DEJA SIN EFECTO RESOLUCIÓN QUE INDICA Y APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO NACIONAL DE PESCA Y ACUICULTURA/

VALPARAÍSO, 03 JUL. 2020

RES. EXENTA Nº 1311

VISTOS: La Hoja de Envío N° 167234, del Jefe del Departamento de Tecnologías de Información y Comunicaciones; el Decreto con Fuerza de Ley N°5 de 1983, del actual Ministerio de Economía, Fomento y Turismo, y sus modificaciones; lo dispuesto en la Ley N° 19.880 que Establece las Bases de los Procedimientos que Rigen los Actos de los Órganos de la Administración del Estado; el Decreto Supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia; las Normas Técnicas NCh-ISO 27001:2013 y NCh-ISO 27002:2013; la Resolución Exenta N° 702, de fecha 25 de febrero de 2019, de este Servicio; y las Resoluciones N° 7 y N° 8, de 2019, ambas de la Contraloría General de la República.

CONSIDERANDO:

Que, la seguridad de la información es entendida como la protección de los activos de información contra una amplia gama de amenazas, garantizando así la continuidad de la prestación de los servicios, minimizar posibles daños a la institución y maximizar la eficiencia y las oportunidades de mejora de gestión de la organización.

Que, para el cumplimiento de su misión institucional y objetivos estratégicos, el Servicio Nacional de Pesca y Acuicultura reconoce la importancia de proteger los recursos de información que genera y gestiona, así como la tecnología usada para su procesamiento, de las amenazas internas o externas, deliberadas o accidentales, que puedan interferir en la correcta prestación de los servicios que entrega esta Institución.

Que, en este contexto, la Política General de Seguridad de la Información está orientada a resguardar la información en todo su proceso de creación, difusión, modificación, almacenamiento, preservación y eliminación, asegurando asimismo los medios que permiten dicho ciclo y las personas que acceden a esa información.

Que, con el objeto de contar con un sistema de gestión de Seguridad de la Información que permita lograr niveles adecuados de integridad, confidencialidad, disponibilidad y confiabilidad para todos los activos de información considerados relevantes, mediante la citada Resolución Exenta N° 704, se aprobó la Política General de Seguridad de la Información del Servicio Nacional de Pesca y Acuicultura.

Que, conforme a lo solicitado en la Hoja de Envío N° 167234, también citada en Vistos, resulta indispensable dejar sin efecto la precitada resolución y actualizar, en concordancia con la legislación vigente en el país y los criterios definidos en las normas técnicas chilenas, la Política General de Seguridad de la Información que se aprobará en la parte resolutiva del presente acto administrativo.

RESUELVO:

1. DÉJASE SIN EFECTO la Resolución Exenta N° 702, de fecha 25 de febrero de 2019, que aprueba Política General de Seguridad de la Información del Servicio Nacional de Pesca y Acuicultura para el año 2019.

2. APRUÉBASE la Política General de Seguridad de la Información del Servicio Nacional de Pesca y Acuicultura año 2020, cuyo texto se transcribe a continuación:

V°B°
Subdirección
JURIDICA

POLÍTICA GENERAL
DE SEGURIDAD DE LA INFORMACIÓN

NOTA DE CONFIDENCIALIDAD

1. Objetivos

El Servicio Nacional de Pesca y Acuicultura es una entidad pública dependiente del Ministerio de Economía, Fomento y Turismo, cuya misión es "contribuir a la sustentabilidad del sector y a la protección de los recursos hidrobiológicos y su medio ambiente, a través de una fiscalización integral y gestión sanitaria que influye en el comportamiento sectorial promoviendo el cumplimiento de las normas".

1.1 Objetivos estratégicos

- Contar con un enfoque de fiscalización integral eficaz para generar una disuasión efectiva de las conductas transgresoras.
- Participar de la agenda normativa sectorial para contribuir activamente a un buen diseño y evaluación de las normas de manera que incorporen elementos claves para su cumplimiento.
- Facilitar el cumplimiento de la norma a los/as usuarios/as sectoriales proveyendo servicios de calidad, de manera accesible, oportuna y con estándares definidos, para disminuir las conductas transgresoras.
- Fortalecer la seguridad y transparencia del rol fiscalizador, para incrementar la capacidad institucional para realizar controles destinados a optimizar los procedimientos de fiscalización, asegurando la protección de los/as funcionarios/as y la Institución en estas tareas.
- Potenciar el proceso modernizador en Sernapesca a fin de lograr la excelencia institucional para el cumplimiento de su misión, a través del desarrollo tecnológico y de las personas.

