MAT: DEJE SIN EFECTO LA RESOLUCIÓN N° 2821/2020, Y APRUEBA POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA COMISIÓN NACIONAL DE RIEGO

SANTIAGO, 18/ 10/ 2022

RESOLUCION EXENTA Nº: 04539/2022

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 48 del 2022 del Ministerio de Agricultura y la Resolución Nº 7 de 2019 de la Contraloría General de la República; Resolución CNR Exenta N° 2820 y 2821 de 2020 y Resolución CNR Exenta N° 5866 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 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. 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 y 2821 de 2020 del 15 de septiembre de 2020 y Resolución CNR Exenta N° 5866 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:

APRUÉBASE LAS POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA COMISIÓN NACIONAL DE RIEGO

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Declaración de Aplicabilidad
La presente declaración establece la aplicabilidad de los dominios y controles de Seguridad de la Información señalados en las Políticas de Seguridad de la Información de la CNR, todos los cuales 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 Nch.ISO 27001.
En función de lo anterior, en la CNR son definidos lineamientos y que deben ser llevadas a cabo, como actividades y tareas asociadas al cumplimiento de 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.

POLÍTICA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La presente política declara su aplicabilidad para el control definido en la Norma NCh-ISO27.001, más particularmente en sus controles:

- A-06-01-01 Roles y responsabilidades de la seguridad de la información
- A-06-01-02 Segregación de funciones
- A-06-01-03 Contacto con autoridades
- A-06-01-04 Contacto con grupos de interés especiales

Declaración institucional
La presente política se enmarca en la Política General de Seguridad de la información de la CNR junto con la normativa respectiva vigente y en este sentido, en la CNR trabaja en asegurar que los/as funcionarios/as comprendan sus responsabilidades, conforme a los aspectos de la seguridad de la información en su gestión. Para ello se desarrollan e implementan continuamente las medidas necesarias y tendientes a reducir el riesgo de error humano, comisión de ilícitos, uso inadecuado de instalaciones y/o recursos y manejo no autorizado de la información.
Objetivo de la política 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.
Alcance y/o ámbito de aplicación
La presente política está dirigida a todas las personas que componen la Comisión Nacional de Riego.
Responsabilidades específicas
Coordinador/a de la Unidad de Administración y Compras Públicas:
Mantener los contactos con las autoridades pertinentes correspondientes, debiendo contactar e informar los incidentes de seguridad de la información identificados de manera oportuna (es decir, si se sospecha del incumplimiento de las leyes).
Mantener los contactos externos para apoyar a la administración de incidentes de la seguridad de la información, o el proceso de continuidad del negocio y planificación de contingencia.
Los contactos con otras autoridades incluirán a los proveedores de servicios básicos, de servicios de emergencia, electricidad, salud y seguridad, es decir, departamentos de bomberos (en conexión con la continuidad comercial), proveedores de telecomunicaciones (en conexión con el enrutamiento de línea y disponibilidad) y proveedores de agua (en conexión con las instalaciones de enfriamiento para el equipo).
Unidad de Personas y Bienestar:
Identificar la segregación de funciones y deberes de las áreas, departamentos y unidades para reducir las oportunidades de modificación o uso indebido no autorizado o no intencional de los activos de la organización.
Encargado de Seguridad de la Información y Unidad de Tecnología de la Información y la Comunicación (UTIC):

Mantener los contactos adecuados con grupos de interés especiales u otros foros de seguridad de especialistas, asociaciones profesionales o grupos o foros de interés especiales para mejorar el conocimiento sobre las buenas prácticas y permanecer al tanto de la información de seguridad pertinente.
Recibir alertas tempranas de alertas, avisos y parches relacionados con los ataques y vulnerabilidades;
Proporcionar puntos de enlace adecuados al tratar con incidentes de seguridad de la información.
Instrumento de formalización

- Resol.Política General SSI
- Políticas específicas de seguridad de la información por dominio

POLÍTICA SEGURIDAD DE RECURSOS HUMANOS

La presente política declara su aplicabilidad para el control definido en la Norma NCh-ISO27.001: Of2013, más particularmente en sus controles:

- A-07-01-01 Selección de Personal
- A-07-02-02 Concientización, educación y formación en la Seguridad de la información.

Declaración institucional
La presente política se enmarca en la Política General de Seguridad de la información de la CNR junto con la normativa respectiva vigente y en este sentido, en la CNR trabaja en asegurar que los/as funcionarios/as comprendan sus responsabilidades, conforme a los aspectos de la seguridad de la información en su gestión. Para ello se desarrollan e implementan continuamente las medidas necesarias y tendientes a reducir el riesgo de error humano, comisión de ilícitos, uso inadecuado de instalaciones y/o recursos y manejo no autorizado de la información.
Objetivo de la política 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, teniendo presente:

- Realizar la verificación de antecedentes en todos los candidatos al empleo, de acuerdo con las leyes, regulaciones y normas éticas relevantes.
- Velar que todos los empleados de la organización, y en donde sea pertinente los contratistas, deben recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales, pertinentes para su función laboral.

Alcance y/o ámbito de aplicación
La Política de Seguridad de Recursos Humanos está dirigida a todas las personas que componen la Comisión Nacional de Riego.
Responsabilidades específicas
Funcionarios/as CNR
Dar cumplimiento a la presente política, independiente del cargo que desempeñen y la situación contractual. Cada uno es responsable de salvaguardar la información que recibe, crea o controla.
Unidad de Personas y Bienestar:
Es responsable de velar el cumplimiento de la presente política.
Coordinador/a de la Unidad de Personas y Bienestar

- Notificar a todos los/as funcionarios/as que ingresan a la Institución, de sus obligaciones respecto del cumplimiento de la Política 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 los/as funcionarios/as o con terceros que desarrollen funciones al interior de la CNR.
- Concientizar y entrenar a los/ as funcionarios/as de la institución, respecto de las materias y normativas, realizando actividades de inducción en materias relacionadas.

Lineamientos
La gestión de la seguridad de la información depende principalmente de las personas que componen la CNR. La información solo tiene sentido cuando es utilizada por las personas y son éstas las responsables de gestionar adecuadamente este recurso.
Selección del personal
Investigación de Antecedentes: En la CNR se aplican medidas que resguardan la seguridad al momento de la contratación. Los controles y validaciones impuestos en estas etapas podrán evitar el ingreso de una persona que sea una posible amenaza para la Institución desde el inicio.
Es responsabilidad de la Unidad de Gestión de Personas, la verificación de los antecedentes legales u otro antecedente de relevante según la información a la cual tendrá acceso la nueva incorporación.
Términos y Condiciones del Empleo: Los lineamientos de los requisitos del Sistema de Seguridad de la Información en relación con las personas, se difunden al momento de efectuar la inducción al nuevo/a funcionario/a, establecido.
La Unidad de Personas y Bienestar, indicará claramente al personal en el proceso de inducción los términos y condiciones del empleo.
Responsabilidades de Término: Al momento del retiro de una persona de esta Institución se debe asegurar que se realice el cambio de empleo de una manera ordenada. Debe ser supervisado y se revisará que todo el equipo y retiro de los accesos informáticos se cumplan correctamente. Será responsabilidad de la Unidad de Administración y Compras Públicas la devolución de activos que tuviese la persona que deja la Institución.
La Unidad de Personas y Bienestar, será la responsable de realizar la tramitación del cese del contrato. La jefatura directa planificará el traspaso de su trabajo.
Devolución de activos: Todos/as los/as funcionarios/as deberán devolver el activo de la Institución que tengan en su poder a la terminación de su contratación. La Unidad de Administración y Compras Públicas será responsable de efectuar una correcta devolución de activos al momento del retiro de algún/a funcionario/a.

