MATERIA: DEJE SIN EFECTO LA RESOLUCIÓN N° 1597/2023, Y APRUEBA MODIFICACIÓN POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA COMISIÓN NACIONAL DE RIEGO.

SANTIAGO, miércoles, 22 de octubre de 2025

RESOLUCION EXENTA Nº 08413/2025

VISTOS:

Lo dispuesto en el DFL Nº 7, de 1983, que fija texto refundido del DL Nº 1.172, de 1975, modificado por la Ley Nº 19.604, que creó la Comisión Nacional de Riego; Decreto Supremo N° 48, de 2022, del Ministerio de Agricultura; DS Nº 179, de 1984, que fija el texto actualizado del DS Nº 795, de 1975, que aprobó el Reglamento de la Comisión antedicha, todos del Ministerio de Economía, Fomento y Reconstrucción; Ley Nº 18.450, que aprueba normas para el Fomento a la Inversión Privada en Obras de Riego y Drenaje; Decreto Supremo Nº 95, del Ministerio de Agricultura, que aprueba nuevo Reglamento de la Ley Nº 18.450, sobre Fomento a la Inversión Privada en Obras de Riego y Drenaje; y el artículo 102 de la ley N°21.647; el Decreto Nº 11 de 2023 del Ministerio Secretaría General de la Presidencia, que establece norma técnica de calidad y funcionamiento de las plataformas electrónicas que sustentan procedimientos administrativos en los órganos de la administración del estado; el DS N°83 de 2005, del ministerio secretaría general de la presidencia, que aprobó la norma técnica para los órganos de la administración del estado, sobre seguridad y confidencialidad de los documentos electrónicos ; el DS N°164 de 2023 que aprobó la política nacional de ciberseguridad 2023-2028; la Ley N°21.663/2024 Ley Marco de Ciberseguridad, que regula la normativa general aplicable a las acciones de ciberseguridad de los organismos del Estado y establece los requisitos mínimos para enfrentar incidentes de ciberseguridad; el Decreto N° 295, de 2024, del Ministerio del Interior y Seguridad Pública que aprueba el reglamento de reporte de incidentes de ciberseguridad de la ley N° 21.633; el decreto N° 273, de 2022 que establece obligación de reportar incidentes de ciberseguridad, todos del ministerio del interior y seguridad pública; Ley N° 21.719/2024: La Ley de Protección de Datos Personales que regula la forma y condiciones en las que se realiza el tratamiento de este tipo de información y mejorar la protección de los derechos de sus titulares, del ministerio secretaría general de la presidencia; Resolución CNR Exenta N° 1597 de 2023 y Resolución CNR Exenta N° 4539 de 2022.

CONSIDERANDO:

1.- 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.

2.- 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.

3.- 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.

4.- 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.

5.- Que de conformidad a la Norma ISO 27.001 la 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.

6.- 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, N° 4875 del 03 de octubre de 2019, N° 2820 de 2020 del 15 de septiembre de 2020 y N° 5866 de 2019, Nº:0453 del 18 de octubre del 2022 y Nº1597 del 11 de Abril del 2023, se aprobaron las Políticas de Seguridad de la Información de la Comisión Nacional de Riego

7.- 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:

PRIMERO: MODIFÍQUESE la Resolución CNR Exenta Nº1597 de fecha 11 de Abril del 2023.

SEGUNDO: APRUÉBESE la Política de General de Seguridad de la Información de la Comisión Nacional de Riego, cuyo texto es el siguiente y forma parte integrante de este acto administrativo.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN
COMISIÓN NACIONAL DE RIEGO

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 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 específicas y de las materias 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 el Inventario de Activos de Información, el 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 del inventario 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, en los contratos que se redacten incorporando cláusulas de seguridad de la información, incluidas las cláusulas de seguridad establecidas en el marco regulatorio de la Ley Marco de Ciberseguridad.

