NSI : 0126313

Creador :

Fecha de creación : 2020-09-15

Tipo de documento : RESOLUCIÓN EXENTA

Palabras Claves : APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA CNR.

Folio : RES-2820

Fecha Folio : 17/09/2020 10:52

Año :

Ver Documento Adjunto

SECRETARIO/A EJECUTIVO/A

CNR
Firma Electrónica Avanzada

DEJE SIN EFECTO LA RESOLUCIÓN N° 4875 /2019, Y APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA COMISIÓN NACIONAL DE RIEGO.

_____

VISTOS:

Lo dispuesto en el D.F.L. Nº 7 de 1983 que fija texto refundido del D.L Nº 1.172 de 1975 modificado por la Ley Nº 19.604 de 06 de Febrero de 1999, que creó la Comisión Nacional de Riego; el D.S Nº 179 de 1984 que fija el texto actualizado del D.S Nº 795 de 1975, que aprobó el Reglamento de la Comisión antedicha, todos del Ministerio de Economía, Fomento y Reconstrucción; el Decreto Nº 83 del Ministerio Secretaria General de la Presidencia, que aprueba normas técnica para los organismos del Estado sobre Seguridad Informática; Requisitos técnicos y medios de verificación del Programa de Mejoramiento de la Gestión - Sistema de Seguridad de la Información; Decreto Supremo Nº 124 del 2018 del Ministerio de Agricultura y la Resolución Nº 7 de 2019 de la Contraloría General de la República; Resolución CNR Exenta N° 4607 de 2016; Resolución CNR Exenta N° 476 de 2016; Resolución CNR Exenta N° 4791 de 2016; Resolución CNR Exenta N° 5642 de 2017; Resolución CNR Exenta N° 4875 de 2019.

CONSIDERANDO:

Que la información es un bien que tiene gran valor para la institución y necesita ser protegida en forma apropiada con el fin de asegurar la continuidad de las operaciones, minimizar el daño que pueda ocasionarse a la institución, y maximizar la eficiencia y las oportunidades de mejora de la gestión de la organización, independiente de la forma que ésta tome o los dispositivos a través de los cuales es compartida o almacenada.

Que la institución debe identificar y asegurar en forma adecuada y permanente todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de la información de valor para la Comisión Nacional de Riego.

Que en la institución debe gestionarse adecuadamente la Seguridad de la Información, con objeto de mejorar los niveles de protección de los activos de información relevantes que dan sustento a sus procesos de provisión y de soporte.

Que los funcionarios y las funcionarias deben considerar la Seguridad de la Información en el desempeño de sus funciones, procurando que su accionar no ponga en riesgo la seguridad de los activos de información de la Institución.

Que de conformidad a la Norma ISO 27.001: of.2013 en su control A.05.01.01 el cual señala que debe existir un documento denominado Política de Seguridad de la Información, que esté aprobado por el Jefe de Servicio, y que refleja claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad Institucional.

Que por Resoluciones Exentas N° 4543 de fecha 30 de diciembre de 2014, N° 4607 de 03 de noviembre 2016, N° 5421 de 28 de diciembre 2016, N° 5642 de 29 de diciembre 2017, N° 6856 de 31 de diciembre 2018 y N° 4875 del 03 de octubre de 2019 se aprobaron la Política General de Seguridad de la Información de la Comisión Nacional de Riego.

Que, en el marco del mejoramiento continuo, es necesario actualizar a lo menos cada dos años la Política General de Seguridad de la Información de la Comisión Nacional de Riego o cuando se estime necesario.

RESUELVO:

1. **APRUÉBASE** la Política General de Seguridad de la Información de la Comisión Nacional de Riego, cuyo texto se detalla a continuación

2020

Política General de la Seguridad de la Información - Comisión Nacional de Riego

DEPARTAMENTO DE ADMINISTRACIÓN Y FINANZAS ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN

Contenido

DECLARACION INSTITUCIONAL

El Sistema de Gestión de la Comisión Nacional de Riego se basa en el cumplimiento de los requisitos del cliente y partes interesadas, los cuales son manifestados por la legislación y normativa que rige al Servicio, así como también, las políticas públicas de la Administración del Estado

En este sentido, el Sistema de Gestión viene a apoyar la gestión de la CNR en los desafíos de avanzar a una etapa superior de fortalecimiento de su gestión integrada, relacionando con mayor fuerza los avances logrados en calidad y nuevos atributos a su gestión, sean estos Seguridad de la Información y Gestión de Riesgos, en el marco de los nuevos requisitos de la norma ISO 9001:2015. Es por tal razón que en etapas de mayor maduración de su gestión se hace imprescindible integrar estos atributos a un único modelo de gestión basado en el cumplimiento de los requisitos de estándares internacionales, el marco normativo y legislativo vigente, por medio del cual se obtenga profundidad y extensión en la aplicación de las políticas públicas y satisfacción de sectores atendidos; mayores niveles eficacia en los resultados perseguidos; y mayores niveles de eficiencia en las actividades desarrolladas por los Servicios Públicos.

