decreto 14 de 2014, establece disposiciones transitorias para decretos 77, 81, 100, 158, 271, derogados.
- ✓ Decreto 83 de 2004, Seguridad y Confidencialidad de documentos electrónicos.
- ✓ Decreto 93 de 2006, Minimizar efectos perjudiciales de los mensajes electrónicos masivos.
- ✓ Instructivo Presidencial N° 5 de 2001, Desarrollo de Gobierno Electrónico.
- ✓ Instructivo Presidencial N° 6 de 2005, Implementación y uso de firma electrónica.
- ✓ Instructivo Presidencial N° 8 de 2006, Transparencia activa y publicidad de la Información.

7. SERVICIOS Y ACTIVOS ASOCIADOS A LA INFORMACION.

Conforme el ámbito de la Política General de Seguridad de la Información, se establece como materia de atención, los siguientes servicios y activos de información:

7.1. Servicios Tecnológicos.

Consecuentemente con los objetivos y funciones básicas definidas en el Documento Técnico "Modelo Organizacional Orientado a Servicios" de la Unidad de Informática, los "Servicios Tecnológicos" que debe prestar a sus usuarios a efecto de cumplir a cabalidad con su cometido, son los que se establecen a continuación:

- Desarrollo y mantención de sistemas de información y aplicaciones computacionales corporativas.
- Acceso a los sistemas de información y bases de datos (internas / externas) necesarios para apoyar las tareas propias de las distintas unidades o áreas usuarias internas y externas.
- Soporte a los usuarios internos y externos en cuanto al uso y disponibilidad de la infraestructura y de los recursos de informática (acceso a Internet, bases de datos, sistemas de información, impresoras, correo, herramientas de productividad, etc.).
- Suministro, administración, mantención, reparación y renovación del equipamiento menor y herramientas de productividad personal del usuario final.
- Administración, mantención y renovación del equipamiento central.
- Servicios de comunicaciones y su administración (redes de datos, correo electrónico, Internet).
- Servicios de seguridad informática (actualización de antivirus, replicación y respaldo de información, protección de accesos, aplicaciones y datos, etc.).

7.2. Activos Asociados a la Información.

Los activos asociados a la información, en concordancia con lo señalado en el "Plan de Contingencia Institucional", corresponden a todos aquellos recursos o elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la organización, que la seguridad informática tiene como objetivo proteger:

- **Información.** Todos aquellos datos que se generan, capturan, procesan, gestionan, y transmiten en una organización, a través de su plataforma tecnológica institucional. En esta categoría se encuentran:

  - Bases de datos y archivos
  - Contratos y acuerdos
  - Documentación del sistema
  - Procedimientos operacionales o de soporte
  - Planes de contingencia y recuperación
  - Información resultante de auditorías internas y externas
  - Información general digitalizada y archivada

- **Sistemas de Información y/o Aplicaciones.** Todos aquellos sistemas de información y aplicaciones computacionales, que permiten administrar y gestionar la información institucional. La Información es el objeto de mayor valor para una organización, el objetivo es su resguardo, independientemente del lugar en donde se encuentre registrada, ya sea en un medio electrónico o en algún medio físico.
- **Personal.** En esta categoría se encuentran todas aquellas personas, tanto internas como externas a la Organización, que tengan acceso de una manera u otra a los activos de información de la organización, es decir, aquellas que utilizan la estructura tecnológica y de comunicaciones que procesa y almacena la información institucional.
- **Hardware:** Estos activos representan toda la infraestructura tecnológica institucional que brinda soporte a la información durante su uso, tránsito y almacenamiento, es decir:
  - Los elementos de hardware de comunicaciones y seguridad (Switch, Routers, Firewalls, etc.),
  - Servidores (Web, Base de Datos, Impresión)
  - Otros Servidores (Correo, listas, Backups, DNS, Video),
  - UPS,
  - Storage
  - Impresoras

- **Software:** Este grupo de activos contiene todos los programas de computadora que se utilizan para la automatización de procesos (acceso, lectura, tránsito y almacenamiento de la información), es decir:

- Los sistemas de información y aplicaciones computacionales,
- Los programas bases institucionales o software de sistemas,
- Los sistemas operativos y controladores de dispositivos,
- Los administradores de bases de datos y
- Las herramientas de desarrollo y utilidades.