En la CNR, el ámbito de aplicación de la Política de Seguridad de la Información contempla dominios y controles contenidos en la Nch-ISO 27002

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 comprendan sus responsabilidades y adecuados para los roles en los que 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 o el compromiso 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 y la Ley N°21.663/2024 Ley Marco de Ciberseguridad.
16	**Protocolo trabajo a distancia**	Entrega directrices para resguardar la seguridad en el Trabajo a Distancia.

CONTEXTO DE LA ORGANIZACIÓN

En la CNR se desarrolla el Sistema de Gestión de Seguridad de la Información identificando los activos de información, los principales actores, las amenazas y los riesgos a los que podrían estar expuestos con el propósito de definir las capacidades, e identificar el nivel de madurez en materias se seguridad y tomar las medidas necesarias para garantizar su resguardo y protección, pudiéndose generar con ello la confianza en los servicios esenciales que la CNR entrega a los ciudadanos y cumplir con los objetivos y productos estratégicos de la institución.

En la CNR, se identifica el inventario de activos de información, el cual es la línea base que permite a toda organización identificar los elementos críticos e importantes a los cuales debemos brindar una mayor protección y resguardo, ya que dichos activos son los requeridos para que las organizaciones funcionen y consigan los objetivos propuestos.

En la CNR, los activos de información que son identificados y analizados mediante un proceso anual llevado a cabo por el Comité de Gestión de la CNR el cual está integrado por representantes de las respectivas áreas de negocio de la institución, generándose un instrumento denominado Inventario de Activos de Información de la CNR.

En este proceso de identificación se analiza, entre otros, cómo podrían verse afectadas la confidencialidad, la integridad y la disponibilidad de la información, cuál es el valor agregado de los activos de información para la organización, qué impacto tendría la divulgación de información así como también se identifica cuál sería el impacto de la pérdida de confianza en la integridad de su información al ser difundida de forma no autorizada además de identificar y evaluar las vulnerabilidades que podrían afectar a la Seguridad de la Información y en consecuencia al propósito de la organización y a su capacidad para lograr los resultados esperados debido a la influencia de los agentes externos e internos en los que está inmersa la actividad de la organización.

Dicho instrumento permite a la CNR identificar propiedades y atributos como los siguientes:

- Tipo de activo y su ubicación
- Responsable o dueño del activo, Personas autorizadas para manipular, Personas autorizadas para copiar.
- Medio de almacenamiento, Tipo de Soporte, Tipo de Procesamiento y su transmisión
- Tipo de eliminación/destrucción, Tiempo de retención antes de eliminarse y su disposición.
- Criterio de búsqueda, Niveles de Confidencialidad, Integridad y Disponibilidad
- Amenazas, vulnerabilidades/debilidades, Riesgos y probabilidad de ocurrencia
- Impacto y severidad, Criticidad e Impacto de divulgación

- Controles de la norma de Seguridad ISO-27.001 para mitigar riesgos.
- Resultados esperados

De esta forma, en la CNR la Seguridad de la Información se gestiona y gobierna mediante un grupo de actores y representantes con perspectivas de todas las partes interesadas tanto internas como externas a la institución, y que cuentan con el conocimiento y las capacidades para desarrollar los procesos de análisis, evaluación de riesgos y la evaluación de la efectividad de las medidas desarrolladas para garantizar la seguridad de la información sobre los diversos procesos y productos estratégicos de la institución.
En tal sentido, para alcanzar los objetivos de la seguridad de la información, en la CNR se establecen roles y responsabilidades, se desarrollan políticas, procedimientos e instructivos en pos de dar cumplimiento con los requisitos legales y reglamentarios, las normativas, las directrices y los modelos adoptados por la organización, así como las obligaciones contractuales que deben incluirse en los requisitos de las partes interesadas, además de disponibilizar las capacidades, entendidas en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías).

LIDERAZGO, 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.

Del Director 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.