En función de lo anterior, la Comisión Nacional de Riego se compromete a custodiar y proteger sus activos de información de modo tal de mantener su confiabilidad, integridad y disponibilidad frente a amenazas, sean estas internas o externas, deliberadas o accidentales.

En este sentido, se desarrollan e implementan continuamente las medidas necesarias y tendientes a asegurar la continuidad operacional de los servicios brindados por la institución, determinando con ello lineamientos, actores y responsables de velar por el cumplimiento de las medidas de protección y los controles dispuestos a través del Sistema de Seguridad de la Información (SSI) implementado en la CNR.

OBJETIVOS DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Implementar y mejorar continuamente el SSI de la CNR, definiendo los lineamientos, controles y responsables para garantizar la integridad, confiabilidad y disponibilidad de los Activos de Información existentes en la CNR.

Para el logro de este objetivo, se conforma el Comité de Gestión, cuya constitución y funciones son definidas a través de Resolución Exenta

ALCANCE O AMPLITUD DE LA POLÍTICA DE SEGURIDAD DE INFORMACIÓN

En la CNR el Sistema de Seguridad de la Información (SSI) abarca la totalidad de los procesos de provisión de bienes y servicios considerando sus oficinas regionales, priorizando y focalizando sus esfuerzos en aquellos activos de información que han sido definidos como críticos para la Institución y compatibilizando la necesidad de proveer servicios que incorporen un mayor nivel de confianza y calidad hacia sus clientes, usuarios y/o beneficiarios.

Las políticas, lineamientos y procedimientos que se desprenden de la aplicación de la presente Política General de Seguridad de la Información, son implementados y cumplidos en función de establecer controles que permitan minimizar el impacto sobre los activos de información y son reconocidos y aceptados por los diferentes niveles jerárquicos de la CNR; con participación activa y continua de todos sus funcionarios/as, así como por sus proveedores de servicios externos, debiendo la dirección de la CNR fortalecer, difundir e impulsar continuamente la aplicación de la política general de seguridad de la información, sus políticas por dominios y de los procedimientos que de ella se desprenden.

Así mismo, la presente, se aplica sobre todos los activos de información críticos de la CNR, los que son identificados y referenciados en la Matriz de Activos de Información, la cual se asocia con los productos estratégicos, identificando entre otros la criticidad de los activos de información, precisando el dueño y sus responsables de los activos, los niveles de criticidad junto con los riesgos asociados a sus amenazas y vulnerabilidades.

La identificación y la actualización de la matriz de activos de información de la CNR, es llevada a cabo anualmente mediante la revisión de los encargados de gestión de la CNR, con objeto de reconocer y establecer de una manera continua los cambios que se puedan producir identificando también el nivel del riesgo en los procesos críticos para la CNR.

En cuanto a las interfaces y dependencias, entre las actividades realizadas por la institución y los actores externos; estas cumplen los requisitos de seguridad comprometidos por la institución. Respecto a los vínculos con proveedores externos; las actividades y compromisos deberán estar enmarcadas según lo determinado en bases, administrativas y en los contratos que se redacten incorporando cláusulas de seguridad de la información.

El ámbito de aplicación de la Política de Seguridad contempla dominios y controles contenidos en la Nch-ISO 27002:2013 y que son los siguientes:

N°	Dominios	Objetivos por Dominio
1	**Organización de la Seguridad de la Información**	Establecer un marco de administración para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.
2	**Seguridad de recursos humanos**	Garantizar que los empleados y contratistas comprendan sus responsabilidades y que sean adecuados para los roles en los que se les ha considerado.
3	**Administración de activos**	Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.
4	**Control de accesos**	Garantizar el acceso autorizado a los usuarios, evitando el acceso no autorizado a los sistemas/servicios y limitando el acceso a la información y a las instalaciones de procesamiento de la información existentes.
5	**Seguridad física y ambiental**	Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procedimiento de la información.
6	**Seguridad de las operaciones**	Garantizar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
7	**Seguridad en las comunicaciones**	Garantizar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.
8	**Relaciones con los proveedores**	Establecer requisitos de seguridad de la información para cuando se realice la contratación de servicios externos.
9	**Administración de incidentes de seguridad de la información**	Garantizar en la CNR la administración eficaz de los incidentes de seguridad de la información que puedan ocurrir, incluyendo la comunicación de los eventos y las debilidades de seguridad.
10	**Cumplimiento**	Identificar, aplicar y cumplir con los requisitos normativos, legales o contractuales que se aplican a la CNR.