❖ **Suministros:** En esta categoría encontramos:

- Red Eléctrica,
- Cableado de datos y voz
- Enlaces Internet y Punto a Punto.

❖ **Instalaciones Físicas:** En esta categoría encontramos:

- La Sala de Servidores Central (Datacenter),
- Sala de Servidores de Contingencia(Backups Remoto),
- Sala de Edición de Video,
- Salas de Impresión,
- En general, lugares en los que se alojan y utilizan los sistemas deinformación.
-

❖ **Equipamiento auxiliar:** En esta categoría pasan a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos:

- Climatización.
- Sistema de Detección y control de Incendios
- Destrucción de datos
- Sistema de Monitoreo
- Control de acceso

8. TERMINOS Y DEFINICIONES.

En la siguiente tabla se relaciona y explican los principales términos utilizados en el presente documento:

Término	Definición
Activo de Información	Recurso o elemento de la plataforma tecnológica, o relacionado con ella, que participa en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información, necesario para que la organización del MSGG funcione correctamente y alcance los objetivos propuestos.
Amenaza	Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
Análisis de Riesgo	Proceso de identificación, control y minimización o eliminación de los riesgos de seguridad que pueden afectar los sistemas de información.
Ataque	Evento, exitoso o no, que atenta contra el buen funcionamiento del sistema.
Aplicaciones	Programa informático que permite a un usuario utilizar una computadora con un fin específico.
Auditoría	Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del sistema informático de una organización
Base de Datos	Conjunto de Información que está almacenada en forma sistemática, de manera tal que los datos que la conforman puedan ser utilizados en forma fragmentada cuando sea necesario.
Contingencia	Interrupción de la capacidad de acceso a la información y procesamiento de la misma, necesaria para la operación normal de la organización
Control	Las políticas, los procedimientos, las prácticas y las estructuras organizacionales concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
Código Malicioso	Programas destinados a perjudicar o a hacer un uso ilicito de los recursos de los sistemas. Es instalado (por desconocimiento o maldad) en el computador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser por ejemplo, un virus informático, una bomba lógica, un programa espia o Spyware, etc.
Directrices	Líneas de acción relacionadas con la seguridad de la información. **Ejemplo: "La presente directriz tiene por objetivo garantizar que el acceso a la información del MSGG se realizará exclusivamente por el personal autorizado".**
Dispositivos de Almacenamiento	Tecnología de hardware que permite almacenar diferentes tipo de información digital, como por ejemplo: Pendrive, CDs, DVDs, Discos Duros externos, Cintas Magnéticas de respaldo, etc.
Documento	Instrumento que facilita el registro de la información necesaria para realizar los procedimientos y/o para dejar evidencia de que éste se realizó de acuerdo a los lineamientos previamente establecidos.
Dominios ISO	Formas de estructurar documentalmente las directrices, normas y procedimientos relacionados con la seguridad.
Encriptación	Es el proceso mediante el cual cierta información o "texto plano" es cifrado de

	forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación.
Evaluación de Riesgo	Cuantificación de las amenazas de impactar y vulnerar la información y las instalaciones de procesamiento de la información y la probabilidad de ocurrencia.
Impacto	Consecuencia al materializarse una amenaza.
Incidente	Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Instrucciones Técnicas	Acciones detalladas para aspectos concretos a cumplir en la ejecución de un procedimiento o las tareas a considerar cuando se ejecuta un procedimiento. **Ejemplo de Instrucción Técnica para el Alta de Usuarios en entornos Microsoft Windows:** **"Esta instrucción debe detallar el siguiente aspecto: Configuración inicial de la contraseña, indicando que el usuario en el primer inicio deberá forzosamente cambiar la contraseña por defecto para garantizar la confidencialidad de la misma".**
Instrucciones de Uso	Establecen las normas de comportamiento que deben cumplir los usuarios en el uso de los activos informáticos. **Ejemplo de Instrucciones de Uso de Contraseñas:** **"Mantenga su contraseña en secreto: La contraseña es algo muy serio y no debe ser proporcionada a nadie bajo ningún concepto. Cualquier persona que pueda conocerla tiene la posibilidad de suplantarle en cualquier momento, con los problemas que eso le puede ocasionar a usted y no a él."**
Inventario de Activos	Lista de todos aquellos recursos (hardware, de información, software, documentos, servicios, persona, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por lo tanto ser protegidos de potenciales riesgos.
ISO 27001	Código de buenas prácticas en gestión de la seguridad de la información
Norma	Disposición de carácter obligatorio, especifico y preciso que persigue un fin determinado enmarcado dentro de una política. Establece los requisitos que es necesario garantizar. **Ejemplo:** **"Se limitan a tres el número de reintentos sucesivos sin éxito en la introducción de contraseña para bloquear a un usuario".**
Plan de Continuidad del negocio	Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro
Política	Conjunto de lineamientos o directrices relacionadas con la seguridad informática. Establece los objetivos a cumplir.
Procedimiento	Módulos homogéneos que especifican y detallan un proceso, los cuales conforman un conjunto ordenado de operaciones o actividades determinadas secuencialmente en relación con los responsables de la ejecución, que deben cumplir políticas y normas establecidas señalando la duración y el flujo de documentos. Detalla los procesos a seguir para cumplir con los objetivos y las normas. **Ejemplo:** **"Debe documentarse el procedimiento de alta, modificación y baja de usuarios"**
Proceso	Un proceso se puede definir como una serie de actividades, acciones o eventos organizados e interrelacionados, orientadas a obtener un resultado específico y predeterminado, como consecuencia del valor

	agregado que aporta cada una de las fases que se llevan a cabo en las diferentes etapas por los responsables que desarrollan las funciones de acuerdo con su estructura orgánica.
Redes	Equipos de Procesamiento de Datos, de comunicaciones y sistemas de información en una organización
Riesgo	Posibilidad de que se produzca un impacto determinado en un activo o en toda la organización.
Seguridad de la Información	Preservación de la confidencialidad, integridad y disponibilidad de la información.
Sistema Informático	Es el conjunto de partes interrelacionadas, hardware, software y recursos humanos que permite almacenar y procesar información. El hardware incluye computadoras estacionarias o portables, el Software incluye sistemas operativos, programas básicos, sistemas de información y aplicaciones computacionales, y por último, el soporte humano que incluye al personal técnico que crean y mantienen el sistema y a los usuarios que lo utilizan.
Telemática	Disciplina científica y tecnológica que surge de la evolución y fusión de las telecomunicaciones y la informática
Vulnerabilidad	Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
07/09/2016	0.1	Unidad de Informática	Creación del documento
19/10/2016	0.2	Unidad de Informática	Modificaciones al documento
10/10/2017	0.2.6	Unidad de Informática	Actualizaciones numeral 2 Declaración Institucional, numeral 3 Roles y Responsabilidades, numeral 4 Política General de Seguridad de la Información/Directrices Generales, numeral 6 Marco Legal.

	Norma Chilena NCh-ISO 27001:2013	
ISO International Organization for Standardization	**Medio de Verificación de Control**	• A.05.01.01 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN • A.05.01.02 REVISIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

RESUMEN POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION V0.2.6

Código	POL-03-2016	
Versión:	0.2.6	
ELABORADO POR	**REVISADO POR**	**AUTORIZADO POR**
Encargado de Gestión Unidad de Informática	Encargado de Seguridad de la Información	Subsecretario Ministerio Secretaría General de Gobierno
FECHA	FECHA	FECHA
10/10/2017		
FIRMA	FIRMA	FIRMA

MINISTERIO SECRETARÍA GENERAL DE GOBIERNO

Subsecretaría General de Gobierno

Gobierno de Chile

RESUMEN
POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

1. *DECLARACIÓN INSTITUCIONAL*

El Ministerio Secretaría General de Gobierno, hace suyo e incorpora a su quehacer diario, un conjunto de **políticas, normas y procedimientos** tendientes a regular el uso, almacenamiento, acceso y distribución de sus activos informáticos.