Representantes 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 y Ciberseguridad; este comité estará compuesto 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 de Seguridad de la Información.
- 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 general de Seguridad de la Información, así como también de las políticas Específicas de Seguridad de la Información de la CNR.
- Proponer estrategias y soluciones específicas para la implantación de los controles para la adecuada aplicación de los procedimientos de seguridad establecidos y la debida solución y monitoreo de las situaciones y notificaciones de riesgo detectadas sobre los activos de información de las áreas de negocio o unidades que representan.
- 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.
- Velar y cautelar los activos de información, mediante el cumplimiento de las Políticas 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 áreas de negocio 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 centros de responsabilidad y al Encargado de Seguridad de la Información los incidentes de seguridad/ciberseguridad y los avances de solución o remediación.

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

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.

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

- Tener a su cargo la elaboración de la Política General de Seguridad de la Información al interior de la Institución.
- Identificar y controlar los requerimientos de seguridad de la información para los activos de seguridad de la CNR, gestionando y requiriendo a los respectivos responsables de los activos de información la implementación de medidas y remediaciones de seguridad para asegurar la operación contemplando controles para asegurar la disponibilidad, integridad y confidencialidad.
- Asesorar a la Jefatura en materia de Seguridad de la Información.

- Revisar y actualizar las Políticas Específicas de seguridad de la información, alineando la seguridad de la información con los objetivos de negocio.
- 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.
- 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.
- Es contraparte con la Agencia Nacional de Ciberseguridad.

Del/De la Coordinador/a de la Unidad de Tecnología de la Información y la Comunicación

- Proveer del soporte, mantenimiento y la administración de la infraestructura y plataforma de los servicios tecnológicos garantizando de manera eficiente, efectiva, segura y oportuna la correcta y continua entrega de los servicios tecnológicos que satisfagan las necesidades operacionales informáticas y de comunicaciones de la CNR.
- Identificar, controlar y remediar prontamente situaciones de riesgo que podrían afectar a los activos de información, los servicios, las plataformas tecnológicas y la información existentes en la CNR, garantizando que estos no se vean impactados o comprometidos.
- Desarrollar y actualizar las políticas, los procedimientos/instructivos documentados para los controles de seguridad y las actividades asociadas a la tecnología de la información existente en la CNR.
- Controlar los accesos a las plataformas, los sistema y los servicios, controlando los cambios asociados con la infraestructura tecnológica y los sistemas de información.
- Remediar prontamente las alertas y vulnerabilidades técnicas de seguridad que sean identificadas.
- Dar cumplimiento con los controles de seguridad de su responsabilidad indicados en las Políticas Específicas de Seguridad de la Información.
- Asegurar que los contratos de proveedores de tecnología se incluyan las cláusulas de Ciberseguridad conforme a lo indicado en el Decreto N°273, de 2022 y la Ley N°21.663/2024, Ley Marco de Ciberseguridad del Ministerio del Interior y Seguridad Pública.
- Gestionar con proveedores externos la remediación de alertas y vulnerabilidades técnicas de seguridad.

Del/De la Coordinador/a de la Unidad de Gestión de Personas

- Notificar a todo el personal que ingresa al Servicio, de sus obligaciones respecto del cumplimiento de las Políticas de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.
- Suscribir los compromisos de Confidencialidad que sean requeridos con el personal o con terceros que desarrollen funciones al interior de la CNR.
- Considerar en el Comité Bipartito de Capacitación de la CNR la realización de actividades de inducción en materias de Seguridad de la Información.

