APRUEBA POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA SUPERINTENDENCIA DEL MEDIO AMBIENTE

RESOLUCIÓN EXENTA Nº 1597

Santiago, 15 de septiembre de 2022

VISTOS: Lo dispuesto en el Decreto con Fuerza de Ley N°1/19.653, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Ley N° 19.880, que establece las Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; en la Ley Orgánica de la Superintendencia del Medio Ambiente, fijada en el artículo segundo de la ley N° 20.417, de 2010, que crea el Ministerio del Medio Ambiente, el Servicio de Evaluación Ambiental y la Superintendencia del Medio Ambiente, modificada por la Resolución Exenta N° 2124, del 30 de septiembre del 2021 que "Fija Organización Interna de la Superintendencia del Medio Ambiente"; en el Decreto con Fuerza de Ley N°29, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; en la ley N°19.799 sobre Documentos Electrónicos y Firma Electrónica; en el Decreto N°83 de 2004, del Ministerio Secretaría General de la Presidencia; en el Decreto Exento RA N° 118894/55/2022, de 18 de marzo de 2022, del Ministerio del Medio Ambiente , que fija el Orden de Subrogación del Superintendente del Medio Ambiente; en el Decreto con Fuerza de Ley N°3, de 11 de septiembre de 2010, del Ministerio Secretaría General de la Presidencia, que fija la Planta del Personal de la Superintendencia del Medio Ambiente y su Régimen de Remuneraciones; y en la Resolución N°6 y 7 de 2019 de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón, de las materias de personal que se indica, a partir de las cuales los actos que se individualizan quedarán sujetos a toma de razón y a controles de reemplazo cuando corresponda.

CONSIDERANDO:

1. Que, la Superintendencia del Medio Ambiente es el servicio público creado para ejecutar, organizar y coordinar el seguimiento y fiscalización de las Resoluciones de Calificación Ambiental, de las medidas de los Planes de Prevención y/o de Descontaminación Ambiental, del contenido de las Normas de Calidad Ambiental y Normas de Emisión, y de los Planes de Manejo, cuando corresponda, y de todos aquellos otros instrumentos de gestión ambiental que establezca la ley, así como imponer sanciones en caso que se constaten infracciones de su competencia.

2. Que, en razón de lo establecido en el Decreto N°89 de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba la norma técnica para los órganos de la Administración del Estadio sobre seguridad y confidencialidad de los documentos electrónicos, es menester dictar Políticas de Seguridad de la Información en la Superintendencia del Medio Ambiente.

3. Que, la NCh-ISO 27001:2013 dispone que "*la adopción del sistema de gestión de la seguridad de la información es una decisión estratégica para la organización. El establecimiento e implementación de un sistema de gestión de seguridad de la información de la organización está influenciada por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales utilizados y el tamaño y la estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo. El sistema de gestión de la seguridad de la información conserva la confidencialidad, integridad y disponibilidad de*

la información al aplicar un proceso de gestión de riesgo y la entrega confianza a las partes interesadas cuyos riesgos son gestionados de manera adecuada".

4. Que, adicionalmente, la misma norma indica que "*la organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, según los requerimientos de esa norma*".

5. Que, mediante sucesivos actos administrativos, este servicio ha aprobado y actualizado las políticas necesarias para implementar el sistema de seguridad de la información de la Superintendencia del Medio Ambiente, encontrándose vigentes las políticas y procedimientos establecidos mediante la Resolución Exenta N°1507, de fecha 30 de noviembre de 2018 y la Resolución Exenta N°1928, de fecha 24 de diciembre de 2019.

6. Que, mediante correo electrónico de fecha 2 de agosto de 2022, el Jefe de la División de Seguimiento e Información Ambiental solicitó la aprobación de la actualización de la "**Política General de Seguridad de la Información**", contenida en la Resolución Exenta N°1507 de 2018, y la adición de un nuevo procedimiento denominado "**Procedimiento de Administración del Sitio Público-Internet y Privado-Intranet de la Superintendencia del Medio Ambiente**", conforme a los acuerdos a que arribó el Comité de Seguridad de la Información de la Superintendencia del Medio Ambiente durante su última sesión realizada con fecha 29 de junio del año 2022.