Para llevar a cabo dicho compromiso, está implementando un Sistema de Seguridad de la Información (SGSI), el cual tiene como finalidad resguardar los activos informáticos, garantizando un alto nivel de continuidad operativa de sus procesos de negocio, que contribuyan al cumplimiento de la misión y objetivos estratégicos de nuestro Servicio.

La información, directrices y alcances definidos en el presente documento, como también de aquellos relacionados al presente, como los que consignan normas y procedimientos de seguridad informática, son susceptibles de continuas mejoras mediante modificaciones que permitan mantenerlos vigentes de acuerdo a las condiciones requeridas por el Ministerio respecto a la seguridad de sus medios tecnológicos.

A objeto de contar con un documento que permita a los usuarios del MSGG, conocer los principales conceptos que se abordan en la Política General de Seguridad de la Información, se ha elaborado el presente Resumen de la Política General de Seguridad de la Información.

2. *ROLES Y RESPONSABILIDADES*

Cumpliendo con los objetivos de la norma ISO 27001:2013, se han definido los siguientes roles y responsabilidades en al ámbito de Seguridad de la Información:

a) Autoridad Superior del Servicio.

Subsecretario (a) General de Gobierno.
Responsable de aprobar la Política de Seguridad Informática y sus modificaciones, con la asistencia del Comité de Seguridad de la Información.

b) Comité de Seguridad de la Información.

El Comité de Seguridad de la Información, dispondrá y autorizará toda la documentación necesaria que permita y facilite el correcto funcionamiento del proceso de Seguridad de la Información, debiendo para lo mismo, reunirse en forma trimestral y/o en función de las contingencias que requieran su convocatoria. Dicha convocatoria será refrendada mediante la correspondiente Acta con las resoluciones pertinentes.

El Comité estará conformado por representantes de las diferentes áreas del Ministerio y/o los representantes que ellos designen para tales efectos.

Subsecretario Ministerio Secretaria General de Gobierno.
Jefe de la División de Administración y Finanzas.
Jefe de la División de Comunicación y Cultura.
Jefe de la División de Organizaciones Sociales.
Encargado de Seguridad y Confidencialidad de la Información, como Secretario Ejecutivo.

Este Comité podrá autorizar la elaboración, revisión, actualización y publicación de Políticas específicas de Seguridad de la Información y formalizarlas mediante un Acta.

c) Encargado de Seguridad y Confidencialidad de la Información.

El Encargado de Seguridad es el Jefe(a) de la Unidad de Informática, y será nombrado por el Jefe (a) Superior del Servicio mediante Resolución. El Encargado desarrollará las siguientes tareas y responsabilidades:

i. Tener a su cargo la implementación de las Políticas de Seguridad Informática y velar por su correcta aplicación, en coordinación con el Comité de Seguridad de la Información del Ministerio, en el MSGG.
ii. Proponer al Comité referido, la respuesta a incidentes que afecten los activos informáticos institucionales, como también mejoras a las políticas, normas y procedimientos de seguridad informática.
iii. Establecer canales de comunicación con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan conocer las tendencias, normas y métodos de seguridad implementados.
iv. Actuar como Secretario Ejecutivo del Comité de Seguridad de la Información.

3. POLITICA GENERAL DE SEGURIDAD DE LA INFORMACION

El Ministerio Secretaría General de Gobierno, basa su accionar en la automatización constante de sus procesos estratégicos, por lo que ha incorporado en su quehacer diario, tecnologías tales como, Internet, Intranet, Correo Electrónico, Sistemas de Información y diversas arquitecturas de Redes de Datos, lo que ha llevado a la repartición a depender, en gran medida, de ellas para realizar sus actividades diarias, lo que conlleva el riesgo de pérdida de la confidencialidad, integridad y disponibilidad de su información corporativa estratégica. Por consiguiente, la política de seguridad, se elabora con el fin de que tenga

aplicación a largo plazo y guíe el desarrollo de normas o criterios más específicos de los recursos tecnológicos, constituyéndose en una declaración formal de principios generales de la organización en materia de información y alta tecnología.