Del/De la Coordinador/a Análisis Jurídico y Asuntos Legales

- Identificar la legislación vigente, los requisitos legales y reglamentarios para ser considerados en materias contractuales.
- Verificar el cumplimiento de la presente Política en la celebración de los contratos, los acuerdos u otra documentación que emane de la CNR con sus empleados y con terceros.
- Revisar y gestionar el cumplimiento de medidas de protección a los registros para garantizar el derecho a la privacidad y proteger los datos personales de las personas.
- Incorporar en los contratos que CNR celebre con los proveedores de tecnologías, las exigencias de la Ley Marco de Ciberseguridad en el sentido de exigir a los proveedores de servicios de tecnologías de la información que compartan la información sobre las amenazas y vulnerabilidades que puedan afectar a las redes, plataformas y sistemas informáticos de los órganos de la administración del Estado, al igual que las medidas de mitigación aplicadas a éstas, así como las políticas y prácticas de seguridad de la información incorporadas en los servicios prestados.
- Supervisar el desarrollo y aprobación de la Política de Privacidad y Protección de la Información de Identificación Personal.
- Asesorar a la CNR en lo que se refiere a materias legales atingentes a la Seguridad de la Información y Ciberseguridad.
- Revisar, actualizar y validar el catastro normativo aplicable a la Seguridad de la Información y Ciberseguridad, determinando su aplicabilidad al contexto organizacional, cuando así le sea requerido.

De los Administradores de los Sistemas de Información y Servicios digitales de las respectivas Unidades y Áreas de Negocio

Los Administradores contrapartes encargadas de los Sistemas de Información y Servicios digitales pertenecientes a 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.

- Deberán gestionar la implementación de niveles de seguridad capaces de responder las exigencias y lineamientos de la guía técnica para el desarrollo de Software de MinSegpres y la Ley N°21.663/2024, Ley Marco de Ciberseguridad.
- Realizar verificaciones, de la efectividad de los cambios o mejoras realizadas para mantener los servicios estables y seguros.
- Gestionar y solicitar la pronta remediación de las vulnerabilidades técnicas y alertas de ciberseguridad identificadas.
- Desarrollar y mantener la continuidad operativa de los servicios a su cargo y administración en la CNR.
- Incorporar en los contratos que CNR celebre con los proveedores de tecnologías, las exigencias de la Ley Marco de Ciberseguridad en el sentido de exigir a los proveedores de servicios de tecnologías de la información que compartan la información sobre las amenazas y vulnerabilidades que puedan afectar a las redes, plataformas y sistemas informáticos de los órganos de la administración del Estado, al igual que las medidas de mitigación aplicadas a éstas, así como las políticas y prácticas de seguridad de la información incorporadas en los servicios prestados.
- Asegurar que, los contratistas, los proveedores y terceras personas que tengan acceso a los activos de información que tienen a su cargo en la CNR, estén obligados a cumplir las Políticas de Seguridad de la Información de la CNR.

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 y Ciberseguridad, 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 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.
- Los usuarios de la CNR deberán conocer la Política General de Seguridad de la Información de la CNR, comprometiéndose a cumplirla.

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 de CNR.
- Los Proveedores, contratistas y terceros a la CNR, deberán salvaguardar los bienes, los accesos, los datos y los activos digitales facilitados por la Comisión Nacional de Riego, debiendo asegurar de esta manera la integridad, la confidencialidad y la disponibilidad de los activos de la información existentes en la CNR.
- Para dar cumplimiento de la Política de Seguridad de la Información de la CNR, es que, se informa al proveedor de su disponibilidad y cumplimiento, el cual ha sido señalado en la página web de la institución (https://www.cnr.gob.cl), la que incluye información de la relación que debe existir entre CNR y sus proveedores de servicios. El proveedor se compromete en este acto a dar cumplimiento a esta política.
- Los proveedores de servicios de tecnologías de la información, deberán compartir la información sobre las amenazas y vulnerabilidades que puedan afectar a las redes, plataformas y sistemas informáticos, al igual que las medidas de remediación o mitigación aplicadas a éstas, así como las políticas y prácticas de seguridad de la información incorporadas en los servicios prestados.
- De acuerdo con los contratos de prestación de servicios los proveedores deberán informar sobre amenazas por parte del prestador de servicios, siempre y cuando con ello no se comprometa la seguridad y protección de datos, incluida la confidencialidad y protección de la propiedad intelectual.
- En este mismo sentido, el proveedor deberá adoptar todas las medidas de resguardo necesarias a efecto de impedir actos que puedan dañar la seguridad de la información de la institución, así como a remediar a la brevedad las alertas y vulnerabilidades que atenten contra la seguridad informática o la ciberseguridad en la CNR.
- El proveedor deberá otorgar oportunamente a la CNR la mantención y soporte con objeto de mantener el correcto funcionamiento de los servicios contratados, donde se deberán incluir actualizaciones, parches de seguridad, control de licencias, control de versiones, control de errores y correcciones, control y optimización de las bases de datos, como así mismo, aquellas intervenciones menores que no signifiquen desarrollo de piezas de software propiamente tal, las cuales podrán ser resueltas mediante las herramientas de edición disponibles.