11	**Protección de los registros y privacidad, protección de la información de identificación personal**	Aplicar y cumplir las directrices que rigen las acciones para proteger los registros y la información de carácter personal contra uso indebido, destrucción, falsificación o acceso no autorizado de acuerdo con los requisitos legislativos o normativos.
12	**Seguridad en escritorio y pantalla despejados**	Evitar pérdidas, daños, robos y la interrupción a las operaciones de la organización, reduciendo el riesgo del acceso al personal no autorizado, la pérdida o daño de la información durante y fuera de las horas laborales normales.
13	**Respaldo de la información**	Establecer las directrices para brindar protección contra la pérdida de datos mediante respaldos de la información considerando su protección y resguardo permanente.
14	**Protección contra código malicioso**	Garantizar un control preventivo y la protección permanente ante riesgos provocados por amenazas de código malicioso como Virus, Gusanos, Spyware, Código móvil, Keylogger, Ransomware, Phishing y otras variantes.
15	**Ciberseguridad**	Desarrolla actividades y planificaciones necesarias para dar cumplimiento con el instructivo presidencial Nro.8 (23/10/2018) que imparte instrucciones en materias de Ciberseguridad para los órganos del estado.
16	**Protocolo trabajo a distancia**	Entrega directrices para resguardar la seguridad en el Trabajo a Distancia.

ROLES Y RESPONSABILIDADES GENERALES

Con el objetivo de establecer un marco de administración para controlar la implementación y operación, se definen y asignan las responsabilidades para la protección de activos individuales y para realizar procesos en los siguientes roles.

Los roles y responsabilidades específicas estarán definidas en las Políticas de Seguridad de Información por dominio, según la materia que compete.

1. Del Secretario Ejecutivo de la CNR

- Aprobar la Política General de Seguridad de la Información obtenida como resultado del proceso de su revisión y actualización para el cumplimiento de los requisitos técnicos de seguridad y de la normativa vigente.
- Validar el compromiso de la dirección con la seguridad de la información en toda la organización.

Aprobar las estrategias 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, así como también aprobar la obtención de los recursos necesarios para su ejecución.

2. Del Comité de Gestión CNR

Este Comité tiene como responsabilidad, desarrollar, analizar, revisar y discutir temas y/o materias relacionadas con el Sistema de Seguridad de la Información, liderado por un/a Encargado/a, definido en Resolución vigente; este comité estará compuesto además por representantes de diversas áreas y unidades.

Los representantes del Comité, serán los responsables de:

- Liderar la implementación y mejora continua del Sistema de Gestión.
- Asegurar el mantenimiento del Sistema de Gestión Integral, proponiendo y acordando acciones de mejoras para los distintos procesos de la CNR.
- Revisar la Política General de Seguridad de la Información y las Políticas de Seguridad de Información que de ella se desprendan, así como también el Plan de Continuidad de Seguridad de la Información de la CNR.
- Supervisar la implementación de procedimientos y estándares que se desprenden de la presente política.
- Proponer estrategias y soluciones específicas para la implantación de los controles necesarios para la adecuada aplicación de los procedimientos de seguridad establecidos y la debida solución de las situaciones de riesgo detectadas.
- Operativizar los lineamientos y Políticas del Sistema de Gestión, dando cumplimiento a los requisitos, políticas, normativas y procedimientos establecidos y de difundir el conocimiento de los lineamientos y responsabilidades señaladas en la Política de Seguridad Institucional;
- Gestionar los riesgos de la CNR, a través de la elaboración de la Matriz y la ejecución del Plan de Tratamiento de Riesgos.
- Gestionar y monitorear los cambios significativos en la exposición de los activos de información ante riesgos, amenazas y debilidades de seguridad de la información.

- Cautelar los activos de información, mediante el cumplimiento de la Política de Seguridad de la Información de la CNR.
- Proponer estrategias y soluciones específicas para el desarrollo de los controles necesarios, para implementar las políticas establecidas y la debida solución de las situaciones de riesgos detectadas.
- Identificar y proponer estrategias y mejoras a los mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucionales.
- Verificar la ejecución de los procesos internos de la Institución.
- Difundir y promover en sus equipos de trabajo, los instrumentos de gestión; las políticas y los procedimientos de seguridad, y en general toda documentación que se desprenda, así como también su estado de ejecución.
- Reportar a las Jefaturas de los CdR y al Encargado de Seguridad de la Información los incidentes de seguridad y su solución.