7. Que, en virtud de lo expuesto, se procede a resolver lo siguiente:

RESOLUCIÓN:

1º. APRUÉBASE la actualización del documento denominado "**Política General de Seguridad de la Información**", elaborado por la División de Seguimiento e Información Ambiental, reemplazando la contenida en la Resolución Exenta N°1507 de 2018, por cuyo texto que es el siguiente:

"POLÍTICA GENERAL DE
SEGURIDAD DE LA INFORMACIÓN

Elaborado por:	Aprobado por:	Versión
Cristián Cortés Correa División de Seguimiento e Información Ambiental	Comité de Seguridad de la Información	Junio 2022

Control de versiones:

N° Revisión	Fecha Aprobación	Motivo de la Revisión	Autor
01	Mayo 2011	Elaboración inicial	Pablo Quintana – Encargado Sistemas TI
02	Enero 2012	Corrección de contenido	Pablo Quintana – Encargado Sistemas TI
03	Mayo 2013	Corrección de contenido	Marco Bassaletti – Encargado Unidad TI
04	Octubre 2014	Corrección de contenido	Marco Bassaletti – Encargado Unidad TI
05	Noviembre 2017	Ajuste de formatos de acuerdo a lo instruido por la Red de Expertos del PMG-SSI 2017	Sebastián Elgueta – Jefe de Departamento de Gestión de la Información
06	Noviembre 2018	Ajuste de formatos de acuerdo a lo instruido por la Red de Expertos del PMG-SSI 2018	Sebastián Elgueta – Jefe de Departamento de Gestión de la Información
07	Junio 2022	Actualización	Cristián Cortés Correa – Jefatura de División Seguimiento e Información Ambiental

1. Declaración Institucional

La Superintendencia del Medio Ambiente, en adelante, SMA, promueve y apoya activamente las acciones que permitan mantener un alto nivel de seguridad de la información, definida ésta como: "la preservación de la confidencialidad, integridad y disponibilidad de los activos de información, necesarios para alcanzar los objetivos de la organización", dado que los activos de información poseen valor para la organización, por lo que deben ser protegidos adecuadamente a fin de que permitan cumplir la misión institucional.

Según lo expuesto, la SMA se compromete a desarrollar y ejecutar un plan de acción de mejora continua de manera de asegurar una adecuada gestión de la seguridad de la información en sus diferentes ámbitos de aplicación, según lo dispuesto en la Norma Chilena de Seguridad de la Información y otras normativas vigentes relacionadas como la Modernización del Estado, el Gobierno electrónico, la Transparencia y Acceso a la Información Pública, de Protección a la Vida Privada y de Datos Personales, Procedimientos Administrativos, entre otras.

La presente Política General de Seguridad de la Información, define las directrices, objetivos, alcances esenciales para la custodia y el uso de los activos de información y de los bienes asociados a su tratamiento, velando por su disponibilidad, confidencialidad e integridad, acorde a la normativa legal y reglamentaria vigente.

2. Importancia de la Política General de Seguridad de la Información

La importancia de la Política de Seguridad de la Información se expresa en los siguientes principios:

- Se reconoce la información como un activo, valioso y fundamental para la institución, que debe ser administrado con igual atención que el resto de los activos de la institución.
- Se define como Seguridad de la Información, toda acción que busque proteger la integridad, confidencialidad y disponibilidad de los activos de información institucionales.
- Se reconoce la seguridad de la información como un atributo necesario de los servicios ofrecidos por la institución.
- Los activos de información deben ser protegidos adecuadamente
- La institución incorpora en sus políticas de seguridad de información los controles y resguardos necesarios para cumplir con la normativa relacionada con la reserva y privacidad de la información.
- La institución reconoce el compromiso de toda la organización de cautelar y velar por la confidencialidad y reserva de la información que las instituciones, las empresas, las personas naturales y sus Funcionarios/as le han proporcionado u obtenido en el ejercicio de sus funciones, y también a proporcionar la disponibilidad de acceso a esta información.
- La seguridad de la información y de los bienes asociados a su manejo, es responsabilidad de todos los/as funcionarios/as de la SMA y terceros independientemente del cargo o funciones que desempeñen.
- La información sujeta a confidencialidad o reserva, de acuerdo con el marco legal vigente, no debe quedar disponible a personas o entidades externas, salvo en las situaciones y formas expresamente establecidas en las normas vigentes y con controles que garanticen su protección.