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 Dirección Ejecutiva de la CNR, 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 la descarga, el uso e instalación de programas de intercambio o almacenaje de archivos (como Kazaa, eMule, eDonkey, Ares, lmesh, Sharezaa, Mega.nz, BitTorrent, Dropbox, WesTranfer, etc.), ya que podrían comprometer y poner en riesgo la seguridad y la privacidad de los dates, además de 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 y detección 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 y el Encargado de Seguridad de la Información, 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.

SOPORTE

RECURSOS Y COMPETENCIAS

Para la correcta implementación y el mantenimiento del Sistema de Gestión de la Seguridad de la Información, la CNR identifica y proporciona todos los recursos que se necesitan para su establecimiento.

Además, la CNR identifica qué competencia personal es la necesaria para realizar cada trabajo que afecta al desempeño de la seguridad de la información asegurándose:

- Que el personal es competente, fundamentándose en la educación, formación o experiencia.
- Tomar acciones, cuando sea necesario, para adquirir la competencia necesaria.
- Que, como pruebas de esta competencia, conserva la información documentada pertinente.

CONCIENTIZACIÓN DE LAS MEDIDAS DE SEGURIDAD

La CNR establece que la concientización en materias de seguridad de información se 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, 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/Ciberseguridad.
- 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.
- Inducción de nuevos funcionarios: Se les informa a través de una charla, debiendo la persona comprometerse al respeto de las normas establecidas, a su estudio y aplicación permanente en la Institución.

COMUNICACIÓN INTERNA Y EXTERNA

En la CNR, la Política General de Seguridad de la Información, se difunde al exterior de la organización en la página web institucional, para ser consultada por usuarios externos, proveedores y partes interesadas. 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

GESTIÓN DOCUMENTAL

Para la aplicación de la presente política, en el marco del sistema de gestión de calidad existente en la CNR se establece la gestión documental como el conjunto de normas técnicas y prácticas usadas para administrar los documentos creados en la organización por medio de la cual la CNR controla y mantiene la información documentada para asegurar que se encuentre disponible para su uso, dónde y cuándo se necesite y protegida adecuadamente. Es decir, que no haya riesgos de pérdida de confidencialidad considerando su distribución, el acceso, la recuperación adecuada de la información y el correcto almacenamiento y preservación de documentos, así como también el control de cambios.

OPERACIÓN

En la CNR, a través de los respectivos responsables de implementación y operación de los controles se seguridad de la información definidos en las Políticas Específicas de Seguridad de la Información por Dominios en la CNR, se pone en operación el funcionamiento del sistema de Gestión de Seguridad de la Información, abordando materias como el seguimiento y el control operacional de los requisitos técnicos, la evaluación de los riesgos y el tratamiento o mitigación de riesgos de la seguridad de la información.