Concientización, educación y formación en la seguridad de la información
Responsabilidades de la Dirección: El Secretario Ejecutivo imparte a través de las Políticas de Seguridad de la Información, instrucciones sobre el uso de sistemas informáticos, poniendo énfasis en el cuidado y buen uso de los activos de información.
El/la Encargado/a de Seguridad de la información en conjunto con el Comité de Gestión, serán los responsables de velar por la difusión de tales instrucciones.
Inducción Institucional: La Unidad de Personas y Bienestar en su PD-GP-01, “Selección, Contratación e Inducción”, indica como actividad que a la persona contratada se le realizará la inducción de acuerdo con el Programa de Inducción Institucional. Este Programa indica que posee una tarea específica en materias de Seguridad de la Información:

- Reunión con actores transversales de la institución, dependiendo del cargo que asuma el/la nuevo/a integrante deberá ser contactado con el/la representante designado/a en las áreas transversales de trabajo en CNR como lo es Seguridad de la Información.
- Dentro de los contenidos de la Plataforma Inducción CNR, el/la nuevo/a funcionario/a deberá ingresar y revisar los módulos de trabajo, la información asociada a cada uno de ellos. Uno de estos módulos cuenta con la información en materia de Seguridad de la Información.

Instrumento de formalización

- Políticas específicas de seguridad de la información por dominio
- PD-GP-01 Selección, Contratación e Inducción

Política Administración de Activos

La presente política declara su aplicabilidad para el control definido en la Norma NCh-ISO27.001:Of2013, más particularmente en sus controles:

- 5.9 Inventarios de Activos de Información (ISO/IEC 27002:2022)

(A-08.01.01 Inventarios de Activos)

- 5.10 Uso aceptable de la información y otros activos asociados (ISO/IEC 27002:2022)
- 5.12 Clasificación de la Información(ISO/IEC 27002:2022)

- A-08.01.04 Devolución de Activos
- A-08.03.02 Eliminación de Medios

Declaración institucional
La presente política se enmarca dentro de la Política General de Seguridad de la información de la CNR junto con la normativa respectiva vigente y en este sentido, en la CNR 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 el alcance, lineamientos, actores, responsabilidades y los procedimientos y medidas necesarias para velar por el cumplimiento de medidas y desarrollar la gestión y operación en materias relacionadas con la Administración de Activos de Información a través del Sistema de Seguridad de la Información implementado en la CNR.
Objetivos de la política de administración de activos
Identificar los activos de información organizacionales y definir las responsabilidades de protección adecuadas, considerando:

- Realizar Inventarios de Activos.
- Asegurar, que la información y los activos usados se protegen y se manejan adecuadamente.
- Garantizar el correcto procedimiento para la devolución de Activos.
- Eliminación de medios

Para asegurar que la información y otros activos asociados, se protegen, usan y manejan adecuadamente.
Alcance y/o ámbito de aplicación
El alcance de la presente política se extiende a las instalaciones relativas al procesamiento de datos, los sistemas de información, los servicios y el equipamiento tecnológico existente en la CNR.
Esta política es aplicable a todos los funcionarios/as, la suplencia y el personal a honorarios que en la facultad de sus funciones le ha sido asignados activos en la CNR.
Responsabilidades específicas
Comité de Gestión CNR:

- Los miembros del Comité de Gestión CNR son representantes de las áreas de negocio y las unidades existentes en la CNR, a través de un proceso formal, a lo menos anualmente deberán revisar y actualizar los activos de información que son administrados en sus respectivas áreas debiendo realizar el análisis de riesgos y vulnerabilidades de los mismos.

Encargado de Activo Fijo:

- El/La Encargado/a del Activo Fijo o el Apoyo Administrativo de Activo Fijo es responsable de registrar todos los bienes inventariables en el sistema informático de gestión de activos.
- El/La Encargado/a del Activo Fijo de la Unidad de Administración y Compras Públicas debe exigir la confección de registros que respalden los movimientos que provoquen variaciones en el inventario de los bienes fiscales. Para ello mantiene registros individuales y actualizados de los activos fijos (inversión real y control administrativo), detallando sus características generales y particulares.
- El/La Encargado/a del Activo Fijo o el Apoyo Administrativo de Activo Fijo verifica las planillas de inventario y recepción del bien, que la asignación de éstos se haya realizado conforme a lo requerido.
- El/La Encargado/a del Activo Fijo gestionará ante el/la secretario/a Ejecutivo/a de CNR, las solicitudes de baja de bienes, por intermedio del Jefe/a de Departamento de Administración y Finanzas, para que sean decretadas oportunamente, a través de una Resolución de bajas, posterior a la aprobación del Ministerio de Bienes Nacionales mediante un oficio de autorización. De igual manera una vez efectuada la donación o destrucción de los bienes, procederá a excluirlos de los registros del inventario y posteriormente enviará la información pertinente a la Unidad de Finanzas, todo lo anterior previo a salida de los bienes de las dependencias del Servicio.

Coordinador Unidad de Tecnología de la Información y Comunicaciones
Es responsable de realizar procesos regulares de revisión y actualización del inventario de los activos y servicios tecnológicos de la CNR con el objetivo que sea preciso, incluido su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción, versiones, proveedores, vigencia, garantizando el resguardo y la protección de los activos y servicios tecnológicos de la CNR.
Usuarios/as internos de CNR

- Todo el personal de la CNR es responsable directo del buen uso y resguardo de los activos asignados a su cargo, para el desarrollo de sus funciones y en sus respectivos centros de responsabilidad. Las responsabilidades administrativas del personal a honorarios radicarán en su jefatura directa.
- El personal debe solicitar la actualización de su planilla de inventario cada vez que se produzcan movimientos en el inventario de bienes que tiene a cargo o bien, solicitar que se corrija cuando aparezcan bienes que no son de su responsabilidad.
- El personal no podrá tomar decisiones arbitrarias o individuales sobre los bienes de activo fijo, como, por ejemplo, redestinarlos a otra Unidad, desecharlos o donarlos, sin antes pedir autorización a la Unidad de Administración y Compras Públicas, previa validación de su Jefatura Directa.
- En caso de que el personal responsable de bienes inventariables deje de cumplir funciones, la Unidad de Personas y Bienestar informará a la Unidad de Administración y Compras Públicas para que se proceda a verificar la entrega exacta de los bienes a cargo, si corresponde a través del sistema de gestión documental existente en CNR. En caso de reasignación de bienes, será responsabilidad de la Jefatura del Área informar la designación de un nuevo responsable de los bienes.
- En caso de extravío, pérdida, robo y/o hurto de un bien, el/los responsable/s directo/s deberá/n dar cuenta inmediata a su Jefe de Área o al responsable del bien designado en cada Centro de Responsabilidad, para que se tomen las medidas pertinentes y que procedan en derecho, (denuncia ante Carabineros de Chile y/o Policía de Investigaciones y/o Ministerio Público) con copia a la Unidad de Administración y Compras Públicas, para que se solicite al Jefe de Departamento de Administración y Finanzas que requiera a la Secretaría Ejecutiva una investigación sumaria y/o sumario administrativo según proceda, con el objetivo de determinar él o los presuntos responsables y el grado de responsabilidad administrativa que afecte a él o los funcionarios a cargo del o los bienes, esto sin perjuicio de las responsabilidades civiles o penales que eventualmente se determinen.