Lo anterior significa que el proponer o identificar directrices informáticas institucionales, requiere de la participación de todas las instancias decisionales y operativas de la institución, como también del compromiso para aplicar, renovar y actualizar dichas políticas en función del dinámico contexto en que se desenvuelven las organizaciones o instituciones modernas, por cuanto las políticas informáticas deben estar en función del propósito del Ministerio, así como de los objetivos que se desean alcanzar desde la perspectiva de las directrices tecnológicas.

Definición.

La política de seguridad de la información comprende un conjunto de **directrices, normas y procedimientos** documentados que regulan la forma en que se deben dirigir, proteger y distribuir los recursos informáticos de la organización para llevar a cabo los objetivos de seguridad de la misma. Entre los recursos informáticos de mayor trascendencia encontramos: Servidores, Sistemas de Procesamiento y Datos, Espacios de información compartida, equipamiento computacional y servicios de comunicación de datos.

Objetivos de la Política

- Proveer a los usuarios, funcionarios y autoridades superiores del MSGG, las **directrices, normas y procedimientos** que se deben cumplir y utilizar para proteger los elementos de hardware y software de la plataforma tecnológica de servidores y comunicación de la institución, así como la información que es procesada y almacenada en éstos.
- Proteger los **activos de información** Institucionales frente a amenazas, internas o externas, sean ellas deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información que estos recursos generan.
- **Mantener actualizadas** las Directrices de Seguridad del MSGG, a efectos de asegurar su vigencia y nivel de eficacia.

- Implementar acciones conducentes a optimizar y actualizar las tareas cotidianas, de **normas y procedimientos,** por la vía de "Protocolos - Operativos", que permitan transmitir adecuadamente el proceder en cada situación.

Directrices Generales.

Para el desarrollo del presente documento, y en cumplimiento a lo establecido en el marco legal vigente, en particular lo señalado por la Norma Internacional ISO 27001-2013 (Control A.05.01.01 Políticas de Seguridad de la Información), que es la principal norma a nivel internacional y la de mayor aplicación respecto a la evaluación, implementación y certificación de medidas de seguridad aplicadas a las tecnologías de la información y comunicación, y la normativa legal vigente que se consigna en el numeral 5 del presente documento, para consideración se definen las siguientes directrices generales:

- **Documento de Política.** El presente documento es un marco que define directrices globales de uso de los recursos tecnológicos de la Institución, por lo tanto la Unidad de Informática, deberá dentro de este marco, definir las **normas y procedimientos** que por la vía de "Protocolos - Operativos", que permitan el buen uso de los servicios e infraestructura informática.

- **Difusión del Documento de Política.** La Política de Seguridad de la Información del MSGG, sus **normas y procedimientos**; así como sus actualizaciones deben darse a conocer a todos los funcionarios y terceros que utilicen los recursos informáticos institucionales, por medio de los canales regulares que permitan o favorezcan el proceso de su difusión (como correo electrónico, publicación en intranet o sitio web institucional).

- **Revisión y Actualización de la Política.** Debido a la propia evolución de las tecnologías informáticas, eventuales amenazas a la seguridad, y de los cambios a las normativas en el Estado; es responsabilidad de la Unidad de Informática mantener, revisar, reformular y difundir; si así se requiere, **anualmente** la **política, normas y procedimientos,** y sus directrices asociadas, verificando su debida aplicación institucional y el registro documental correspondiente.

- **Excepciones a la Política.** Todas las excepciones a la política de seguridad de la Información, deben ser analizadas y autorizadas por la Autoridad Superior del Ministerio. Cuando el MSGG requiera

- Implementar acciones conducentes a optimizar y actualizar las tareas cotidianas, de **normas y procedimientos,** por la vía de "Protocolos - Operativos", que permitan transmitir adecuadamente el proceder en cada situación.

Directrices Generales.