De acuerdo con lo anterior, la información que genera y gestiona esta Institución constituye un activo estratégico clave para asegurar la prestación de los servicios y el cumplimiento de la misión institucional. En este contexto, la Política General de Seguridad de la Información está orientada a proteger la información en la totalidad de su ciclo de vida (creación, difusión, modificación, almacenamiento, preservación y eliminación), los medios que permiten dicho ciclo y las personas que acceden y/o manipulan la información. Lo anterior, con el fin de garantizar su integridad, disponibilidad y confidencialidad.

2. Declaración de la intención de la Dirección

El Servicio Nacional de Pesca y Acuicultura declara su compromiso de proteger los recursos de información y la tecnología usada para su procesamiento, de las amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los requisitos de confidencialidad, integridad, disponibilidad y confiabilidad de la información. Además de minimizar la pérdida o daño a la información que pueda interferir en la correcta entrega de la prestación de los servicios.

3. Principios de seguridad de la información

- Comprometer a las autoridades de la Institución en la difusión, consolidación y cumplimiento de esta y otras políticas que apoyen el logro de la declaración precedente.
- Implementar las medidas de seguridad comprometidas identificando los recursos y las partidas presupuestarias disponibles.
- Mantener las políticas, normativas y procedimientos actualizados, con el fin de asegurar su vigencia y nivel de eficacia.
- Promover prácticas que aseguren la continuidad en la prestación de los servicios que entrega la Institución de acuerdo con los dominios de seguridad establecidos.
- Promover una cultura organizacional orientada a la seguridad de la información.

4. Objetivos de la gestión de seguridad de la información

4.1 Objetivo general

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información institucional considerando el esquema de clasificación de la información establecido, con el objeto de asegurar la prestación de los servicios que entrega el Servicio Nacional de Pesca y Acuicultura, en el alcance definido del Sistema de Seguridad de la Información, mediante el resguardo de los activos de información asociados a los procesos críticos del negocio y su soporte.

4.2 Objetivos específicos

- Identificar y clasificar los activos de información de la Institución en el alcance definido del Sistema de Seguridad de la Información, para lograr niveles adecuados de integridad, confidencialidad y disponibilidad de éstos.
- Controlar, prevenir y/o mitigar los riesgos de seguridad de la información, identificando las vulnerabilidades y amenazas que enfrentan los activos, en orden a asegurar la prestación de los servicios que entrega la institución en el alcance definido del Sistema de Seguridad de la Información.
- Establecer políticas, normas y procedimientos que permitan resguardar y proteger los activos de información de la Institución en el alcance definido del Sistema de Seguridad de la Información.
- Definir un plan de difusión y capacitación que dé a conocer el Sistema de Seguridad de la Información y las buenas prácticas asociadas a éste.

5. Alcance de la política de seguridad de la información

5.1 Alcance general

El Servicio Nacional de Pesca y Acuicultura tiene como tarea principal fiscalizar el cumplimiento de las disposiciones de la Ley General de Pesca y Acuicultura, con especial foco en desincentivar la pesca ilegal, lo que está definido, además, como objetivo estratégico institucional en el Formulario A-1 "Contar con un enfoque de fiscalización integral eficaz para generar una disuasión efectiva de las conductas transgresoras".

Conforme lo anterior, el alcance y la aplicabilidad del Sistema de Seguridad de la Información, al que aplica esta política y el resto de los controles implementados se define en el documento Alcance del Sistema de Seguridad de la Información.

Cabe destacar que la información que se genera en los procesos incluidos en el alcance del Sistema de Seguridad de la Información es muy relevante para el logro de los objetivos estratégicos asociados, y la misión institucional, por lo que el garantizar la integridad, disponibilidad y confidencialidad de los activos de cada uno de ellos es vital para la institución pues esto permite asegurar la prestación de los servicios y la continuidad del negocio.