Personal y usuarios externos a la CNR, que usen o tengan acceso a la información de la organización y otros activos asociados deben conocer los requisitos de seguridad de la información para proteger y manejar la información de la organización y otros activos asociados. Deben ser responsables de su uso de cualquier instalación de procesamiento de información.
Lineamientos
En la CNR se deberán tomar las precauciones necesarias para identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.
Inventario de Activos: La CNR deberá identificar los activos pertinentes en el ciclo de vida de la información *y* documentar su importancia.
La CNR debe identificar su información y otros activos asociados y determinar su importancia en términos de seguridad de la información.
El inventario de información y otros activos asociados debe ser preciso, actualizado, consistente y alineado con otros inventarios.
Se deberá garantizar la precisión del inventario de información y otros activos incluyendo:
a) Realizar revisiones periódicas de la información identificada y otros activos asociados contra el inventario de activos.
b) Actualizar el inventario en el proceso de instalación, cambio o eliminación de un activo.
c) Se debe asignar la titularidad cuando se crean activos o cuando se transfieren activos a la organización.
Requisitos para el cumplimiento del control
El propietario del activo es responsable de la gestión y los adecuados resguardos necesarios para garantizar la protección de un activo de información durante todo el ciclo de vida incluyendo su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción, asegurando que:
a) Se realice registro e inventario de la información y otros activos asociados.
b) La información y otros activos asociados se revisen periódicamente y estén debidamente clasificados y protegidos.
c) Los componentes que respaldan los activos tecnológicos se enumeren y se vinculen, como bases de datos, almacenamiento, software, hardware, equipos, componentes y subcomponentes.
d) Las restricciones de acceso se correspondan con la clasificación, que sean efectivas y sean revisadas periódicamente.
e) La información y otros activos asociados, cuando se elimina debe ser manejada de manera segura.
f) Están involucrados en la identificación y gestión de riesgos asociados con su(s) activo(s).
g) Apoya al personal que tiene los roles y responsabilidades de administrar su información.
h) El titular de un activo es responsable de la entrega del servicio, incluida la explotación de sus activos.

Uso aceptable de la información y otros activos asociados (ISO/IEC 27002:2022- Ctrl.5.10)
La CNR se deberá identificar las normas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados debe identificarse, documentarse e implementarse.

Requisitos para el cumplimiento del control
a) Los usuarios deben comportarse asegurando no afectar o impactar los activos de seguridad de la información pertenecientes a la CNR.
b) El uso de los activos de información solo se permitirá con la autorización de los dueños de los mismos.
c) Se deberán considerar restricciones de acceso a los activos de información, que respalden los requisitos de protección.
d) Se deberá mantener de un registro de los usuarios autorizados de información y otros activos asociados.
e) Aplicar protección a las copias temporales o permanentes de información a un nivel consistente con la protección de la información original;
f) El almacenamiento de los activos asociados a la información debe ser efectuado de acuerdo con las especificaciones de los fabricantes.
g) Se deberá realizar el marcado claro de todas las copias de los medios de almacenamiento (electrónicos o físicos).
h) La disposición de información y otros activos asociados, así como la supresión de esta deberá ser autorizada.
Clasificación de la Información(ISO/IEC 27002:2022 – Ctrl.5.12)
Requisitos para el cumplimiento del control

- En la CNR, la información debe clasificarse de acuerdo con las necesidades de seguridad de la información de la organización en función de sobre confidencialidad, integridad, disponibilidad y requisitos pertinentes de las partes interesadas, asegurando la identificación y comprensión de las necesidades de protección de la información de acuerdo con su importancia para la organización.
- La CNR toma en cuenta los requisitos de confidencialidad, integridad y disponibilidad en el esquema de clasificación.
- Las clasificaciones y los controles de protección asociados para la información deben tener en cuenta necesidades de compartir o restringir información, para proteger la integridad de la información y para asegurar la disponibilidad, así como los requisitos legales relativos a la confidencialidad, integridad o disponibilidad de la información.
- Los propietarios de la información deben ser responsables de su clasificación y resguardo.
- Los resultados de la clasificación deben actualizarse de acuerdo con los cambios de valor, sensibilidad y criticidad de la información a lo largo de su ciclo de vida.
- La clasificación puede ser determinada por el nivel de impacto que tendría el compromiso de la información.
- El esquema de clasificación debe ser consistente en toda la organización e incluirse en sus procedimientos para que todos clasifican la información y otros activos asociados aplicables de la misma manera. De esta forma, todos tienen un entendimiento común de los requisitos de protección y aplican la protección adecuada,

Devolución de Activos: Todos los empleados y usuarios externos a CNR deberán devolver todos los activos organizacionales en su poder al finalizar su contrato. El proceso de finalización de empleo se debería formalizar para incluir la devolución de todos los activos físicos y electrónicos previamente entregados de propiedad de o encomendados a la organización. En los casos donde el empleado o el usuario externo cuenta con conocimiento importante para las operaciones continuas, dicha información se debería documentar y transferir a la organización.
Eliminación de Medios: En la CNR, los medios se deberían eliminar de manera segura cuando ya no se necesitan, a través de procedimientos formales Se deberían establecer procedimientos formales para la eliminación segura de los medios, a fin de minimizar el riesgo de filtración de información confidencial a personas no autorizadas. Los procedimientos para la eliminación segura de medios que contienen información confidencial deberían ser proporcionales a la sensibilidad de esa información. Se deberían considerer los siguientes elementos:

- Los medios que contiene información confidencial se deberían almacenar y eliminar de manera segura, es decir, mediante la incineración, o la destrucción o bien a través del borrado de datos para el uso por parte de otra aplicación dentro de la organización.
- Deberán existir procedimientos en vigencia para identificar los artículos que pueden requerir de una eliminación segura especia

La eliminación de los artículos sensibles se debería registrar para mantener un seguimiento de auditoría.

Instrumento de formalización

- Políticas específicas de seguridad de la información por dominio
- Inventario de Activos de la Información actualizado

POLÍTICA DE CONTROL DE ACCESOS

La presente política declara su aplicabilidad para los controles definidos en la norma NCh-ISO27.001:Of2013, más particularmente en sus controles:

- A-09.01.01 Política de control del Acceso
- A-09.01.02 Acceso a redes y servicios de red
- 5.16 Administración de identidades (ISO 27002:2022)

(A-09.02.01 Registro de identidades de Usuarios)

- A-09.02.03 Administración de derechos de acceso privilegiado
- A-09.04.01 Restricción de acceso a la información
- A-09.04.02 Procedimiento de inicio de Sesión Seguro
- 5.17 Autenticación (ISO/IEC 27002:2022)

(09.04.03Sistema de administración de contraseñas)

- A-09.04.04 Control sobre el uso de programas de utilidad privilegiados

Declaración institucional
La presente política se enmarca dentro de la Política General de Seguridad de la información de la CNR junto con la normativa respectiva vigente y en este sentido, en la CNR 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 el alcance, lineamientos, actores, responsabilidades y los procedimientos y medidas necesarias para velar por el cumplimiento de medidas y desarrollar la gestión y operación en materias relacionadas con el Control de Accesos a través del Sistema de Seguridad de la Información implementado en la CNR.
Objetivo de la política de control de accesos
Garantizar en la CNR el acceso autorizado a los usuarios/as, 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 en la CNR, considerando:

- Establecer, documentar y revisar una política de control de acceso en base a los requisitos del negocio y de la seguridad de la información.
- Asegurar que los usuarios solo tengan acceso a la red y a los servicios de red en los que cuentan con autorización específica.
- Controlar la asignación y el uso de derechos de acceso privilegiado mediante un proceso de autorización formal de acuerdo con la política de control de acceso.
- Generar sistemas de administración de contraseñas que deberían ser interactivos y garantizar contraseñas de calidad.
- Restringir y controlar el uso de programas de utilidad que pueden ser capaces de anular el sistema.