3. Objetivo de la Política General de Seguridad de la Información

Proteger y preservar la confidencialidad, integridad y disponibilidad de la información de la SMA, en concordancia con las definiciones estratégicas y la normativa vigente.

La política de seguridad de la información en la Superintendencia del Medio Ambiente tiene como principales objetivos:

- Establecer una estructura y gobierno que permita realizar una gestión de riesgo de seguridad de la información eficaz y eficiente, con una clara definición de los roles y responsabilidades.
- Vigilar que los medios de procesamiento y/o conservación de información sensible, cuenten con medidas de protección física y tecnológica que eviten el acceso y/o fuga y/o utilización indebida por cualquier persona, asimismo que las medidas que se implementen sean las adecuadas al nivel de riesgo de la información.
- Implementar y propender al cumplimiento de las políticas generales y específicas, normas, procedimientos, prácticas y estándares referentes a la seguridad de la información.
- Clasificar la información según su grado de sensibilidad e implementar mecanismos de seguridad adecuados a dicha categoría
- Realizar difusión permanente de las Directrices de Seguridad de la Información, con el objeto de sensibilizar a todos los usuarios de la Superintendencia del Medio Ambiente, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes y otros, en el cumplimiento de las medidas de seguridad establecidas.
- Revisar, monitorear, auditar y mejorar continuamente las directrices de seguridad que garanticen el mantenimiento de los niveles de seguridad requeridos.
- Reducir de manera eficaz y eficiente la frecuencia e impacto de los problemas e incidentes

de seguridad de la información y tecnología, a través de la adopción de mejores prácticas y metodologías.

- Destinar los recursos necesarios para desarrollar todas las medidas de seguridad que se determinen.

4. Alcance de la Política de Seguridad de la Información

La Política General de Seguridad de la Información se aplicará a todos los activos de información, independientemente de su soporte o almacenamiento, de los sistemas que lo procesen o de los métodos de transporte utilizados (base de datos, respaldos magnéticos, información impresa, internet y otros) y las personas que tengan acceso, manipulen o utilicen dichos activos en el cumplimiento de sus labores.

Los ámbitos de control, o dominios de seguridad de la información, especificados en la NCh-ISO 27001.Of2013 y NCh-ISO 27002.Of2013 a los que aplica la política, son los siguientes:

A.05.01.01 – Conjunto de políticas para la seguridad de la información.
A.05.01.02 - Revisión de las políticas para la seguridad de la información.

5. Roles y Responsabilidades

a) **Comité de Seguridad de la Información:** deberá proponer las medidas de seguridad destinadas a proteger y preservar los activos de información de la institución. Además, es el encargado de aprobar las Políticas de Seguridad de la Información.

b) **Encargado/a de Seguridad de la Información**: deberá, entre otras materias, coordinar la implantación y efectiva aplicación de las políticas de seguridad que se definan, y adicionalmente aprobar los Procedimientos que se generen dentro de la implementación del Sistema de Seguridad de la Información. Estos serán a su vez presentados al Comité de Seguridad de la Información para su difusión.

c) **Funcionarios/as y terceros relacionados al Servicio**: deberán acceder exclusivamente a la información que sea necesaria para cumplir sus labores y tendrán la obligación de notificar cualquier actividad o situación que contravenga estos lineamientos. Se entenderá por "terceros" a todos aquellos que, no siendo funcionarios de planta o a contrata, tengan acceso a activos de información del Servicio, incluidos los empleados y representantes de las personas naturales o jurídicas con quienes el Servicio mantenga algún tipo de relación.