5.2 Definición de los activos de información

Son todos aquellos elementos relevantes que intervienen o se generan como resultado de la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución, en la que se distinguen las siguientes categorías:

- La información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, entre otros);
- Los equipos/sistemas/infraestructura que soportan esta información;
- Bases de datos;
- Las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

5.3 Definición de seguridad de la información

El Servicio Nacional de Pesca y Acuicultura entiende que la seguridad de la información es la protección de los activos de información contra una amplia gama de amenazas para asegurar la continuidad de la prestación de los servicios, minimizar el daño a la institución y maximizar la eficiencia y las oportunidades de mejora de la gestión de la organización, considerando la confidencialidad, integridad y disponibilidad de los activos de información.

6. Aspectos generales de la política de seguridad de la información

- La Política General de Seguridad de la Información ha sido elaborada en concordancia con la legislación vigente en el país, considerando, además, su compatibilidad con los requisitos y criterios definidos en las normas chilenas NCh-ISO 27001:2013 y NCh-ISO 27002:2013.

- La Dirección se compromete a realizar las acciones que estén a su alcance para garantizar la seguridad de la información, la prestación de los servicios y coadyuvar a la continuidad operativa de manera de hacer frente a las interrupciones de las actividades institucionales y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

- La Dirección se compromete también a considerar como parte integrante de la seguridad de la información, los aspectos asociados a ciberseguridad, de acuerdo con la normativa vigente, las orientaciones emanadas de las entidades rectoras en este campo y evaluando los cambios en el contexto en que se desarrollan las actividades institucionales, al tomar en cuenta el uso creciente y extendido de infraestructura informática para el logro de su misión.

- La Política General de Seguridad de la Información es aprobada mediante resolución exenta por el (la) Director(a) Nacional de Pesca y Acuicultura.

- La implementación de la presente política general y sus políticas específicas, procedimientos y controles asociados será de responsabilidad del (de la) Director(a) Nacional y su equipo directivo a nivel nacional, además del Comité de Seguridad de la Información, la Secretaría Técnica para la Gestión de la Seguridad de la Información y el (la) Encargado(a) de Seguridad de la Información.

- La evaluación del cumplimiento de la presente política general, sus políticas específicas, procedimientos y controles asociados se efectuará a través de actividades de seguimiento del proceso de identificación, evaluación y definición de acciones para el tratamiento de los riesgos de seguridad de la información, para lo cual se utiliza la metodología propuesta por la Red de Expertos, y la evaluación de la eficacia de las acciones y controles definidos.

- El incumplimiento de la Política General de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y características del aspecto no cumplido y según lo establecido en la legislación vigente.

7. Evaluación y revisión

La Política General de Seguridad de la Información será revisada en su contenido al menos cada tres años a solicitud del (de la) Director(a) Nacional, del Comité de Seguridad de la Información, del (de la) Encargado(a) de Seguridad de la Información o, antes del plazo indicado, en las siguientes circunstancias: frente a cambios en el contexto de la institución, ya sean de carácter político, económico o social, tecnológico, el ambiente de la Institución, incluyendo el clima organizacional, o debido a las circunstancias del servicio, considerando la disponibilidad presupuestaria, las condiciones legales y al ambiente técnico, con la finalidad de asegurar que la institución ha implementado sus directrices.

8. Mecanismos de difusión

La difusión de la presente Política General se realizará a través de la intranet institucional para el personal de SERNAPESCA y, a través de la web institucional a terceros que presten servicios en la institución o entidades externas relevantes.

9. Marco de control de la seguridad de la información

Los controles de seguridad de la información se establecen en base a la norma chilena NCh-ISO 27001:2013, a través de lo especificado en cada uno de los dominios de seguridad y considerando la legislación aplicable vigente. Por ello, el marco para fijar los controles estará dado por el diagnóstico del estado de la seguridad de la información institucional, la evaluación de riesgos de seguridad de la información y la planificación de las acciones para cubrir las brechas detectadas. Además de la mantención, evaluación y mejoramiento de los controles posterior a la etapa de implementación efectuada.

9.1 Otras políticas y procedimientos

La estructura documental para la gestión de la seguridad de la información en la institución está compuesta por una Política General de Seguridad de la Información, políticas específicas para la seguridad de la información y procedimientos (manuales, instructivos, guías, entre otros documentos). Así, en el caso de la Política General de Seguridad de la Información, ésta será formalizada por Resolución Exenta del (de la) Director(a) Nacional, mientras que políticas específicas y procedimientos (manuales, instructivos, guías, entre otros documentos) serán formalizados mediante actas del Comité de Seguridad de la Información.