Alcance y/o ámbito de aplicación
El alcance de la presente política se extiende a la plataforma TICs e instalaciones relativas al procesamiento de datos y los sistemas y servicios de información. Incluidos los sistemas y servicios contratados por la CNR en modalidad Cloud.
Esta política es aplicada a los diversos sistemas, equipos e instalaciones de procesamiento de información, en base a los requerimientos de negocios y de seguridad de la CNR.
Responsabilidades específicas
Encargado de la Infraestructura TI

- Cautelar los activos de información, velando y garantizando el cumplimiento de los requisitos de seguridad y las normativas vigentes.
- Gestionar, administrar, autorizar, revocar y controlar los accesos de usuarios a los sistemas de información y a las instalaciones donde se desarrolle procesamiento de información de la CNR
- Revisar los derechos de acceso de los usuarios de manera periódica.

Administradores de los Sistemas de Información de los respectivos centros de responsabilidad
En los centros de responsabilidad, los respectivos Administradores de los Sistemas que son provistos, administrados y soportados directamente por proveedores externos tales como (CeroPapel, Docal, ESIIR, Cege, Ungasoft, Sistema Ley de Fomento al Riego, ESIIR, entre otros.) y que son coordinados por contrapartes de los CdR de la CNR:

- Controlan, limitan y restringen los derechos de acceso de todos los empleados los y usuarios externos a la información y a la vez revocar estos accesos una vez que termine su relación laboral o contrato.
- Aseguran que los sistemas de información sean interactivos y deben asegurar contraseñas de calidad.
- Restringen el acceso al código fuente de los programas.
- 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, están obligados a cumplir las políticas de Seguridad de la Información de la CNR.

Unidad de Tecnología de la Información y la Comunicación (UTIC)

- Restringe y controla el uso de los programas utilitarios que pueden estar en capacidad de anular los sistemas y los controles de la aplicación.
- Controla el acceso a las redes locales y el Servicio de Mensajería Electrónica.
- Instala, configura y entrega soporte a la herramienta de protección contra software malicioso, manteniendo operativa y actualizada una plataforma de hardware y software de control de antivirus y firewall para la red de servidores y computadores de la CNR evitando la propagación de código malicioso, virus y sus variantes a través de redes internas y estaciones de trabajo existentes en la CNR.
- Valida que el proceso de ejecución de "Detección y Eliminación de Códigos Maliciosos" sea realizado acorde a lo indicado en la presente política.
- Implanta controles de detección, prevención y recuperación

Usuarios/as internos de CNR

- Los/as usuarios/as y dueños de los activos de información son responsables de cautelar el cumplimiento de las normativas señaladas en esta Política de Control de Accesos.
- Usuarios Externos, Proveedores y Terceros: Los contratistas, proveedores y terceros que presten algún servicio a la Comisión, y que tengan acceso a los activos de información de la CNR, están obligados a cumplir las Políticas de Seguridad de la Información y sus procedimientos de aplicación.
- Es responsabilidad de los usuarios ingresar solo a los servicios de la red e instalaciones para los cuales han sido autorizados.

En el marco general, los funcionarios/as de la CNR tienen la obligación de cumplir con la presente Política de Control de Acceso, así como con todas las instrucciones y/o políticas específicas que se generen a partir del Sistema de Seguridad de la CNR.
Lineamientos
Política de control de Acceso: En la CNR, los dueños de los activos deberían determinar las reglas de control de la información, los derechos y restricciones de acceso para los roles específicos de los usuarios hacia sus activos, minimizando los riesgos de seguridad de la información asociados.
En la CNR deberá considerarse controlar los accesos de conformidad a las siguientes normativas:

- Se deberán administrar los derechos de acceso en un entorno de red distribuido que reconozca todos los tipos de conexiones disponibles
- Se deberá realizar la segregación de los roles de control de acceso, es decir se deberá controlar la solicitud de acceso, su autorización de acceso y la administración de acceso.
- Se deberán cumplir requisitos formales de autorización para las solicitudes de acceso mediante el Sistema de Soporte SSG existente en la CNR.
- En la CNR se deberá realizar revisión periódicos para los derechos de acceso.
- Deberán registrarse los eventos de importancia que involucran la administración de identidades de usuario e información de autenticación.
- Deberán controlarse las funciones con acceso privilegiado
- En la CNR todo acceso para nuevos usuarios/as a sistemas y servicios estará prohibido a menos que se autorice expresamente.
- Los cambios en los permisos del usuario sobre los sistemas de información existentes en la CNR, deberán ser controlados y administrados directamente por los respectivos Administradores de los Sistemas de Información de los respectivos centros de responsabilidad
- Se deberá controlar, limitar y restringir los derechos de acceso de los funcionarios/as y de los usuarios externos a la información y a la vez revocar estos accesos una vez que termine su relación laboral o contrato.
- Asegurar que los sistemas de información sean interactivos y deben asegurar contraseñas de calidad.
- En la CNR solo se otorgarán accesos a las instalaciones de procesamiento de información (Data Center CNR) solo al personal de la Unidad de Tecnología de la Información y la Comunicación (Utic) y a los proveedores autorizados de conformidad a lo señalado en el procedimiento PD-SSI-02 Seguridad Física y Entorno, en que se determina que el ingreso a la sala de procesamiento de datos (DataCenter) debe ser controlada previamente, la que debe ser coordinada, dejando constancia en el libro de ingreso al Data Center.
- El ingreso de visitas al interior del DataCenter considera la necesidad de registrar en libro de visitas, el propósito de la visita además de la obligatoriedad de solicitar el RUT/Pasaporte como medio de identificación válida de los visitantes externos a la CNR

Acceso a redes y servicios de red: En la CNR, deberán considerarse controlar los accesos a las redes y servicios de red de conformidad a los siguientes lineamientos:

- Los usuarios solo deberían tener acceso a la red y a los servicios de red en los que cuentan con autorización específica. Para ello existirá un procedimiento de autorización para determinar a quién se le permite acceder a qué redes y servicios.
- Deberán controlarse el acceso a las conexiones de red y a los servicios de red.
- Deberán identificarse los medios que se utilizarán para acceder a las redes y a los servicios con redes (Wifi y VPN)
- Deberán monitorearse del uso de los servicios de red.

Administración de derechos de acceso privilegiado: En la CNR, la asignación de derechos de acceso se debería controlar mediante un proceso de autorización formal considerando que:

- Se deben identificar los derechos de acceso asociados a los sistemas existentes en la CNR.
- Se deben asignar derechos de acceso privilegiado a los usuarios en base a su necesidad de uso y en base al requisito mínimo para sus roles funcionales.
- No se deben otorgar derechos de acceso privilegiado hasta que el proceso de autorización se haya completado.
- Se deberán definir los vencimientos de los derechos de acceso

Administración de identidades (ISO/IEC 27002:2022 - Crtl.5.16)
En la CNR debe administrarse el ciclo de vida completo de las identidades con el objetivo de permitir la identificación única de personas y sistemas que acceden a la información de la organización para permitir la asignación adecuada de los derechos de acceso, donde los procesos utilizados en el contexto de la gestión de la identidad deben garantizar que:

- Las identidades asignadas a personas, una identidad específica sólo se vincula a una sola persona para poder responsabilizar a la persona por las acciones realizadas con esta identidad específica.
- Las identidades asignadas a varias personas (por ejemplo, identidades compartidas) solo se permiten cuando son necesarios por razones comerciales u operativas y están sujetos a aprobación y documentación.
- Las identidades asignadas a entidades no humanas están sujetas a aprobación y supervisión continua independiente.
- Las identidades se deshabilitan o eliminan de manera oportuna si ya no son necesarias (por ejemplo, si las entidades asociadas se eliminan o ya no se usan, o si la persona vinculada a una identidad ha dejado la organización o cambió el rol).
- Se deberá evitar la duplicidad de identidades (una sola identidad se asigna a una sola entidad).
- Se deberá conservar los registros de la información de autenticación de todos los eventos significativos relacionados con el uso y la gestión de las identidades de los usuarios.
- La CNR debe tener un proceso de apoyo para manejar los cambios en la información relacionada a las identidades de los usuarios. Pueden incluir la reverificación de documentos confiables relacionados con una persona.
- Previamente se deberá verificar la identidad de una entidad antes de asignarles una identidad lógica.
- Se deberá proveer o revocar derechos de accesos específicos para las identidades, ,basadas sobre autorizaciones apropiadas o decisiones de derechos.