Consecuente con lo anterior, los terceros deberán conocer y acatar la presente política y las que de ésta se desprendan, lo que quedará expresamente consignado en los respectivos contratos o acuerdos de servicio.

6. Medios de Difusión

La Política General de Seguridad de la Información, así como las políticas que se desprendan de ella, se difundirán a través de la intranet del Servicio, de su página web y boletín, según corresponda.

La responsabilidad de la difusión de la Política General de Seguridad será de responsabilidad del Encargado de Seguridad de la Información.

7. De la Revisión de esta Política

La Política General, las políticas específicas que de ella se desprendan y los procesos que las soporten, deberán ser revisados por lo menos una vez cada dos años o ante cualquier cambio significativo de tecnología, personal o evento que amerite su reevaluación para asegurar su continuidad, idoneidad, eficiencia y efectividad.

8. Evaluación del cumplimiento de la política

Las normas y políticas sobre Seguridad de la Información serán debidamente controladas y auditadas en su cumplimiento por las unidades correspondientes de la institución cada 2 años.

9. Sanciones

Las faltas incurridas en el cumplimiento de las obligaciones y deberes establecidos en la Política General de Seguridad de la Información y en las políticas específicas que la acompañen, por parte de los funcionarios, se considerarán como un incumplimiento de las obligaciones funcionarias contempladas en el artículo 61 del D.F.L. 29/2014 que fija el texto refundido, coordinado y sistematizado de la Ley 18.834, Estatuto Administrativo, y podrán dar origen a procesos administrativos disciplinarios, ya sea investigación sumaria o sumario administrativo.

Lo anterior, con independencia de las responsabilidades civiles o penales que pudiera acarrear alguna infracción de estas normas o sus consecuencias.

En cuanto al personal que preste servicios a honorarios, estará sujeto a cláusulas de confidencialidad y apego a estas disposiciones, las cuales formarán parte de su respectivo convenio de prestación de servicios. Su incumplimiento se considerará como incumplimiento del contrato pudiendo implicar el término anticipado e inmediato de éste, siéndoles, además, plenamente aplicables las responsabilidades civiles o penales que pudiera acarrear alguna infracción a estas normas o sus consecuencias.

Del mismo modo, se perseguirán las responsabilidades civiles o penales que pudieran acarrear alguna infracción a estas normas, o sus consecuencias, por parte de proveedores u otros prestadores de servicios (contratistas y usuarios de terceros), respecto de los cuales deberán considerarse medidas de información y suscripción.

10. Principios de confidencialidad

Toda la información y documentación electrónica que genera, y procesa la SMA debe ser tratada desde el punto de vista de la confidencialidad, de acuerdo con la normativa de la Ley Nº 20.285 y el reglamento establecido DS Nº 13, de 2009, del Ministerio Secretaría General de la Presidencia, sobre el acceso a la información pública.

Además, deberá ser considerado lo establecido en la ley orgánica de la SMA, respecto de los registros públicos de sanciones y los expedientes de los procesos de fiscalización y sanción.

11. Glosario

Para los propósitos de esta Política, las siguientes palabras se entenderán en el sentido que a continuación se indica:

a) Activo: todo aquello que tenga valor para la organización. Para el ámbito de seguridad de la información, se puede clasificar en:

- Activos de Información: Los Activos de Información corresponden a todos aquellos elementos relevantes en la producción, procesamiento, emisión, almacenamiento,

comunicación, visualización y recuperación de información de valor para la institución. De esta forma podemos distinguir 3 niveles básicos de activos de información:

- La 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 que tienen el conocimiento de los procesos institucionales.
- Activos de Software: Constituidos por las Aplicaciones de software, Software de sistemas y, Herramientas de desarrollo y utilidades.
- Activos Físicos: Constituidos por el Equipamiento computacional, Equipamiento de comunicaciones, Medios móviles y otros equipamientos.
- Servicios: Servicios de computación y comunicaciones. Utilidades generales (ej. electricidad, luz, aire acondicionado, etc.)
- Personas: Constituidos por los usuarios, que utilizan la estructura tecnológica, el área de comunicaciones y que gestionan la información.
- Intangibles: Constituidos por los activos referidos a la reputación e imagen de la institución.