PLANIFICACIÓN Y CONTROL OPERACIONAL

En la CNR se toman las medidas adecuadas para lograr los objetivos de la Seguridad de la Información y seleccionado los controles que deben implementarse para abordar los riesgos y oportunidades de la seguridad de la información como parte de la planificación del sistema de gestión de la seguridad de la información de la CNR

EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En la CNR se identifican los activos de información y se realiza su evaluación de riesgos de seguridad e implementar evaluaciones de riesgos, identificando los controles necesarios que deben ser implementados para asegurar que la información supere un determinado nivel de riesgo establecido según los criterios establecidos por la institución.

TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Finalmente, en la CNR se implementa el tratamiento de riesgos de seguridad de la información y, se registran los resultados de los indicadores establecidos.

El tratamiento de riesgos se debe llevar a cabo después de aplicar las evaluaciones de riesgos de seguridad para garantizar que se implementen los controles o mitigaciones correctas.

EVALUACIÓN DEL DESEMPEÑO

En la CNR, para el Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27002 ante la instrucción de la Dirección, se podrá hacer necesario llevar a cabo auditorías internas cada cierto tiempo para poder comprobar que el estado del Sistema de Gestión de Seguridad de la Información sea el idóneo.

El principal objetivo es realizar auditorías internas en la CNR para poder determinar si los objetivos, los controles, los procesos y los procedimientos asociados a la Seguridad de la Información se encuentran:

- Conforme a los requisitos que establece el estándar internacional de la norma ISO27002, la normativa regulatoria y los lineamientos señalados por Gobierno.
- De acuerdo y conforme a la legislación y la normativa vigentes.
- Acorde a los requisitos técnicos establecidos para seguridad de la información.
- Implementados y mantenidos eficazmente.
- Habilitados, en operación y comportándose de la manera esperada

Las auditorías podrán ser realizadas por auditores independientes del personal o el área de negocio a auditar o que tengan algún tipo de responsabilidad directa respecto a la actividad que será auditado, por lo que el auditor:

- No puede ser el responsable ni pertenecer a la unidad o área de negocio a ser auditada.
- No podrá formar parte de una unidad o área de negocio dependiente del proceso auditado.

Las responsabilidades en torno a las auditorías internas se establecerán, es decir, se debe conocer quién(es) es(son) las personas encargadas de la realización de las auditorías y quienes serán las unidades o áreas de negocio auditadas y sus responsables.
La unidad o área de negocio auditada deberá llevar a cabo las acciones necesarias para subsanar las no conformidades que se hayan detectado en los procesos de auditoría interna y fundamentar las razones o motivos que causaron la no conformidad lo antes posible.
En resumen, en la CNR se podrán realizar auditorías de evaluación del desempeño para comprobar el estado del Sistema de Gestión de Seguridad de la Información y así poder determinar el estado de cumplimiento de los controles y los procedimientos implantados que cumplen los requisitos establecidos por la norma ISO 27002.

ACCIONES DE MEJORA, CORRECTIVAS Y SEGUIMIENTO DE AUDITORÍAS

Si como resultado del proceso auditoría se han detectado desviaciones a los requisitos de cumplimiento, el auditor deberá realizar las comprobaciones necesarias para corroborar que se están aplicando las acciones o remediaciones propuestas dentro del plazo de tiempo establecido para cada una de ellas.
Durante el seguimiento de las actividades realizadas se incluirá la verificación de las acciones que se han llevado a cabo para corregir las desviaciones detectadas durante la auditoría, además de un informe que indique la verificación de los resultados obtenidos los que podrán quedar reflejados en el apartado de cierre de esta. Si por algún motivo persiste o se reiteran las desviaciones, y estas podrían afectar al buen funcionamiento del Sistema de Gestión de Seguridad de la Información, entonces .el auditor deberá informar a la alta dirección de la organización.