Lo anterior, sin perjuicio de las demás funciones que determine el Secretario Ejecutivo de la CNR, y que sean necesarias para el normal funcionamiento del Sistema de Seguridad de la Información de la CNR.

3. Del/De la Encargado/a de Seguridad de la Información de la CNR

- Tener a su cargo la Política de Seguridad de la Información al interior de la Institución y velar por su correcta aplicación y supervisar el desarrollo de estas.
- Identificar y controlar los requerimientos de seguridad de la información para los activos de seguridad de la CNR, gestionando con los respectivos responsables de los activos de información la implementación de medidas de seguridad para asegurar la operación contemplando controles para asegurar la disponibilidad, integridad y confidencialidad.
- Asesorar de manera permanente a la Jefatura en materia de Seguridad de la Información.
- Generar e implantar políticas de seguridad de la información, alineando la seguridad de la información con los objetivos de negocio, revisando y actualizando las políticas de seguridad necesarias para aumentar los niveles de seguridad.
- Revisar y analizar los incidentes o eventos de seguridad de la información que le son reportados.
- Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
- Proponer instancias de mejoramiento que impliquen un desempeño eficiente de la Seguridad de la Información al interior de los procesos de la CNR.

- Coordinar reuniones de trabajo, atingentes a la Seguridad de la Información, entre los diferentes estamentos internos o externos de la CNR.
- Promover la difusión de la Política de General de Seguridad de la Información de la CNR

4. De los usuarios/as internos o externos

- Los/as usuarios/as y dueños de los activos de información son responsables de cautelar el cumplimiento de los lineamientos, las normas asociadas a la Seguridad de la Información, salvaguardando la integridad, disponibilidad y confidencialidad de los activos de información a su cargo o utilización.
- Cada vez que algún usuario/a detecte actividad anormal, sospechosa o producto de alarmas, deberán reportar el incidente en el Sistema de Servicios Generales (Mesa de Ayuda) existente en la CNR.
- Es responsabilidad de los usuarios ingresar solo a los servicios e instalaciones para los cuales han sido autorizados.
- Los usuarios de la CNR deberán conocer la Política General de Seguridad de la Información de la CNR, comprometiéndose a cumplirla.

5. De los Administradores de los Servicios

Los Administradores de los Servicios de los respectivos centros de responsabilidad velarán por el desarrollo la documentación técnica asociada con las actividades de administración, soporte y procesamiento de los respectivos Servicios a su cargo, controlando la gestión de los cambios que se pudieran generar sobre dichos Servicios, para garantizar que dichos cambios no provoquen impacto negativo en los activos de información y los servicios que son ofrecidos por la CNR.

- Implementar los niveles de seguridad capaces de responder las exigencias y lineamientos de la guía técnica para el desarrollo de Software de MinSegpres.
- Realizar verificaciones, de la efectividad de los cambios o mejoras realizadas para mantener los servicios estables y seguros.
- Desarrollar y mantener la continuidad operativa de los servicios a su cargo y administración en la CNR.
- Asegurar que los contratistas, proveedores y terceros que tengan acceso a los activos de información que tienen a su cargo o administración en la CNR, estén obligados a cumplir las políticas de Seguridad de la Información de la CNR.

6. De los contratistas, proveedores y terceros

Los contratistas, proveedores y terceros que presten algún servicio a la CNR, y que tengan acceso a los activos de información de la CNR, están obligados a cumplir las políticas.

7. Del/ De la Coordinador/a Área de Gestión Estratégica y/o Representante de la Dirección del Sistema de Gestión de la Calidad

Es el/la responsable de:

- Controlar en forma oportuna el levantamiento, la actualización y mejora de los procesos y procedimientos relacionados a la Seguridad de la Información.
- Supervisar el Control Documental de las Políticas de Seguridad de la Información, de los procedimientos, instructivos y/o registros que de ella se desprendan. Incluir dentro de la revisión por la Dirección todos los aspectos relevantes atingentes a la seguridad de la Información.
- Liderar el Comité de Gestión en aspectos relacionados con seguridad de la información, de acuerdo con lo señalado en la Resolución vigente que crea y nombra el Comité de Gestión de la CNR.
- Crear y coordinar las instancias de integración de los diferentes Sistemas de Gestión de Calidad, Riesgos y Seguridad de la Información al interior de la CNR y de sus procesos.

SEGREGACIÓN DE DEBERES

CNR se compromete a velar por la segregación de deberes, reduciendo con ello las oportunidades de modificación, uso indebido y acceso no autorizado o intencional a los activos de información. Por tal motivo, se realiza la detección y definición de perfiles, donde se señalan las funciones de cada cargo en las áreas de la Institución, con la finalidad de evitar posibilidades de colusión o el uso indebido o accidental de activos de información.