b) **Amenaza**: Una causa potencial de un incidente no-deseado, el cual puede derivar en daño a un sistema u organización.

c) **Control:** Medios para manejar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas, o estructuras de la organización, que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

d) **Confidencialidad**: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. La información podrá ser:

- Información Pública: En virtud del principio de transparencia de la función pública, los actos y resoluciones de los órganos de la Administración del Estado, sus fundamentos, los documentos que les sirvan de sustento o complemento directo y esencial, y los procedimientos que se utilicen para su dictación son públicos, salvo las excepciones que establece la ley N° 20.285 en su artículo 21° y las previstas en otras leyes de quórum calificado.
- Información de Uso Interno: Aquella información cuyo conocimiento está circunscrito a las personas de la organización, sean de planta o contrata.
- Información reservada: Aquella información confidencial, que está circunscrita únicamente a las personas de la organización que la deben conocer, de conformidad al marco de sus atribuciones y/o funciones, en el ámbito de la División, Departamento, Sección, Oficina o área que corresponde.

e) **Corta Fuegos** (*Firewall*, en inglés): Es un sistema diseñado para prevenir el acceso no autorizado hacia o desde una red privada.

f) **Debilidad**: Deficiencia de uno o de un grupo de activos, los que pueden ser explotados por amenazas que ponen en riesgo la confidencialidad, integridad y disponibilidad de estos.

g) **Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

h) **Equipo de respuesta a incidentes de seguridad de la información o CSIRT** (Computer Security Incident Response Team, por sus siglas en inglés): Es un equipo interno o externo a la organización, cuyo objetivo principal es minimizar y controlar los daños ante un ciberataque

i) **Evento**: Ocurrencia o cambio de un conjunto particular de circunstancias (NCh-ISO 27000:2013, página 7)

j) **Evento de Seguridad de la Información**: Ocurrencia o cambio identificado como el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de controles, o una situación desconocida que pueda ser relevante para la seguridad (NCh-ISO 27000:2013, página 7).

k) **Gestión de Eventos e Información de Seguridad o SIEM** (Security Information and Event Management, por sus siglas en inglés): Es un software de análisis centralizado de datos de seguridad, obtenidos desde múltiples sistemas, que incluyen aplicaciones antivirus, firewalls y soluciones de prevención de intrusiones.

l) Incidente de Seguridad de la Información: Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información (NCh.ISO 27000:2013, página 7).

m) **Integridad**: Propiedad de salvaguardar la exactitud y completitud de los activos de información.

n) **Política**: Intención y dirección general expresada por la Jefatura del Servicio.

o) **Seguridad de la Información**: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades, tales como autenticidad, responsabilidad con obligación de informar, no repudio y confiabilidad.

p) **Soporte de procesamiento de la información**: Todo sistema de procesamiento de la información, servicio o infraestructura, o las localizaciones físicas que los contienen.

q) **Tecnología de la Información y de las Comunicaciones (TIC)**: Constituida por la agrupación de los elementos y las técnicas utilizadas en el tratamiento y la transmisión de la información, principalmente de informática, internet y telecomunicaciones.

r) **Tercero**: Empresa o persona externa que tiene algún vínculo contractual con la institución.

s) **Protocolo de Internet o IP** (Internet Protocol, por sus siglas en inglés): Se trata de un estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes de información

t) **Puerto de seriado universal o USB** (Universal Serial Bus, por sus siglas en inglés): Tipo más común de entrada y salida de una computadora para la conexión de dispositivos informáticos físicos."

2º. APRUÉBASE el documento denominado "**Procedimiento de Administración del Sitio Público-Internet y Privado-Intranet de la Superintendencia del Medio Ambiente",** elaborado por la División de Seguimiento e Información Ambiental, y cuyo texto es el siguiente:

"PROCEDIMIENTO DE ADMINISTRACIÓN DEL SITIO PÚBLICO-INTERNET y PRIVADO-INTRANET DE LA SUPERINTENDENCIA DEL MEDIO AMBIENTE

La Superintendencia del Medio Ambiente (SMA) establece un procedimiento que tiene por objeto determinar la estructura y responsabilidades asociadas a las áreas encargadas del contenido y actualización de la Web institucional.