Para el desarrollo del presente documento, y en cumplimiento a lo establecido en el marco legal vigente, en particular lo señalado por la Norma Internacional ISO 27001-2013 (Control A.05.01.01 Políticas de Seguridad de la Información), que es la principal norma a nivel internacional y la de mayor aplicación respecto a la evaluación, implementación y certificación de medidas de seguridad aplicadas a las tecnologías de la información y comunicación, y la normativa legal vigente que se consigna en el numeral 5 del presente documento, para consideración se definen las siguientes directrices generales:

- **Documento de Política.** El presente documento es un marco que define directrices globales de uso de los recursos tecnológicos de la Institución, por lo tanto la Unidad de Informática, deberá dentro de este marco, definir las **normas y procedimientos** que por la vía de "Protocolos - Operativos", que permitan el buen uso de los servicios e infraestructura informática.

- **Difusión del Documento de Política.** La Política de Seguridad de la Información del MSGG, sus **normas y procedimientos**; así como sus actualizaciones deben darse a conocer a todos los funcionarios y terceros que utilicen los recursos informáticos institucionales, por medio de los canales regulares que permitan o favorezcan el proceso de su difusión (como correo electrónico, publicación en intranet o sitio web institucional).

- **Revisión y Actualización de la Política.** Debido a la propia evolución de las tecnologías informáticas, eventuales amenazas a la seguridad, y de los cambios a las normativas en el Estado; es responsabilidad de la Unidad de Informática mantener, revisar, reformular y difundir; si así se requiere, **anualmente la política, normas y procedimientos,** y sus directrices asociadas, verificando su debida aplicación institucional y el registro documental correspondiente.

- **Excepciones a la Política.** Todas las excepciones a la política de seguridad de la Información, deben ser analizadas y autorizadas por la Autoridad Superior del Ministerio. Cuando el MSGG requiera

utilizar infraestructuras de redes de organismos externos (como el caso de CGR, Registro Civil, Ministerio de Hacienda, Ministerio del Interior, otros), las políticas, normas y procedimientos de estas instituciones serán de aplicación obligada en la red del MSGG.

- **Contingencias.** La utilización diaria de la tecnología, podría generar situaciones que afecten el normal funcionamiento de las comunicaciones e información; por ello se dispondrá de un Plan de Contingencia que permita minimizar los efectos adversos al normal funcionamiento.

Dicho lo anterior, las siguientes diez (10) áreas buscan cubrir los puntos de atención prioritarios que la **política, normas, procedimientos,** y sus directrices asociadas deben documentar en su diario quehacer.

Áreas

1. Organización de la Seguridad de la Información.

Objetivos

- Administrar la seguridad de la información dentro del MSGG y establecer un marco normativo para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades en estas materias.
- Garantizar la aplicación de medidas de seguridad adecuadas en el acceso de terceros a la información institucional.

2. Activos asociados a la Información.

Objetivo

- Garantizar que los activos asociados a la información tengan un apropiado nivel de protección.
- Garantizar que las modificaciones de los elementos o activos que componen la plataforma tecnológica institucional, cumplen con las normas de seguridad establecidas.

3. Seguridad de los Recursos Humanos.

Objetivo

- Definir las responsabilidades en materias de seguridad informática, a partir de la etapa de reclutamiento de personal y verificar su cumplimiento durante el desempeño del individuo como funcionario.

4. Seguridad Física y Ambiental

Objetivos

- Prevenir e impedir accesos no autorizados a la información, daños e interferencia a las instalaciones de almacenamiento, procesamiento de información y comunicaciones institucionales.
- Proteger el equipamiento de procesamiento de información crítica institucional, ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados, considerando además los factores medioambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático institucional, (humedad, temperaturas extremas, residuos nocivos, etc).

5. Operaciones y Comunicaciones.

Objetivo

- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

6. Sistemas de Información.

Objetivos

- Asegurar la implementación de controles de seguridad, validación y auditoría de datos en el desarrollo de los sistemas de información
- Definir y documentar la metodología, normas y procedimientos que se aplicarán durante el ciclo de vida de los sistemas, sus aplicaciones y la infraestructura base en la cual operan.