10. Responsabilidades en materia de seguridad de la información

La política de seguridad de la información es de aplicación obligatoria para todo el personal de la institución, cualquiera sea su calidad jurídica, el área a la cual pertenezca y cualquiera sea el nivel de las tareas que desempeñe. A continuación, se detallan algunas de las responsabilidades asociadas a la seguridad de la información institucional.

10.1 Director(a) Nacional:

Es el responsable final por la seguridad de la información de la institución y velará por el cumplimiento de las medidas de seguridad de los activos de información y de la infraestructura de información. En particular, debe garantizar la ejecución de las siguientes acciones:

a. Establecer lineamientos claros y oportunos sobre la gestión de la seguridad de la información.
b. Aprobar la Política de Seguridad de la Información institucional.
c. Validar el proceso de gestión de seguridad de la información.
d. Sancionar las estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucionales, que se generen como resultado de los reportes o propuestas del Comité de Seguridad de la Información.
e. Proveer los recursos necesarios para la ejecución de un Sistema de Seguridad de la Información.

10.2 Comité de Seguridad de la Información:

a. Supervisar la implementación de políticas, procedimientos y estándares que se desprenden de la Política General de Seguridad de la Información en la institución.
b. Proponer estrategias pormenorizadas para la implementación de la Política General de Seguridad de la Información, políticas específicas y procedimientos, coadyuvando en la debida solución de las situaciones de riesgo detectadas.
c. Presentar una propuesta de Política General de Seguridad de la Información al (a la) Director(a) Nacional para su aprobación final.
d. Aprobar el inventario de activos de información institucional, su análisis de riesgo y plan de tratamiento.
e. Aprobar las políticas y procedimientos que se sometan a consulta, a través de la firma de su presidente.
f. Arbitrar conflictos que se generen en materia de seguridad de la información y los riesgos asociados, proponiendo soluciones concretas a los mismos.
g. Mantener una coordinación permanente con el Comité de Riesgos de la institución para generar estrategias comunes de gestión.
h. Reportar periódicamente al Director(a) Nacional respecto de oportunidades de mejora en el proceso de gestión de la seguridad de la información, así como también, de aquellos incidentes relevantes y la solución implementada en cada caso.
i. Apoyar permanentemente al Encargado(a) de Seguridad de la Información en la gestión de la Política General de Seguridad de la Información.
j. Velar por la adecuada aplicación del procedimiento de gestión de incidentes de seguridad de la información.

10.3 Encargado(a) de Seguridad de la Información:

Es un funcionario nombrado por el (la) Director(a) Nacional como su asesor(a) directo(a) en materia de seguridad de la información. El (la) Encargado(a) de Seguridad de la Información tendrá que ejecutar las siguientes acciones:

a. Liderar y organizar al Comité de Seguridad de la Información.
b. Organizar las actividades del Comité de Seguridad de la Información.
c. Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la institución y el control de su implementación; y velar por su correcta aplicación.
d. Supervisar el monitoreo del avance general de la implementación de las estrategias de control y tratamiento de riesgos.

e. Gestionar la coordinación con otras unidades del Servicio para apoyar los objetivos de seguridad.
f. Supervisar el establecimiento de puntos de enlace con los encargados de seguridad de otros Servicios públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de la seguridad pertinentes.
g. Asesorar y asistir a cada una de las áreas en la definición de los criterios mencionados.
h. Velar por la adecuada aplicación del procedimiento de gestión de incidentes de seguridad de la información.

10.4 Coordinador(a) de Seguridad de la Información:

a. Convocar a la Secretaría Técnica para la gestión de la seguridad de la información a solicitud del Secretario(a) Ejecutivo(a) del Comité de Seguridad de la Información.
b. Monitorear el avance general de la documentación e implementación de políticas específicas y procedimientos de seguridad de la información al interior de la institución.
c. Establecer puntos de enlace con los encargados de seguridad de otros servicios públicos y especialistas externos que favorezcan el estar al tanto de las tendencias, normas y métodos de la seguridad pertinentes.
d. Mantener actualizada la política general de seguridad de la información, el manual de roles y responsabilidades y el glosario de términos y definiciones.
e. Difundir en la intranet institucional los documentos asociados a la gestión de la seguridad de la información.