Restricción de acceso a la información
En la Comisión Nacional de Riego, la restricción de acceso a la información y a las funciones del sistema se deberían restringir de acuerdo los siguientes hitos de apoyo:

- Proporcionar menús para controlar el acceso a las funciones del sistema de aplicación
- Controlar los datos a los que un usuario en particular puede acceder
- Controlar los derechos de acceso de los usuarios, es decir, de lectura, escritura, eliminación y ejecución
- Controlar los derechos de acceso de otras aplicaciones proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos o sistemas de aplicación.

Procedimiento de inicio de Sesión Seguro

En la CNR el control de inicio de sesión seguro estará en concordancia a las siguientes directrices:
Se establece una técnica de autenticación adecuada para corroborar la identidad que un usuario afirma tener.
El control de inicio de sesión tendrá las siguientes características:

1. No se proporcionan mensajes de ayuda durante el inicio de sesión que pudieran servir de ayuda a un usuario no autorizado;
2. Se valida la información de inicio de sesión solo al completar todos los datos de entrada.
3. No mostrar una contraseña que se ingresa
4. No se transmiten contraseñas en texto sin cifrar a través de una red o mensajes electrónicos.
5. Se controla el término de las sesiones inactivas después de un periodo de inactividad.
6. Se restringen los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo y reducir la ventana de oportunidad para el acceso no autorizado.

Autenticación de información (ISO/IEC 27002:2022 - Crtl.5.17)

En la CNR, la asignación y gestión de la información de autenticación debe ser controlada por un administrador, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación para garantizar la autenticación adecuada.
El proceso de asignación y gestión debe garantizar que:
a) Contraseñas personales o números de identificación personal (PIN) generados automáticamente durante los procesos de inscripción como información de autenticación secreta temporal no se puedan adivinar y son únicos para cada persona, y que los usuarios están obligados a cambiarlos después del primer uso.
b) Se establezcan procedimientos para verificar la identidad de un usuario antes de proporcionar un nuevo, reemplazo o información de autenticación temporal.
c) La información de autenticación, incluida la autenticación temporal, se transmite a los usuarios de manera segura, a través de un canal autenticado y protegido evitando los mensajes de correo electrónico sin protección (texto claro) para este fin.
d) Los usuarios deben acusar recibo de la información de autenticación.
e) La información de autenticación predeterminada predefinida o proporcionada por los proveedores, debe ser cambiada inmediatamente después de la instalación de sistemas o software.

1. Los registros de eventos significativos relacionados con la asignación y gestión de la información de autenticación se conservan y se garantiza su confidencialidad.
2. Las mismas contraseñas no se utilizan en distintos servicios y sistemas;
3. Los sistemas de administración de contraseñas deben ser interactivos y deberán garantizan el uso de contraseñas de calidad.
4. Se forzará el uso de identificación de usuario y contraseñas individuales para mantener la responsabilidad.
5. El cifrado de contraseñas y el hash deben realizarse de acuerdo con las normas criptográficas aprobadas.

Responsabilidades del usuario

Cualquier persona que tenga acceso o utilice información de autenticación debe ser advertida de que se asegure de que:
a) La información de autenticación secreta, como las contraseñas, se mantiene confidencial.
Secreto personal. La información de autenticación no se debe compartir con nadie. Información de autenticación secreta utilizada en el contexto de identidades vinculadas a múltiples usuarios o vinculadas a entidades no personales podrán ser compartidas únicamente con personas autorizadas.
b) La información de autenticación afectada o comprometida se debe cambiar inmediatamente después de la notificación de o cualquier otra indicación de compromiso.
Cuando se utilizan contraseñas como información de autenticación, el sistema de administración de contraseñas debe:
a) Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para dirección de errores de entrada.
b) Aplicar contraseñas seguras de acuerdo con las recomendaciones de buenas prácticas.
c) Obligar a los usuarios a cambiar sus contraseñas en el primer inicio de sesión.
d) Hacer cumplir los cambios de contraseña según sea necesario.
e) Impedir la reutilización de contraseñas anteriores/históricas.
f) Evitar el uso de contraseñas de uso común y nombres de usuario, contraseñas combinaciones de sistemas pirateados.
g) No mostrar contraseñas en la pantalla cuando se ingresan.
h) Almacenar y transmitir contraseñas en forma protegida.

Control sobre el uso de programas de utilidad privilegiados

El uso de programas de utilidad que pueden ser capaces de anular el sistema y los controles de aplicación se restringe y controla considerando las siguientes pautas para el uso de estos programas:

1. Limitar el uso de programas de utilidad al número mínimo.
2. Obligatoriedad en la autorización para la instalación de programas de utilidad ad hoc.
3. Eliminar o deshabilitar todos los programas de utilidad innecesarios.
4. No dejar disponibles programas de utilidad debiéndose realizar la segregación de deberes.

Instrumento de formalización

- Políticas específicas de seguridad de la información
- PD-UTIC-02 Continuidad Operacional de Tecnología
- Instructivos Utic

POLÍTICA SEGURIDAD FÍSICA Y AMBIENTAL

La presente política declara su aplicabilidad para el control definido en la Norma NCh-ISO27.001:Of2013, más particularmente en sus controles:

- A-11.01.01 Perímetro de Seguridad
- A-11.01.02 Controles de entrada física
- A-11.01.04 Protección contra las amenazas externas y ambientales
- A-11.02.01 Ubicación y Protección del Equipamiento
- A-11.02.02 Elementos de soporte, protección de elementos de energía
- A-11.02.04 Mantenimiento del Equipamiento
- A-11.02.05 Retiro de Activos
- 7.9 Seguridad de los activos fuera de las instalaciones (ISO 27002:2022)
- A-11.02.07 Seguridad en reutilización o descarte de equipos
- A-11.02.08 Equipo de usuario desatendidos
- A-11.02.09 Política de escritorio y pantallas limpias

Declaración institucional

La presente política se enmarca dentro de la Política General de Seguridad de la información de la CNR junto con la normativa respectiva vigente y en este sentido, en la CNR 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 el alcance, lineamientos, actores, responsabilidades y los procedimientos y medidas necesarias para velar por el cumplimiento de medidas y desarrollar la gestión y operación en materias relacionadas con la Seguridad Física y Ambiental a través del Sistema de Seguridad de la Información implementado en la CNR.

Objetivos de la política física y ambiental

- Evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.
- Evitar la pérdida, el daño, el robo o el compromiso de los dispositivos externos y la interrupción de las organizaciones operaciones:
- Establecer un perímetro de seguridad física para las áreas que contienen información y a las instalaciones de procesamiento de información
- Las áreas seguras deberían estar protegidas con controles de entrada adecuados para garantizar que solo se permita el acceso al personal autorizado.
- Brindar protección contra las amenazas externas y ambientales diseñando una protección física contra desastres naturales, ataques maliciosos o accidentes.
- Asegurar el debido emplazamiento y la protección de los equipos
- Brindar protección a los equipos contra interrupciones provocadas por fallas en los servicios básicos de apoyo
- Realizar un adecuado control en el retiro de Activos
- Verificar extracción o sobreescritura de datos sensibles y software con licencia en la eliminación o reutilización de equipos
- Asegurar los equipos de usuarios no supervisados
- Adoptar una la política de escritorio y pantalla despejados.