7. Control de Acceso a la Información.

Objetivos

- Controlar el acceso lógico a los sistemas de información y bases de datos por parte de los usuarios, implementando las respectivas medidas de seguridad.
- Controlar la seguridad en la conexión entre la red institucional y otras redes públicas o privadas.
- Controlar a los funcionarios y terceras personas respecto a la utilización de sus cuentas de accesos a los sistemas y equipamiento informático institucional, (administración de claves).

8. Incidentes de Seguridad de la Información.

Objetivo

- Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas informáticos, sean comunicados de forma tal que permita realizar en forma oportuna una acción correctiva.
- Contar con una Política de Gestión de Incidentes de Seguridad, la cual define los procedimientos y responsabilidades para el manejo de un incidente de seguridad de la información. Este documento estará en constante actualización de parte de la Unidad de Informática.
- Por lo anterior la Unidad de Informática, cuenta con una Política de Gestión de Incidentes de Seguridad, la cual define los procedimientos y responsabilidades para el manejo de un incidente de seguridad. Documento que estará en constante actualización.

9. Continuidad Operativa.

Objetivo

- Minimizar los efectos o trastornos que puedan afectar la disponibilidad del servicio informático institucional, asegurando de esta manera su oportuna o pronta reanudación operativa.

10. Cumplimiento.

Objetivos

- Cumplir con las disposiciones legales y normativas internas a fin de evitar eventuales sanciones administrativas al Ministerio y/o al funcionario.
- Garantizar que los sistemas informáticos cumplan con la política, normas y procedimientos de seguridad del MSGG.

4. ALCANCE DE LA POLITICA DE SEGURIDAD DE LA INFORMACION

Las directrices de la Política de Seguridad de la Información aplican a todos los recursos institucionales y a la totalidad de procesos relacionados con la utilización de las tecnologías informáticas y de comunicaciones, sean internas o externas, y vinculadas al MSGG a través de contratos o acuerdos realizados con terceros.

5. *MARCO LEGAL PARA LA POLITICA DE SEGURIDAD DE LA INFORMACION.*

Normativa legal vigente y aplicable:

- ✓ Ley 19.223, Delitos Informáticos
- ✓ Ley 17.336, Propiedad Intelectual
- ✓ Ley 19.927, Que modifica Código Penal, Código de Procedimiento Penal y Código de Procesal Penal en materias de delitos de Pornografía Infantil.
- ✓ Ley 19.628, Protección de la vida privada.
- ✓ Ley 19.799, Documentación Electrónica, Firma Electrónica y servicios de certificación de dicha firma.
- ✓ Ley 19.927, Pornografía Infantil.
- ✓ Ley 20.285, Acceso a Información Pública
- ✓ Ley 19.880, Procedimientos Administrativos que rigen los actos de los órganos de la administración del estado.
- ✓ Decreto 14 de 2014, establece disposiciones transitorias para decretos 77, 81, 100, 158, 271, derogados.
- ✓ Decreto 83 de 2004, Seguridad y Confidencialidad de documentos electrónicos.
- ✓ Decreto 93 de 2006, Minimizar efectos perjudiciales de los mensajes electrónicos masivos.
- ✓ Instructivo Presidencial N° 5 de 2001, Desarrollo de Gobierno Electrónico.
- ✓ Instructivo Presidencial N° 6 de 2005, Implementación y uso de firma electrónica.
- ✓ Instructivo Presidencial N° 8 de 2006, Transparencia activa y publicidad de la Información.

6. *SERVICIOS Y ACTIVOS ASOCIADOS A LA INFORMACION.*

Conforme el ámbito de la Política de Seguridad de la Información, se establece como materia de atención los siguientes servicios y activos de información:

a. Servicios Tecnológicos.