Los/las responsables intervendrán en el desarrollo de los contenidos y además generarán propuestas para priorizar temas relevantes.

ESTRUCTURA ORGANIZACIONAL DE LA ADMINISTRACIÓN DE LA WEB

Se establece, a través de este acto, una estructura organizacional, la cual estará a cargo de la administración de la página Web de la Superintendencia del Medio Ambiente.

La estructura no modifica, altera, ni interfiere en la actual estructura funcional ni orgánica de la Superintendencia, aprobada mediante Resolución Exenta N°2124 de fecha 30 de septiembre de 2021, de la Superintendencia del Medio Ambiente.

La estructura organizacional para la administración de la Web estará compuesta por:

1. Encargados/as de las áreas temáticas.
2. Comité Editorial Web.
3. Encargada/o Sitio Público-Internet.
4. Encargada/o Sitio Privado-Intranet

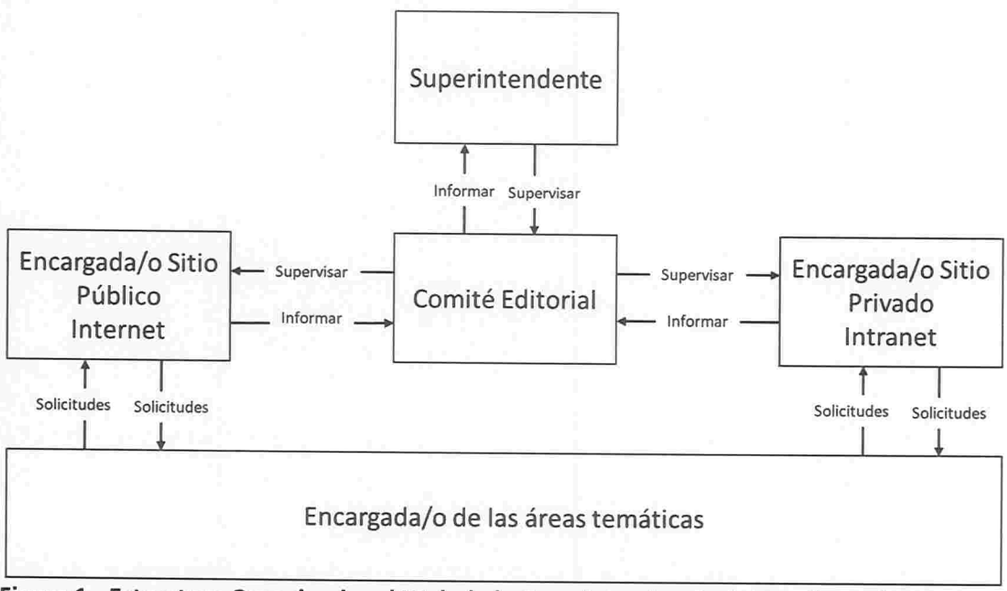

Figura 1 - Estructura Organizacional Web de la Superintendencia del Medio Ambiente

1. ENCARGADAS/OS DE LAS ÁREAS TEMÁTICAS

Rol: Cada área de la SMA que interviene en la actualización de contenidos, asume la responsabilidad de producir y administrar las secciones que le son asignadas. Así, la jefatura de dicha división, sección o área será el responsable titular de los contenidos de su sección pudiendo designar a un representante, quien deberá mantener las coordinaciones necesarias para el trabajo cotidiano de actualización.

Contenidos y responsables: Se establecen las siguientes áreas temáticas de la Web, con sus respectivos responsables por División, Departamento, Sección y/o Área.