Alcance y/o ámbito de aplicación
El alcance de la presente política se asociada a lo definido en el Sistema de Seguridad de la Información y su objetivo se traduce en contar con espacios seguros e implementar medidas que permitan resguardar la seguridad de los activos de información, para que de esta forma se impida que una interrupción de carácter grave e imprevista, causada por desastres naturales, siniestros, atentados u otras circunstancias de fuerza mayor o caso fortuito tenga consecuencias catastróficas para el negocio.
Para asegurar físicamente el perímetro de las oficinas de la CNR, tanto a nivel central como en regiones existen procedimientos formales que regulan el ingreso de personal o servicios externos. Es de responsabilidad del Departamento de Administración y Finanzas (DAF) a través de la Unidad de Administración y Compras Públicas velar por su cumplimiento.

En el caso de existir algún tipo de catástrofe la evacuación de las personas desde las oficinas de la CNR se realizará mediante las instrucciones y directrices que imparte el personal de seguridad habilitado de la administración del edificio, a través de los equipos de seguridad (brigadas) instruidos para tales efectos. Una vez estacionados en los espacios de seguridad, los brigadistas CNR se someten a las instrucciones dictadas en el Plan de Emergencia y Seguridad de la Comunidad. Así mismo se cuenta con: Controles de Ingreso físico, protección contra amenazas externas e internas, trabajo en áreas aseguradas, áreas de acceso público, de entrega y carga, ubicación y protección de equipos, Servicios básicos de soporte, seguridad de cableado, mantenimiento de equipos, seguridad de equipos fuera de las instalaciones de la CNR y un adecuado retiro de bienes para su eliminación.
Responsabilidades específicas
Encargado de Seguridad Física de la CNR

- Encargado de velar por las normas de seguridad física dentro de la Institución, tanto en Santiago como en Regiones.
- Liderar plan de emergencia y evacuación de la institución en caso de que la urgencia lo amerite, realizando las gestiones que sean necesarias para asegurar el bienestar de los funcionarios/as.
- Realizar la mantención del equipamiento que se utiliza en emergencias y urgencias.
- Prestar apoyo al encargado/a de Higiene y Seguridad en las distintas dinámicas que existan, además de evaluar y canalizar las observaciones del Comité Paritario, y las necesidades de los/as funcionarios/as, con el apoyo de la Mutual de Seguridad y la Administración del Edificio.

Usuarios/as internos de CNR

- Los/as usuarios/as y dueños de los activos de información son responsables de cautelar el cumplimiento de las normativas señaladas en esta Política de Seguridad Física y Entorno.
- Cada vez que algún usuario/a detecte actividad anormal, sospechosa o producto de alarmas locales producidas en sus zonas de trabajo, deberán reportar el incidente en el Sistema de Servicios Generales (Administración).

Lineamientos
Perímetro de seguridad física En la CNR se tomar las precauciones necesarias para definir los perímetros de seguridad y proteger las áreas que contienen información en las instalaciones con procesamiento de información sensible o crítica como se indica a continuación:
Se definen los perímetros de seguridad y el emplazamiento y la ubicación de cada uno de los perímetros dependerá de los requisitos de seguridad de los activos dentro del perímetro y los resultados de una evaluación de riesgos.
Los perímetros del edificio de CNR donde se albergan las instalaciones de procesamiento de información será físicamente sólido; el techo exterior, las paredes y el piso del sitio deberán ser una construcción sólida y todas las puertas externas deberán estar protegidas adecuadamente contra el acceso no autorizado con mecanismos de control, (es decir, barras, alarmas, candados); las puertas y ventanas se deberían cerrar con llave correctamente, cuando se dejan sin vigilancia y se debería considerar una protección externa para las ventanas, en particular a nivel del suelo.
Se contará con un área de recepción atendida por una persona u otros medios para controlar el acceso físico al sitio o al edificio; el acceso a los sitios.
Se construirán barreras físicas donde corresponda para evitar el acceso físico no autorizado y la contaminación ambiental.
Las instalaciones de procesamiento de información que administra la CNR estarán separada físicamente de las que administran terceros.
Controles de entrada física: Las áreas seguras estarán protegidas con controles de entrada adecuados para garantizar que solo sea permitido el acceso al personal autorizado.

- Se registra la fecha y la hora de entrada y salida de las visitas y, se supervisar a todas las visitas a menos que su acceso haya sido aprobado anteriormente; solo se les otorga acceso para propósitos específicos y autorizados y se emite de acuerdo con las instrucciones de los requisitos de seguridad del área y a los procedimientos de emergencia. Se autentica la identidad de las visitas con un medio adecuado.
- El acceso a las áreas donde se procesa o almacena la información confidencial estará restringido a las personas autorizadas sólo mediante la implementación de controles de acceso adecuados, es decir, al implementar un mecanismo de autenticación como una tarjeta de acceso o control biométrico.
- Se otorgará acceso restringido al personal externo de apoyo a las áreas seguras o a las instalaciones de procesamiento de información confidencial sólo cuando sea necesario; este acceso se deber ser autorizado y monitoreado.
- Los empleados, contratistas y partes externas portarán una identificación visible y se notificará inmediatamente al personal de seguridad si encuentran visitas sin escolta y a cualquier persona que no porte una identificación visible.
- Se otorgará acceso restringido al personal de servicios de apoyo de terceros a las áreas seguras o a las instalaciones de procesamiento de información confidencial sólo cuando sea necesario siendo obligatoria su autorización y monitoreo.
- Los derechos de acceso a las áreas protegidas se revisarán y actualizarán de manera regular y, se revocarán cuando sea necesario.

Protección contra las amenazas externas y ambientales En la CNR se diseña y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
La Comisión Nacional de Riego cuenta con equipos de emergencia debidamente habilitados, además cuenta con una brigada de emergencia cuyo objetivo es apoyar la implementación del plan de evacuación en el caso de una catástrofe.
Servicios Básicos de Apoyo Los equipos estarán protegidos contra cortes de energía y otras interrupciones provocadas por fallas en los servicios básicos de apoyo y para ello dichos equipos:

- Se cumplirá con las especificaciones del fabricante del equipo y con los requisitos legales locales.
- Se someten a inspecciones y pruebas regularmente para garantizar su funcionamiento correcto.
- En caso de ser necesario los equipos contarán con alarmas para la detección de fallas.
- En caso de ser necesario, en la CNR dispondrá de varias alimentaciones con distintos enrutamientos físicos.

Emplazamiento y Protección de Equipos: Los equipos se emplazarán y protegerán para reducir los riesgos de las amenazas y peligros ambientales y las oportunidades de acceso no autorizado.

- Los equipos se emplazarán en un lugar determinado para minimizar el acceso innecesario a las áreas de trabajo y para reducir el riesgo de que personas no autorizadas tengan acceso a instalaciones de procesamiento de información que manejan datos sensibles.
- Las instalaciones de almacenamiento se deberían proteger para evitar el acceso no autorizado.
- Se adoptarán controles para minimizar el riesgo de posibles amenazas físicas y ambientales, es decir, robos, incendios, humo, agua (o una falla del suministro de agua), polvo, vibraciones, efectos químicos, interferencia del suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética, atentados y vandalismo.
- Se señalará la prohibición para comer, beber y fumar en la proximidad de las instalaciones de procesamiento de información.
- Se monitorearán las condiciones ambientales como la temperatura y la humedad de los centros de cómputos y equipos relacionados en busca de condiciones que pudieran afectar adversamente a la operación de las instalaciones de procesamiento de información.