Por tal motivo y como requisito mínimo se cuenta con un organigrama específico e identificación de perfiles de cargos de las Unidades (nombre, dependencia, jefatura directa, personas a cargo y su reemplazo en caso de ausencia), el objetivo general del cargo, los conocimientos mínimos y requisitos de formación, sus principales funciones, las competencias transversales y específicas.

Lo anterior, sin perjuicio de las demás roles, responsabilidades y funciones que determine esta Secretaria Ejecutiva, y que sean necesarias para el normal funcionamiento del Sistema de Seguridad de la Información de la CNR.

DIRECTRICES

Prohibiciones

En la CNR todo acceso para nuevos usuarios/as a sistemas y servicios estará prohibido a menos que se autorice expresamente.

Están estrictamente prohibidos el uso o descarga de programas de intercambio de archivos (como Kazaa, eMule, eDonkey, Ares, lmesh, Sharezaa, Mega.nz, BitTorrent, etc.), ya que podrían comprometer y poner en riesgo la seguridad, proveen de copias ilegales de material protegido y, además, son grandes consumidores del ancho de banda de Internet que la CNR dispone para la realización de sus funciones.

Quedará prohibido para los proveedores revelar, modificar, destruir o hacer mal uso de la información, cualquiera sea el soporte en que se encuentre contenida.

Se prohíbe comer, beber y fumar en la proximidad de las instalaciones de procesamiento de información.

Queda estrictamente prohibido el uso de programas informáticos que no cuenten con su respectiva licencia y autorización de la Jefatura DAF o la Unidad de Tecnología de la Información y la Comunicación (UTIC).

Todo equipo computacional perteneciente a la CNR, que no cuente con una herramienta de protección contra software malicioso, no podrá ser conectado a la red de datos de la CNR

En la CNR se prohíbe que los/as funcionarios/as se conecten a la red interna de datos institucional con equipos personales a menos que: sea expresamente autorizado y validado por la UTIC; y que dichos equipos cuenten con las debidas actualizaciones de antivirus, parches de seguridad, con software licenciado, debiendo cumplir con los requisitos de Ciberseguridad y su acceso será a través de una conexión VPN.

Está absolutamente prohibido a los/as funcionarios/as del Servicio, divulgar cualquier información de clasificación "Reservada", salvo que sea explícitamente autorizado por el propietario de la información (dueño del proceso).

Queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización de CNR.

Quienes trabajen en conjunto con CNR, no podrán divulgar información sobre los procesos internos de éste.

Se prohíbe a los proveedores dar usos no propios de su responsabilidad, a ningún material o información confiada por CNR.

Excepciones

Se entenderán por excepciones a las políticas de seguridad de la información de la CNR a todos aquellos actos o determinaciones que no están considerados en el cumplimiento de las Políticas de Seguridad de la Información de la CNR los que podrán ser evaluados, asumidos e incluidos frente a casos muy particulares o bajo condiciones puntuales y muy especiales de exclusión en el cumplimiento de las directrices de las Política de Seguridad de la Información, siempre que no infrinjan la legislación vigente ni afecte las directrices de otras Políticas.

En la CNR, las excepciones deberán estar autorizadas únicamente por la Dirección Superior, debiéndose dejar constancia de los riesgos que se asumirán de forma consciente y el período de vigencia de la excepción.

En la CNR, toda solicitud de excepción de alguna política de seguridad deberá ser solicitada con la debida justificación y documentación conforme a la naturaleza del cargo del funcionario solicitante o dado por eventos no contemplados en las directrices de la presente política, previa evaluación de su alcance y de su impacto.

Las solicitudes de excepción son gestionadas a través del Comité de Gestión, quienes velan porque las solicitudes estén documentadas formalmente, justificadas y autorizadas por la Dirección Superior, debiéndose dejar constancia de los riesgos que se asumen, además de detallar las responsabilidades, el motivo que justifica el no-cumplimiento de las políticas, debiendo efectuar monitoreo y seguimiento a través de un proceso de revisión, para determinar si amerita una nueva directriz particular o un cambio en otra ya existente.

PUBLICACIÓN

Evaluación

La Comisión Nacional de Riego se reserva el derecho a modificar la presente Política General de Seguridad de la Información, al menos cada dos años, con el objeto de adaptarla a cambios legislativos o normativos, o a prácticas generales de la Comisión para asegurar su continua idoneidad, eficiencia y efectividad. Cualquier modificación será debidamente anunciada a los funcionarios/as.

Las modificaciones realizadas sobre la política General de Seguridad serán aprobadas por resolución. Así mismo, esta política será difundida a todos/as los/as funcionarios/ as, a través de la Intranet Institucional de la Comisión.