AREAS TEMATICAS	RESPONSABLE
Noticias e Imagen Corporativa. Encargada/o del Sitio Público-Internet.	Representante de la Oficina de Comunicaciones.
Informaciones internas y administrativas. Encargado del Sitio Privado-Intranet.	Representante de la jefatura de la Sección de Gestión y Desarrollo de Personas (información vinculada a RR.HH.) y de la Oficina de Comunicaciones (resto de contenidos institucionales).
Información Ciudadana	Representante de la jefatura del Departamento de Participación y Relacionamiento Comunitario (DPAC).
Información Ambiental	Representante de la jefatura de División de Seguimiento e Información Ambiental (DSI).
Fiscalizaciones	Representante de la jefatura de División de Fiscalización y Conformidad Ambiental (DFZ).
Procedimientos sancionatorios	Representante de la jefatura de División Fiscalía (FIS).

Tabla 1 - Estructura de Responsabilidad en la Administración Web de la Superintendencia del Medio Ambiente

Cada área dedicará el tiempo necesario para realizar las acciones requeridas para la actualización del contenido que está a su cargo. Con todo, para estos efectos deberá coordinarse directamente con el Encargado/a.

2. COMITÉ EDITORIAL WEB.

Rol: El Comité Editorial de la página Web interviene en los lineamientos generales de la administración de la Web, asumiendo un rol colaborador estratégico y supervisor.

El Comité Editorial de la Página Web tendrá las siguientes funciones específicas:

- Dar lineamientos generales de la administración de la Web, sobre las modificaciones, mejoras, contenidos y estructuras requeridas.
- Supervisar el trabajo desarrollado por los Encargados/as, en lo que dice relación al presente procedimiento.

El Comité Editorial de la Página Web, estará conformado por:

- Jefatura/representante del Gabinete.
- Jefatura/representante de la Oficina de Comunicaciones (COM).
- Jefatura/representante del Departamento de Participación y Relacionamiento (DPAC)
- Jefatura/representante de la División de Seguimiento e Información Ambiental (DSI)

El Comité Editorial de la Web, dedicará el tiempo necesario para realizar las acciones requeridas. Con todo, se reunirá a lo menos una vez cada dos meses.

El Comité deberá dejar constancia de sus acuerdos, lineamientos generales y de cualquier materia relevante, a través de un acta-minuta.

3. ENCARGADO/A DEL SITIO PÚBLICO - INTERNET

Rol: El Encargado/a del sitio público deberá realizar acciones de coordinación requeridas para administrar el sitio Web de la Superintendencia.

La persona encargada del sitio público tendrá las siguientes funciones específicas:

- Revisión y edición permanente de la Web, responsable que sus contenidos estén actualizados. Coordinar la acción de los encargados de las áreas temáticas de la web.
- Preparar informes del estado de la Web, para las sesiones del Comité Editorial Web.
- Recibir solicitudes de proyectos posibles de realizar a través de la página (por ejemplo: e-learning, subsitios especiales, etc.).
- Recibir las solicitudes de publicación que la Institución y sus respectivas Áreas requieran.
- Realizar acciones de coordinación con DSI para gestionar publicaciones, actualizaciones, cambios de estructuras, soporte técnico y desarrollo en general.

La persona encargada del sitio público deberá informar directamente al Comité Editorial de la Web.

4. ENCARGADO/A DEL SITIO PRIVADO – INTRANET

Rol: El/la Encargado/a de la Intranet deberá realizar acciones de coordinación requeridas para administrar el sitio interno de la Superintendencia.

La persona encargada del sitio privado tendrá las siguientes funciones específicas:

- Revisión y edición permanente de la Intranet, responsable que sus contenidos estén actualizados. Coordinar la acción de los encargados/as de las áreas temáticas de la web.
- Preparar informes del estado de la Web, para las sesiones del Comité Editorial Web.
- Recibir solicitudes de proyectos posibles de realizar a través de la página (por ejemplo: e-learning, subsitios especiales, etc.).
- Recibir las solicitudes de publicación que la Institución y sus respectivas Direcciones, Unidades y Áreas requieran.
- Realizar acciones de coordinación con DSI para gestionar publicaciones, actualizaciones, cambios de estructuras, y soporte técnico y desarrollo en general.

La persona encargada del sitio privado deberá informar directamente al Comité Editorial de la Web.