- Se aplicará protección a la luminaria y se instalarán filtros de protección de iluminación a los cables de tendido eléctrico y de comunicación entrantes.

Mantenimiento del Equipamiento: En la CNR, se realizará las correspondientes mantenciones para los equipos con el objeto de garantizar su disponibilidad e integridad, considerando las siguientes pautas:

- Se realizará el mantenimiento a los intervalos y especificaciones de servicio recomendados por el proveedor, manteniendo registros de las fallas y de todo el mantenimiento preventivo y correctivo.
- Solo el personal de mantenimiento autorizado podrá realizar reparaciones y labores de mantenimiento y servicio a los equipos y donde sea necesario se eliminará la información confidencial del equipo.

Retiro de Activos: Los equipos, la información o el software no se podrá retirar sin una autorización previa

- Será obligatoria la identificación de los empleados y partes externas que tienen autorización para retirar fuera de la institución los activos, estableciéndose límites de tiempo para el retiro de activos y los retornos se verificarán para comprobar su cumplimiento.

Seguridad de los activos fuera de las instalaciones (ISO 27002:2022 – Ctrl.7.9)
Cualquier dispositivo utilizado fuera de las instalaciones de la CNR que almacene o procese información necesita protección.
El uso de estos dispositivos debe ser autorizado por la jefatura.
Se deben considerar las siguientes pautas para la protección de dispositivos que almacenan o procesan información fuera de las instalaciones de la organización:
a) No dejar el equipo y los medios de almacenamiento retirados de las instalaciones sin supervisión en público y sin seguridad lugares;
b) Observando las instrucciones del fabricante para proteger el equipo en todo momento (por ejemplo, protección contra exposición a fuertes campos electromagnéticos, agua, calor, humedad, polvo);
c) Cuando se transfieren equipos fuera de las instalaciones entre diferentes personas o partes interesadas, se deberá mantener un registro que defina la cadena de custodia del equipo, incluidos al menos los nombres y organizaciones de los que son responsables del equipo.
d) Considerar la necesidad de eliminar información de forma segura antes de la transferencia del equipo.
e) Implementar el seguimiento de ubicación y la capacidad de borrar dispositivos de forma remota.
f) Monitoreo de la seguridad física.
g) Protección contra amenazas físicas y ambientales.
h) Controles de acceso físico y lógico a prueba de manipulaciones.

Eliminación o reutilización segura de equipos: Se verificarán los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se haya sobrescrito de manera segura antes de su eliminación o reutilización.
Equipos de usuarios no supervisados: Se asegurará que los equipos no supervisados cuentan con la protección adecuada.

- Los usuarios aplicarán protección (bloqueo) a sus equipos cuando finalicen las sesiones activas, a menos que se puedan proteger con un mecanismo de bloqueo adecuado, es decir, un protector de pantalla protegido con contraseña.
- Los usuarios cerrarán sus sesiones en las aplicaciones o servicios de redes cuando ya no se necesiten.
- Se protegerá a los computadores o dispositivos móviles del uso no autorizado mediante un candado con llave o un control equivalente, es decir, acceso con contraseña, cuando no se utilice.

Política de escritorio despejado y pantalla despejada: Se adoptará una política de escritorio despejado para los papeles y para los medios de almacenamiento extraíbles y una política de pantalla despejada para las instalaciones de procesamiento de información

- La información sensible o crítica para el negocio, es decir, disponible en medios de almacenamiento electrónico o papel, se mantendrá guardada bajo llave (idealmente en una caja fuerte o gabinete u otras formas de muebles de seguridad) cuando no se necesite, especialmente cuando la oficina esté desocupada.
- Se mantendrán desconectados los computadores y terminales, protegidos con un mecanismo de bloqueo de pantalla y teclado mediante una contraseña, token o mecanismo de autenticación de usuario similar cuando se deja sin supervisar y se debe proteger con bloqueos de tecla, contraseñas u otros controles cuando no está en uso.
- Se evitará el uso no autorizado de fotocopiadoras u otro tipo de tecnologías de reproducción (es decir, escáneres, cámaras digitales).

Instrumento de formalización

- Políticas específicas de seguridad de la información
- Instructivos Utic
- PD-ADM-02 Administración Activo Fijo

POLÍTICA SEGURIDAD DE LAS OPERACIONES

La presente política declara su aplicabilidad para el control definido en la Norma NCh-ISO27.001:Of2013, más particularmente en sus controles:

- A-12.01.01 Procedimientos de operación de documentados
- A-12.01.02 Gestión de cambios
- A.12.01.04 Separación de entornos de desarrollo, pruebas y operacionales
- A-12.02.01 Controles contra código malicioso
- A-12.03.01 Respaldo de Información
- A.12.04.01 Registro de evento
- A.12.04.03 Registros del administrador y el operador
- A-12.04.04 Sincronización de Relojes
- A-12.05.01 Instalación de software en sistemas operacionales
- 8.8 Gestión de las vulnerabilidades técnicas (ISO/IEC 27002:2022)

(A-12.06.01 Gestión de las vulnerabilidades técnicas)

- A-12.06.02 Restricciones en la instalación de software

Declaración institucional
La presente política se enmarca dentro de la Política General de Seguridad de la información de la CNR junto con la normativa respectiva vigente y en este sentido, en la CNR 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 el alcance, lineamientos, actores, responsabilidades y los procedimientos necesarios para velar por el cumplimiento de medidas y desarrollar la gestión y operación en materias relacionadas con la Seguridad de las Operaciones a través del Sistema de Seguridad de la Información implementado en la CNR.
Objetivo de la política de seguridad de las operaciones
Garantizar las operaciones correctas y seguras de las instalaciones de procesamiento de información, considerando:

- Establecer procedimientos operativos documentados que estén a disposición de todos los usuarios/as que los necesiten.
- Controlar los cambios producidos en las instalaciones de procesamiento de información, en los sistemas y en los servicios que pudieran afectan a la seguridad de la información.
- Garantizar operaciones correctas y la seguridad de la información en las instalaciones de procesamiento de información.
- Garantizar que la información y que las instalaciones de procesamiento de información estén protegidas contra el malware.
- Brindar protección contra la pérdida de datos.
- Registrar eventos, generar evidencias, y su revisión
- Garantizar la sincronización de los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la CNR con una fuente de tiempo de referencia única.

- Garantizar la integridad de los sistemas operacionales controlando la instalación de software en sistemas y aplicando actualizaciones junto a los respectivos parches de seguridad.

Alcance y/o ámbito de aplicación
El alcance de la presente política se extiende a la plataforma TICs interna o bien disponible como servicio Cloud e instalaciones relativas al procesamiento de datos y los sistemas y servicios de información.
Esta política es aplicable a todos los funcionarios/as, la suplencia y el personal a honorarios que en la facultad de sus funciones le ha sido asignado funciones de administración de la infraestructura TI y sistemas de información existentes en la CNR.
Responsabilidades específicas
Administradores y contrapartes encargados de los Sistemas de Información de los respectivos centros de responsabilidad