Cuando se detecte alguna no conformidad, la Unidad responsable o Área de negocio deberá:

- Revisar la no conformidad e identificar su(s) causa(s).
- Reaccionar ante ella y emprender acciones para controlarla y corregirla.
- Evaluar la necesidad de ejecutar acciones que eliminen las causas que produjeron la no conformidad, con el objetivo de que no vuelva a producirse.
- Comprobar la eficacia de las acciones correctivas que se han tomado, debiendo quedar como información documentada los resultados de este proceso como evidencias de:
  - La naturaleza de la no conformidad y las acciones emprendidas.
  - Los resultados de las acciones correctivas.

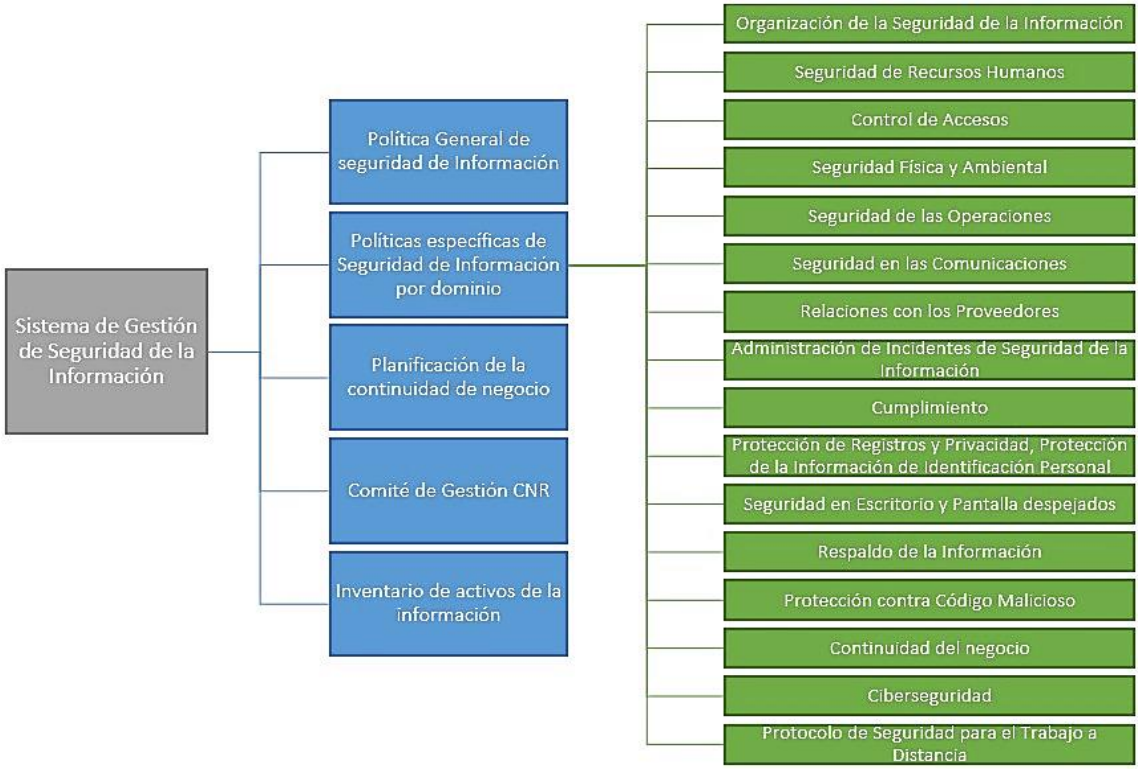
DECLARACIÓN Y CRITERIOS GENERALES PARA LA APLICACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

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 ISO 27002 a través de las cuales se disponen 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.
Todos los controles de seguridad de la información señalados en las Políticas Específicas de Seguridad de la Información por Dominios de la CNR, son aceptados y asumidos por la institución en el marco del Sistema de Gestión de Seguridad de la Información, el que tiene por objetivo la adopción de medidas y actividades que contribuyan a la protección de la información, el cumplimiento de los requisitos y las recomendaciones de la Norma ISO 27002. En función de lo anterior, en la CNR son definidos lineamientos y llevadas a cabo actividades y tareas asociadas a dichos controles de seguridad, los que son aplicados con el objetivo de salvaguardar y proteger los activos de información críticos de la CNR, gestionando los riesgos, dando cumplimiento con los requisitos reglamentarios y las obligaciones contractuales, y satisfaciendo las necesidades de la organización en materias de seguridad de la información.