Consecuentemente con los objetivos y funciones básicas definidas en el Documento Técnico "Modelo Organizacional Orientado a Servicios" de la Unidad de Informática, los "Servicios Tecnológicos" que debe prestar a sus usuarios para cumplir a cabalidad con su cometido, son los que se establecen a continuación:

a) Desarrollo y mantención de sistemas de información y aplicaciones computacionales corporativas.
b) Acceso a los sistemas de información y bases de datos (internas / externas) necesarios para apoyar las tareas propias de las distintas unidades o áreas usuarias internas y externas.
c) Soporte a los usuarios internos y externos en cuanto al uso y disponibilidad de la infraestructura y de los recursos de informática (acceso a Internet, bases de datos, sistemas de información, impresoras, correo, herramientas de productividad, etc.).
d) Suministro, administración, mantención, reparación y renovación del equipamiento menor y herramientas de productividad personal del usuario final.
e) Administración, mantención y renovación del equipamiento central.
f) Servicios de comunicaciones y su administración (redes de datos, correo electrónico, Internet).
g) Servicios de seguridad informática (actualización de antivirus, replicación y respaldo de información, protección de accesos, aplicaciones y datos, etc.).

b. Activos Asociados a la Información.

Los activos asociados a la información, en concordancia con lo señalado en el "Plan de Contingencia Institucional", corresponden a todos aquellos recursos o elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la organización, que la seguridad informática tiene como objetivo proteger:

a) **Información.** Todos aquellos datos que se generan, capturan, procesan, gestionan, y transmiten en una organización, a través de su plataforma tecnológica institucional. En esta categoría se encuentran:
   - Bases de datos y archivos
   - Contratos y acuerdos
   - Documentación del sistema
   - Procedimientos operacionales o de soporte
   - Planes de contingencia y recuperación
   - Información resultante de auditorías internas y externas
   - Información general digitalizada y archivada

b) **Sistemas de Información y/o Aplicaciones.** Todos aquellos sistemas de información y aplicaciones computacionales, que permiten administrar y gestionar la información

institucional. La Información es el objeto de mayor valor para una organización, el objetivo es su resguardo, independientemente del lugar en donde se encuentre registrada, ya sea en un medio electrónico o en algún medio físico.

c) **Personal.** En esta categoría se encuentran todas aquellas personas, tanto internas como externas a la Organización, que tengan acceso de una manera u otra a los activos de información de la organización, es decir, aquellas que utilizan la estructura tecnológica y de comunicaciones que procesa y almacena la información institucional.

d) **Hardware:** Estos activos representan toda la infraestructura tecnológica institucional que brinda soporte a la información durante su uso, tránsito y almacenamiento, es decir:

- Hardware de comunicaciones y seguridad (Switch, Routers, Firewalls, etc.),
- Servidores (Web, Base de Datos, Impresión)
- Otros Servidores (Correo, listas, Backups, DNS, Video),
- UPS,
- Storage.

e) **Software:** Este grupo de activos contiene todos los programas de computadora que se utilizan para la automatización de procesos (acceso, lectura, tránsito y almacenamiento de la información), es decir:

- Los sistemas de información y aplicaciones computacionales,
- Los programas bases institucionales o software de sistemas,
- Los sistemas operativos y controladores de dispositivos,
- Los administradores de bases de datos y
- Las herramientas de desarrollo y utilidades.

f) **Suministros:** En esta categoría se encuentra:

- Red Eléctrica,
- Cableado de datos y voz
- Enlaces Internet y Punto a Punto.

g) **Instalaciones Físicas:** En esta categoría se encuentra:

- La Sala de Servidores Central (Datacenter),
- Sala de Servidores de Contingencia(Backups Remoto),

- Sala de Edición de Video,
- Salas de Impresión,
- En general, lugares en los que se alojan y utilizan los sistemas de información.

h) **Equipamiento auxiliar:** En esta categoría se encuentran todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos:

- Climatización.
- Sistema de Detección y control de Incendios
- Destrucción de datos
- Sistema de Monitoreo
- Control de acceso

7. *HISTORIAL DE MODIFICACIONES*

Fecha	Versión	Creado por	Descripción de la modificación
07/09/2016	01	Unidad	Creación del documento
19/10/2016	02	Unidad	Modificaciones al documento
04/07/2017	0.2.5	Area de Gestión	Actualización numeral 2 CSI.
10/10/2017	0.2.6	Area de Gestión	Actualización numeral 1 Declaración Institucional, numeral 2 C.S.I., numeral 3, Directrices Generales, Incorporación de nuevo numeral 4 sobre Alcance de la Política, Actualización numeral 5, Marco Legal.