Difusión

1. Comunicación Interna y Externa

En la CNR, la Política General de Seguridad de la Información, se difunde al exterior de la organización y en la página WEB CNR, para ser consultada por usuarios externos y proveedores respectivamente. Esta política también es difundida al interior de la organización, quedando disponible en el Sistema Documental DOCAL y en la INTRANET Institucional para ser consultada por los/as funcionarios/as

2. Plan Comunicacional e inducción a las medidas de seguridad

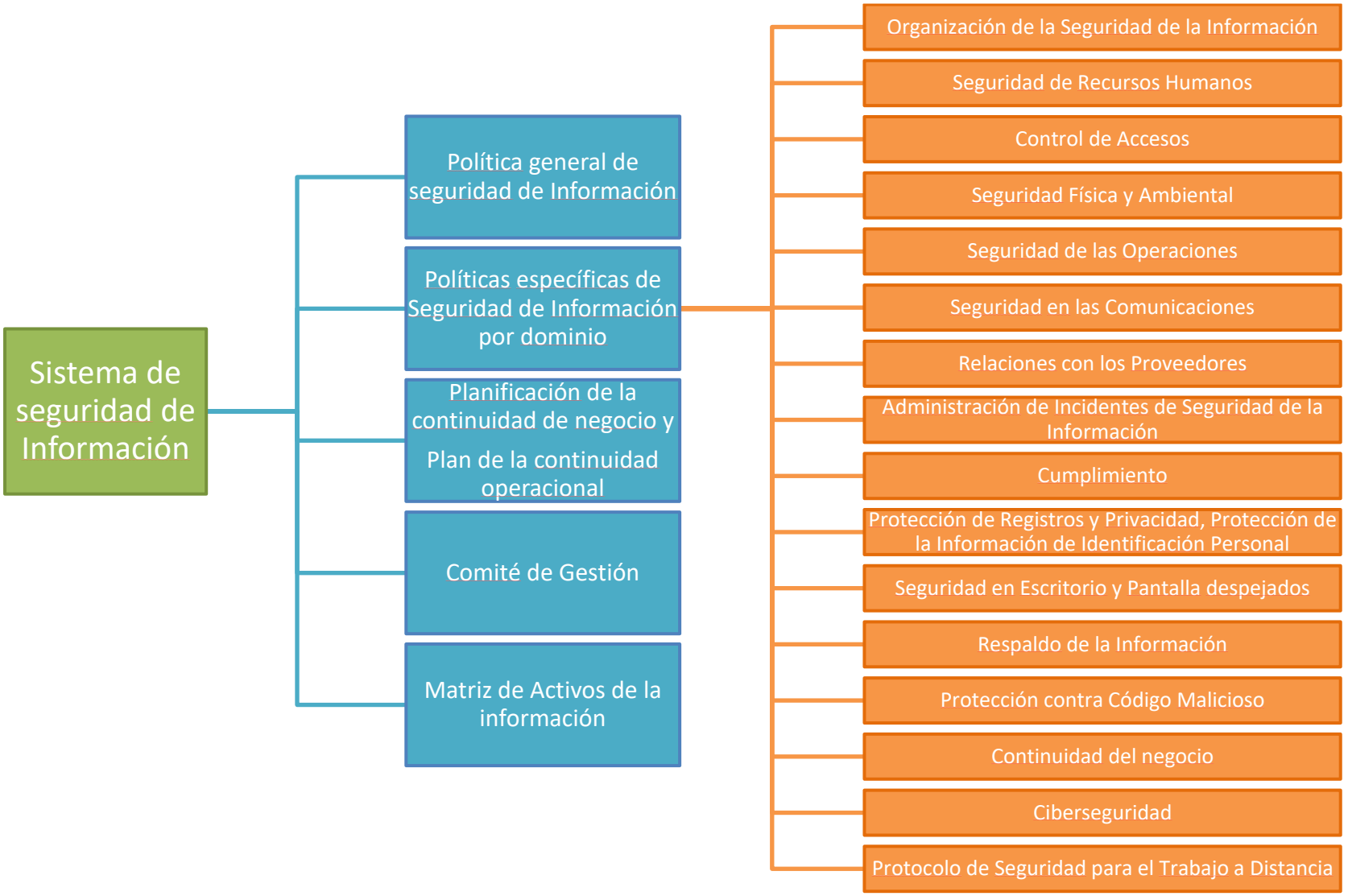
La CNR implementa un Plan Comunicacional anual donde se define como la Institución logrará a través de un proceso formal, la entrega de información e Inducción a sus funcionarios ya sea a través de diversos medios o canales, materiales de difusión, productos, informes, dinámicas, etc., para alinear un comportamiento de sus funcionarios en cuanto a lograr un desempeño eficiente de la Seguridad de la Información y efectuando acciones de difusión e Inducción:

- Comunicaciones Internas: Se difundirá a través de correos electrónicos desde Comunicaciones Internas a todo los/as funcionarios/as de la Institución material en materias de seguridad de la información.
- Intranet: se publicará en la página de internet que dispone la institución para consulta de todos los funcionarios. Además, la Política de Seguridad de la información se deberá mantener actualizada ante todos los cambios, modificaciones o mejoras que puede tener.
- Material Informativo para la Inducción de nuevos funcionarios: se les informa a través de la plataforma de inducción que administra la Unidad de Personas, debiendo la persona comprometerse al respeto de las normas establecidas, a su estudio y aplicación permanente en la Institución.

CRITERIOS GENERALES PARA LA APLICACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Para la aplicación de la presente política, en la CNR se establecen las Políticas específicas de Seguridad de la Información por dominios de la Norma Nch-ISO 27001 a través de las cuales se establecen los controles específicos y los responsables de su desarrollo e implementación, de la vigilancia y del cumplimiento de los requisitos técnicos lo que permitirá verificar y evaluar su efectividad.

MAPA CONCEPTUAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN



ANEXO

NORMATIVA Y REQUISITOS LEGALES APLICABLES

Se establecen los requisitos legales, normativos y contractuales que sustentan el SSI, de manera de evitar incumplimientos y a cualquier requisito de seguridad de conformidad con el control de seguridad de la información Nro. A.18.01.01 de la Norma ISO 27002:2013.

El marco normativo y legal para las políticas de SSI es el siguiente:
Constitución Política de la República de Chile; Decreto N° 100, publicado el 22/09/2005, Ministerio Secretaría General de la Presidencia, Fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile.

Decreto Exento Nº 290, publicado el 28/08/2016, de MINISTERIO DE HACIENDA DIRECCIÓN DE PRESUPUESTOS, que prueba marco de los programas de mejoramiento de la gestión de los servicios en el año 2017.

DS Nº 5996, publicado el 29 abril de 2005, de MINISTERIO DEL INTERIOR; SUBSECRETARIA DEL INTERIOR, que crea red interna (intranet) del estado y entrega su implementación, puesta en marcha, administración, coordinación y supervisión al ministerio del interior.

Ley N° 18.834, Estatuto Administrativo y cuyo texto se refunde en el Decreto con Fuerza de Ley Nº 29 "Fija texto refundido, coordinado y sistematizado de la Ley Nro.18.834, sobre Estatuto Administrativo".

Ley N° 17.336, publicada el 02/10/1970, sobre propiedad intelectual.

Ley N° 19.223, publicada el 07/06/1993, tipifica figuras penales relativas a la informática.

Ley N° 19.628, publicada el 28/08/1999, del Ministerio Secretaría General de la Presidencia, sobre protección de la vida privada; protección de datos de carácter personal.

Ley N° 19.759, publicada el 05/10/2001, que modifica el Código del Trabajo en lo relativo a las nuevas modalidades de contratación, al derecho de sindicación, a los derechos fundamentales del trabajador y a otras materias que indica.

Ley N° 19.799, publicada el 12/04/2002, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

Ley N° 19.880, publicada el 29/05/2003**,** Establece bases de los procedimientos administrativos, que rigen los actos de los órganos de la Administración del Estado (Modificada por Ley 21.180, que establece Transformación Digital del Estado).

Ley N° 20.217, publicada el 12/11/2007, que modifica el Código de Procedimiento Civil y la Ley Nº 19.799 sobre documento electrónico, firma electrónica y los servicios de certificación de dichas firmas.

Ley N° 20.285, publicada el 14/04/2008, sobre acceso a la información pública.

Decreto Nº 5.996, publicado el 12/11/1999, Ministerio de Interior, Subsecretaría del Interior, que crea red interna (intranet) del Estado y entrega su implementación, puesta en marcha, administración, coordinación y supervisión al Ministerio del Interior.

Decreto N° 181, publicado el 17/08/2002, Ministerio de Economía, Reglamento de la Ley Nº 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.

Decreto N° 83, publicado el 12/01/2005, del Ministerio Secretaría General de la Presidencia, aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

Decreto Nº 1.299, publicado el 29/04/2005, del Ministerio de Interior, Subsecretaría del Interior, que establece nuevas normas que regulan la red de conectividad del Estado que administra el Ministerio del Interior y fija los procedimientos, requisitos y estándares tecnológicos para la incorporación a dicha red de instituciones públicas.