5. PUBLICACIONES EN SITIO PUBLICO-INTERNET O PRIVADO-INTRANET

Cada responsable de Área y los/las funcionarios/as en general que requieran una acción de publicación, modificación y/o actualización de los sitios Web, en cualquiera de sus secciones y/o contenidos, ya sea

de carácter parcial o total, deberán remitir dicha solicitud al Encargado/a del sitio público – internet o privado - intranet, quién deberá procesar la solicitud según corresponda.

La solicitud debe ser realizada por escrito, a través de un correo electrónico especificando la acción requerida. En caso de que sea necesario, además deberá acompañar los documentos necesarios.

Las personas encargadas de implementar los cambios serán de la DSI, quienes realizarán el soporte y desarrollo de los requerimientos. En el caso de actualización de contenidos, estos pueden ser realizados directamente por las áreas temáticas, coordinados con las personas encargadas del sitio público – internet o sitio privado – intranet.

Una vez publicada, modificada o realizada la actualización de contenidos, los encargados deberán informar al solicitante para que proceda a validar la acción realizada.

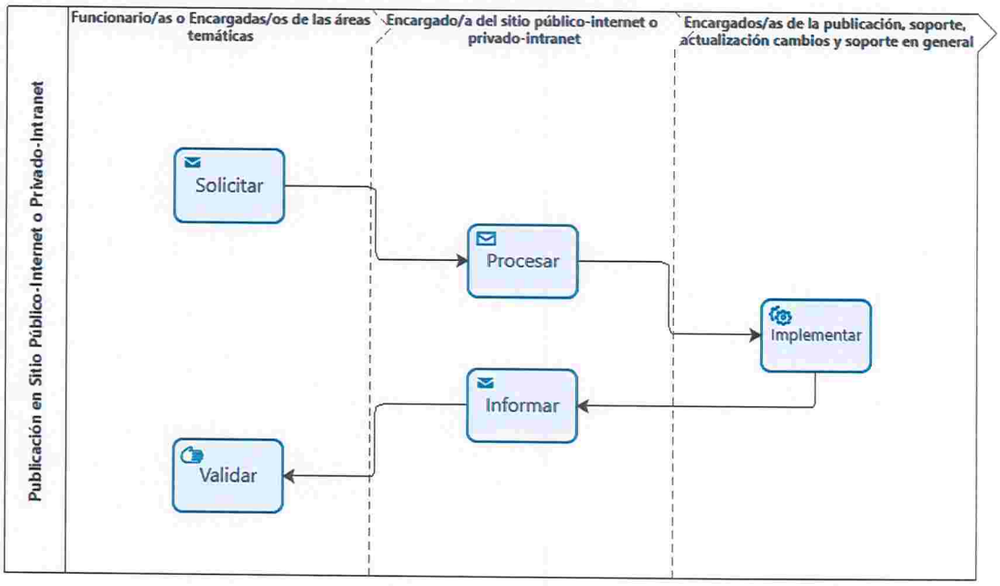

Figura 2 – Proceso Publicación Web de la Superintendencia del Medio Ambiente"

3º. ESTABLÉCESE que en todo lo no modificado por el presente acto administrativo, continúa planamente vigente lo contenido en la Resolución Exenta N°1507, de fecha 30 de noviembre de 2018 y la Resolución Exenta N°1928, de fecha 24 de diciembre de 2019, ambas de este origen.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

EMANUEL IBARRA SOTO
SUPERINTENDENTE DEL MEDIO AMBIENTE (S)

SUPERINTENDENCIA DEL MEDIO AMBIENTE
SUPERINTENDENTE
GOBIERNO DE CHILE

BMA/ODLF/FBG
Distribución

- Gabinete, SMA.
- Fiscalía, SMA.
- División de Seguimiento e Información Ambiental, SMA.
- División de Fiscalización y Conformidad Ambiental, SMA
- Departamento de Participación y Relacionamiento Comunitario, SMA
- Departamento de Administración y Finanzas, SMA
- Oficina de Comunicaciones, SMA
- Oficina de Auditoría Interna, SMA
- Oficinas Regionales, SMA
- Oficina de Partes, SMA.