REVISIÓN Y ACTUALIZACIÓN

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.

SISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CNR (mapa conceptual)



ANEXO

NORMATIVA Y REQUISITOS LEGALES APLICABLES

En la CNR se establecen los requisitos legales, normativos y contractuales que sustentan el sistema de Gestión de Seguridad de la Información, 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 Seguridad de la Información 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.
Decreto Nº 21459, publicado el 20/06/2022, del Ministerio de Justicia y Derechos Humanos, que establece normas sobre delitos informáticos Norma Nch ISO 27000 Tecnologías de la Información - Técnicas de seguridad - Sistemas de Gestión de la seguridad de la información. Norma ISO 27001 Tecnologías de la Información - Técnicas de seguridad - Sistemas de Gestión de la seguridad de la información Requisitos.
Norma ISO 27002 Tecnologías de la Información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información.
Norma 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.
Decreto Nº 11 de 2023, del Ministerio Secretaría General de la Presidencia, que establece norma técnica de calidad y funcionamiento de las plataformas electrónicas que sustentan procedimientos administrativos en los órganos de la administración del estado
Decreto Supremo N°83 de 2005, del Ministerio Secretaría General de la presidencia, que aprobó la norma técnica para los órganos de la administración del estado, sobre seguridad y confidencialidad de los documentos electrónicos
Decreto Supremo N°164 de 2023, del Ministerio Secretaría General de la presidencia, que aprobó la Política Nacional de Ciberseguridad 2023-2028;
Ley N°21.663/2024 Ley Marco de Ciberseguridad, que regula la normativa general aplicable a las acciones de ciberseguridad de los organismos del Estado y establece los requisitos mínimos para enfrentar incidentes de ciberseguridad
Decreto N° 295, de 2024, del Ministerio del Interior y Seguridad Pública que aprueba el reglamento de reporte de incidentes de ciberseguridad de la información
Ley N° 21.633, publicada el 08/04/24, del Ministerio del Interior y Seguridad Pública, Ley Marco de Ciberseguridad.
Decreto N° 273, de 2022, que establece obligación de reportar incidentes de ciberseguridad, todos del ministerio del interior y seguridad pública
Ley N° 21.719/2024, Ley de Protección de Datos Personales que regula la forma y condiciones en las que se realiza el tratamiento de este tipo de información y mejorar la protección de los derechos de sus titulares, del ministerio secretaría general de la presidencia;
Resolución CNR Exenta N° 1597 de 2023 y Resolución CNR Exenta N° 4539 de 2022 que aprueban las Políticas de Seguridad de la CNR
Resolución Exenta N° 01053/2025, del 12/02/2025, 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 y Reemplazante de Seguridad de la Información.
Protocolo de seguridad para trabajo a distancia, del 16/03/2020, del Ministerio del Interior, CSirt de Gobierno.
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.

TERCERO: ESTABLÉZCASE que la Política General de Seguridad de la Información de la Comisión Nacional de Riego entrará en vigor a contar de la fecha de la total tramitación del presente acto administrativo.

CUARTO: DIFÚNDASE ampliamente la Política General de Seguridad de la Información de la Comisión Nacional al de Riego, contenida en el presente acto, por los medios institucionales idóneos para su correcta difusión.

FIRMA ELECTRÓNICA AVANZADA · COMISIÓN NACIONAL DE RIEGO ·

WILSON URETA PARRAGUEZ
DIRECTOR EJECUTIVO
COMISIÓN NACIONAL DE RIEGO

DBA/PCP/AGJ/SCV/CCA