Decreto N° 236, publicado el 01/12/2005, del Ministerio de Economía. Fomento y Turismo, Reglamento de la Ley Nº 19.039, de Propiedad Industrial

Decreto N° 93, publicado el 28/07/2006, del Ministerio Secretaría General de la Presidencia, aprueba norma técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la administración del Estado y de sus funcionarios.

Decreto Nº 14, publicado el 27/02/2014, del Ministerio de Economía, Fomento y Turismo; Subsecretaría de Economía y Empresas de Menor Tamaño, que modifica Decreto Nº 181, de 2002, que aprueba reglamento de la ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica.

Decreto Nº 533, publicado el 27/04/2015, del Ministerio del Interior y Seguridad Pública, de 27 de abril de 2015, crea el Comité Interministerial sobre Ciberseguridad.
Decreto Nº 1, publicado el 11/06/2015, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica sobre sistemas y sitios web de los órganos de la administración del Estado.

Norma Nch ISO 27000 Tecnologías de la Información - Técnicas de seguridad - Sistemas de Gestión de la seguridad de la información.

Norma Nch ISO 27001 Tecnologías de la Información - Técnicas de seguridad - Sistemas de Gestión de la seguridad de la información - Requisitos.

Norma Nch ISO 27002 Tecnologías de la Información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información.

Norma NCh ISO 9.001, que específica los requisitos para el sistema de gestión de la calidad para ser utilizada por las organizaciones.

Política Nacional de Ciberseguridad (PNCS) 2017-2022, de 2017 y las leyes y normas a las que hace referencia.

Instructivo Presidencial Nº 001, del 27/04/2017, que Instruye implementación de la Política Nacional sobre Ciberseguridad.

Instructivo Presidencial N° 001, del 19/02/2018, que entrega directrices sobre evaluación y adopción preferente de servicio en la nube por parte de órganos de la Administración Central del Estado.

Instructivo Presidencial Nº 008, del 23/10/2018, imparte instrucciones urgentes en materia de Ciberseguridad para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado.

Instructivo Presidencial Nº 001, del 24/01/2019 sobre Transformación Digital en los órganos de la Administración del Estado.

Resolución N° 123, publicada el 16/03/2011, de la Contraloría General de la República, Fija Normas sobre Comunicaciones Electrónicas e Interoperabilidad con la Contraloría General de la República.

Resolución N° 908, publicada el 10/08/2011, de la Contraloría General de la República, Fija normas sobre registro electrónico de decretos y resoluciones exentos relativos a las materias que indica.

Las Normas relativas al Uso de Correo Electrónico, Navegación y Descarga de Contenido en Internet se basa en las instrucciones sobre el uso de recursos de tecnologías de la información y comunicaciones (TIC) en la Contraloría General de la República, del 22 de octubre de 2008.

Resolución Exenta N° 585, del 12/02/2020, de la Comisión Nacional de Riego, que Nombra al Comité de Gestión de la CNR.

Resolución Exenta N° 709, del 06/02/2019, de la Comisión Nacional de Riego, que Nombra Encargado de Seguridad de la Información.

Protocolo de seguridad para trabajo a distancia, del 16/03/2020, del Ministerio del Interior, CSirt.

En cuanto a los requisitos contractuales, la CNR, a través de sus áreas, adopta las medidas necesarias para incorporar en sus contratos a honorarios, bases de licitación, contratos con proveedores o convenios, cláusulas con el objeto de resguardar la protección que brinda el Sistema de Seguridad de la Información a los activos de información existentes en la institución.

Asimismo, en los nombramientos, designaciones o acuerdos que no consten en contratos o convenios, la CNR solicita la suscripción de una declaración jurada que señale los compromisos en relación con el Sistema de Seguridad de la Información en la CNR.

2. **DEJESE SIN EFECTO** la Resolución Exenta N° 4875 de fecha 03 de octubre de 2019, de la Política General de Seguridad de la Información de la Comisión Nacional de Riego.

FEDERICO ERRÁZURIZ TAGLE
Secretario Ejecutivo

PLUE/PPCG/EFD/CZP/CCA/ahv
Distribución Electrónica:
Pedro León Ugalde - Jefe División Jurídica
Luis Negroni – Análisis Jurídico y Asuntos Legales
Enrique Foster - Coordinador Área Gestión Estratégica
Claudio Zaror - jefe Administración y Finanzas
Claudio Camblor - Encargado Sistema Seguridad de la Información
Karin Abarzúa – Coord. Auditoría
Sebastián Casabonne – Coord. Unidad de Tecnología y Comunicaciones
Daniella Pinto – Coord. Unidad Personas y Bienestar
José Torres – Coord. Unidad Administración y Compras Públicas
Oficina de Partes