10.5 Secretaría Técnica para la Seguridad de la Información:

a. Levantar y documentar políticas específicas y procedimientos de seguridad de la información al interior de la institución.
b. Implementar políticas específicas y procedimientos de seguridad de la información al interior de la institución.
c. Velar por la aplicación de políticas específicas y procedimientos de seguridad de la información al interior de la institución.
d. Identificar los riesgos de seguridad asociados a la pérdida de confidencialidad, integridad y disponibilidad de los activos de información identificados en el inventario de activos de información.
e. Determinar y aplicar controles de seguridad que sean apropiados para el tratamiento de los riesgos de seguridad identificados.
f. Mantener actualizado el inventario de activos de la información institucional, coordinándose con los propietarios de activos de la información de los procesos del alcance.
g. Gestionar la implementación de las estrategias de tratamiento de riesgos de seguridad de la información y reportar su avance al encargado y coordinador de seguridad de la información.
h. Gestionar operativamente los incidentes de seguridad de la información que afecten los activos de información institucionales.

10.6 Subdirector(a) Jurídico:

a. Administrar las políticas y procedimientos relativos al dominio "Cumplimiento", dando cumplimiento a las directrices establecidas.
b. Definir, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales relevantes en materia de seguridad de la información, estableciendo el enfoque de la institución para satisfacer dichos requerimientos.
c. Velar por la incorporación de las cláusulas en materia de seguridad de la información, en los contratos, acuerdos u otra documentación que la institución firme con funcionarios personal a honorarios o terceras partes.
d. Asesorar en materia legal, asociada a seguridad de la información, a la institución y establecer las pautas legales que permitan cumplir con los requerimientos legales en esta materia.

10.7 Jefe(a) Departamento de Tecnologías de Información y Comunicaciones:

a. Administrar las políticas y procedimientos relativos a los dominios: administración de los activos, control de acceso, seguridad de las operaciones, seguridad de las comunicaciones, adquisición, desarrollo y mantenimiento de sistemas de información, gestión de los incidentes de seguridad de la información, aspectos de seguridad de la información en la gestión de la continuidad del negocio, dando cumplimiento a las directrices establecidas.
b. Gestionar los requerimientos de seguridad informática y de la información establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la institución.

c. Velar por la adecuada aplicación de la Metodología para la gestión de proyectos de desarrollo de software y el Procedimiento de desarrollo y actualización de sistemas de información establecidos para la adecuada y oportuna gestión de las tareas de desarrollo y mantenimiento de sistemas de información, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.
d. Administrar la Secretaría Técnica para atender los problemas relacionados a la seguridad de la información e informática en la institución.
e. Establecer puntos de enlace tácticos y operativos con los encargados de seguridad de otros servicios públicos y especialistas externos que favorezcan el estar al tanto de las tendencias, normas y métodos de la seguridad pertinentes.

10.8 Jefe(a) Departamento de las Personas:

a. Administrar las políticas y procedimientos relativos al dominio "Seguridad ligada a los recursos humanos" dando cumplimiento a las directrices establecidas.
b. Elaborar y ejecutar un "Plan de capacitación y sensibilización" en temas de seguridad de la información, estructurado en base a requerimientos del (de la) Encargado(a) de Seguridad de la Información.
c. Establecer puntos de enlace tácticos y operativos con los(as) encargados(as) de seguridad de otros servicios públicos y especialistas externos que favorezcan el estar al tanto de las tendencias, normas y métodos de la seguridad ligada a los recursos humanos.
d. Notificar a todo el personal que ingresa, sus obligaciones respecto del cumplimiento de la Política General de Seguridad de la Información y de todas las políticas específicas, procedimientos y prácticas que de ella surjan.

10.9 Propietarios de los activos de información:

Este rol recae en los(as) Subdirectores, Directores(as) Regionales de Pesca y Acuicultura, Jefes(as) de Departamentos, Unidades y Secciones y todo el personal responsable del uso y protección de la información, o sobre aquellos(as) funcionarios(as) que la Dirección asigne, quienes deberán:

a. Clasificar los activos de información de acuerdo con el grado de sensibilidad y criticidad de los mismos, y considerando lo establecido en el procedimiento correspondiente, documentar y mantener actualizada la clasificación efectuada.
b. Identificar a los(as) usuarios(as) que deberán tener permisos de acceso a la información de acuerdo con las funciones desempeñadas y competencia.
c. Conocer, acatar y dar cumplimiento a la política general de seguridad de la información, sus políticas específicas y procedimientos.
d. Participar de las auditorías sobre las actividades vinculadas al proceso de gestión de seguridad de la información.
e. Velar por la protección de la información que manejan en el desempeño de sus funciones.

10.10 Departamento de Auditoría Interna:

a. Brindar aseguramiento al Comité de Seguridad de la Información de que la institución cuenta con un correcto nivel de madurez y capacidad para la identificación y mitigación de los riesgos de seguridad de la información y ciberseguridad.
b. Practicar auditorias de forma periódica sobre las actividades vinculadas al proceso de gestión de seguridad de la información, informando sobre su grado de cumplimiento.
c. Identificar y evaluar las capacidades preventivas de control de la seguridad de la información y de ciberseguridad en materia de educación, formación y concienciación de usuarios, así como procesos y herramientas de control y vigilancia digital.
d. Verificar que los riesgos levantados por los equipos operativos estén en concordancia con las orientaciones estratégicas y objetivos institucionales.
e. Analizar y evaluar que los controles de seguridad de la información implementados contribuyan a asegurar el cumplimiento de las medidas adoptadas para minimizar los riesgos de seguridad de la información.

Para más información respecto de los roles y responsabilidades, consultar el documento "Manual de roles y responsabilidades".

11. Excepciones

No aplica.

12. Actuación ante eventos e incidentes

En la eventualidad de ocurrir algún incidente de seguridad de la información relativo a las medidas de seguridad indicadas en esta política, la(s) persona(s) que lo detecte(n) debe(n) informar a la brevedad al correo electrónico incidentes@sernapesca.cl, donde el (la) Encargado(a) de Seguridad de la Información analizará y canalizará el evento o incidente, para que de acuerdo con lo establecido en el procedimiento de Gestión de Incidentes de Seguridad de la Información, adoptar las medidas necesarias para minimizar los potenciales daños a los activos de información definidos por SERNAPESCA, definir las acciones que permitan eliminar las causas del mismo y prevenir la ocurrencia de incidentes y así, dar cumplimiento a esta política.

13. Referencias normativas

La presente política general y documentos asociados a la seguridad de la información han sido elaborados en base a la siguiente documentación:

- Ley N°18.892, que aprueba "Ley General de Pesca y Acuicultura". Ministerio de Economía, Fomento y Reconstrucción.
- Ley N°19.880, que "Establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado". Ministerio Secretaría General de la Presidencia.
- Ley N°20.285, que "Regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la administración del Estado". Ministerio Secretaría General de la Presidencia.
- Ley N°21.132, que "Moderniza y fortalece el ejercicio de la función pública del Servicio Nacional de Pesca". Ministerio de Economía, Fomento y Reconstrucción.
- Decreto Supremo N°83, que "Aprueba norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos". Ministerio Secretaria General de la Presidencia.
- Decreto Supremo N°1, que "Aprueba norma técnica sobre sistemas y sitios web de los Órganos de la Administración del Estado. Ministerio Secretaría General de la Presidencia.
- Instructivo de Gabinete Presidencia N°008, del 23 de Octubre de 2018, que imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la administración del estado.
- NCh-ISO 27001:2013 Tecnología de la información – Técnicas de seguridad – Sistema de gestión de la seguridad de la información – Requisitos.
- NCh-ISO 27002:2013 Tecnologías de la información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información.

Para más información respecto del marco regulatorio, consultar el documento "Marco normativo para la identificación de requisitos legales y contractuales".

3. PUBLÍQUESE la presente Resolución en la intranet institucional y en el Portal de Transparencia Activa del Servicio Nacional de Pesca y Acuicultura.

ANÓTESE, PUBLÍQUESE EN LA FORMA SEÑALADA Y ARCHÍVESE

SERVICIO NACIONAL DE PESCA Y ACUICULTURA * MINISTERIO DE ECONOMÍA, FOMENTO Y TURISMO * DIRECTORA NACIONAL

ALICIA GALLARDO LAGNO
DIRECTORA NACIONAL
SERVICIO NACIONAL DE PESCA Y ACUICULTURA

ACC/acc
Distribución:
-Dirección Nacional.
-Subdirecciones.
-Departamento de Tecnologías de Información y Comunicaciones.
-Direcciones Regionales.
-Oficina de Partes.