- Los respectivos Administradores y contrapartes de los Sistemas de Información tienen a cargo preparar procedimientos e instructivos documentados para las actividades operacionales asociadas con la implementación, el desarrollo, la administración, el procesamiento y el mantenimiento de los respectivos Sistemas de Información a su cargo y controlarán los cambios asociados que podrían afectar la seguridad de la información.
- Para el caso de aquellos sistemas que son provistos, administrados y soportados directamente por proveedores externos como son el caso de los sistemas Ceropapel, Docal, Cege, Ungasoft, SED, ESIIR, entre otros y que son coordinados directamente por las respectivas contrapartes administradoras de los centros de responsabilidad existentes en la CNR, incluyendo el Sistema Ley de Fomento al Riego (Ley 18.450) que es administrado y soportado directamente por la Unidad de Tecnología de la Información y la Comunicación (Utic), es necesario que estas contrapartes, controlen y aseguren en sus aplicativos la implementación de procedimientos de inicio de sesión seguro, gestión de contraseñas, el uso de controles criptográficos, la protección contra código malicioso, el control Instalación de software en sistemas operacionales, solicitar y gestionar con sus proveedores la remediación de vulnerabilidades técnicas y deberán controlar los cambios asociados con los aplicativos de procesos de negocio y los sistemas que podrían afectar la seguridad de la información.
- Proveer y administrar los servicios que satisfagan las necesidades informáticas, con el propósito de apoyar a los usuarios de manera eficiente, efectiva y oportuna en sus funciones y en los procesos administrativos de la organización.
- Satisfacer los requerimientos de seguridad de la información para la operación, administración y comunicación de los sistemas de información y que tienen a su cargo.
- Desarrollar y mantener la administración y la continuidad operativa de los sistemas de información que tienen a su cargo en la CNR, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en sus fases puesta en marcha.
- Utilizar un sistema de control de configuración para mantener el control de todo el software implementado, así como también proveer de toda la documentación técnica de los sistemas que administran o gestionan.
- Garantizar que el software informático a su cargo que sea suministrado de manera externa sea monitoreado y controlado para evitar cambios no autorizados y que pueden introducir falencias en la seguridad.
- 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, están obligados a cumplir las políticas de Seguridad de la Información de la CNR.

Encargado de la Infraestructura TI

- Preparar y actualizar los procedimientos/instructivos documentados para las actividades operacionales asociadas con las instalaciones de procesamiento de datos señaladas en esta Política de Seguridad de las Operaciones.
- Administrar y entregar el soporte técnico para garantizar la disponibilidad, integridad, confidencialidad y la seguridad sobre la Infraestructura tecnológica computacional y servicios tecnológicos existentes en la CNR
- Controlar los cambios asociados con las instalaciones e infraestructura que podrían afectar la seguridad de la información.
- Emitir reportes periódicos con los registros de análisis de vulnerabilidades y amenazas recibidas tanto en estaciones de trabajo, la infraestructura central y de la red interna de comunicaciones de la CNR.

Coordinador Unidad de Tecnología de la Información y Comunicaciones

- Controlar el proceso de gestión de vulnerabilidades técnicas garantizando la remediación de las vulnerabilidades identificadas cuanto antes.
- Informar a la jefatura de la CNR, al encargado de seguridad de la información y a las partes interesadas reportes periódicos con el estado de remediación de vulnerabilidades subsanadas y amenazas controladas.

Usuarios/as internos de CNR

- Los/as usuarios/as y dueños de los activos de información son responsables de cautelar el cumplimiento de las normativas señaladas en esta Política de Seguridad de las Operaciones.
- Cada vez que algún usuario/a detecte actividad anormal, sospechosa o producto de alarmas locales producidas en sus estaciones de trabajo, está en la obligación de reportar el incidente en el Sistema de Servicios Generales (Mesa de Ayuda de Informática).
- Se abstendrán de recibir por correo y/o ejecutar programas o documentos con contenido ejecutable cuya procedencia no sea conocida o sea sospechosa, dado que pueden ser archivos que contienen virus. Asimismo, queda prohibido enviar este tipo de Contenidos.
- Evitar visitar sitios y/o abrir archivos sospechosos, aunque vengan de direcciones de correo conocidas, dado que muchos virus y spyware roban direcciones de correo válidas para propagarse.
- Los funcionarios/as no están autorizados a instalar software en los computadores y notebooks de la CNR, dado que se aumentan las probabilidades de introducción de virus, malware o spyware o provocar cualquier impacto producto de la materialización de ciber amenazas.
- No descargar ni instalar software no autorizado ni aplicaciones desde Internet los cuales podrían comprometer la seguridad de la información y las plataformas tecnológicas existentes en al CNR.
- Los funcionarios/as de la CNR se obligan a conocer la política de Seguridad de las Operaciones y los riesgos relacionados con el tratamiento de la seguridad de los activos de información entendiendo su contenido, su alcance y comprometiéndose a cumplirlas.

Contratistas, proveedores y terceros:
Los contratistas, proveedores y terceros que tengan acceso a los activos de información de la CNR, están obligados a cumplir las políticas de Seguridad de la Información de la CNR.
Lineamientos
En la CNR se tomarán las precauciones necesarias para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información de conformidad a las siguientes normativas:
Uso del Correo electrónico institucional : La Comisión Nacional de Riego proporcionará una herramienta de correos electrónicos (sistema de mensajería) a todo su personal, independiente de su calidad jurídica, lo que permite identificar tanto a la persona como a la Institución, a través de la dirección del correo, direcciones IP o códigos de identificación de los servidores por donde transitan los correos electrónicos enviados o recibidos. Este es el único medio de sistema de mensajería digital y oficial reconocido por la Comisión Nacional de Riego.
El uso de correos privados como hotmail, gmail, yahoo, icloud y otros, desde la plataforma computacional de la CNR, también permite identificar a la Institución como plataforma de origen del correo, por tanto, los funcionarios están obligados a hacer una adecuada y responsable utilización tanto de las casillas Institucionales que se les asignen para el cumplimiento de sus funciones, así como de las casillas privadas que empleen personalmente utilizando la plataforma computacional de la CNR.
La Unidad de Tecnología de la Información y la Comunicación (Utic) podrá tener acceso a las casillas de correo electrónico asignadas a los funcionarios/as, única y estrictamente en los siguientes casos:

- Voluntad del funcionario, manifestada por escrito.
- Por instrucción de un sumario o investigación sumaria, previa solicitud del Fiscal instructor.
- Por instrucciones precisas del Jefe de Servicio.

Los funcionarios/as que utilicen correo electrónico con casilla Institucional o con casilla privada desde la plataforma computacional CNR, deberán:

- Abstenerse de transmitir información confidencial, salvo que ésta se encuentre debidamente encriptada o protegida por una clave de seguridad.
- Usar un lenguaje respetuoso en su texto; los mensajes de ninguna forma podrán ser de contenido insultante, injurioso, amenazador, ofensivo, obsceno, racista o sexista.
- No enviar cadenas de mensajes o promociones comerciales.
- No enviar mensajes masivos al interior de la CNR o hacia el exterior. En caso de ser requerido, se deberá contar con la autorización de la Jefatura y siempre con fines Institucionales.

- Abstenerse de recibir por correo y/o ejecutar programas o abrir documentos con contenido ejecutable u otra cuya procedencia no sea conocida o sea sospechosa, dado que pueden ser archivos que contienen virus, malware u otros códigos maliciosos. Asimismo, queda prohibido enviar este tipo de contenidos.
- Realizar periódicamente limpieza de sus casillas de correo, previniendo que su espacio de datos o cuota asignada se agote.

La Comisión Nacional de Riego maneja respaldos globales del correo electrónico Institucional, con el fin de recuperar dichos correos ante errores, fallas o solicitudes especiales.

Navegación y descarga de Contenido en Internet desde las redes informáticas existentes en la CNR

- El sistema de navegación a través de Internet que la CNR pone a disposición de sus funcionarios, es una herramienta de trabajo que debe ser usada para estos efectos, debiendo los funcionarios ajustarse a una adecuada utilización de dicho sistema.
- La Unidad de Tecnología de la Información y la Comunicación (Utic) dispone de sistemas de monitoreo permanente de los enlaces de comunicación y los accesos de Internet, llevando un registro de éstos.
- Al navegar por Internet desde las instalaciones de la CNR, los funcionarios están obligados a cumplir estrictamente las siguientes normas:
- Abstenerse de visitar sitios que pudieran tratar contenido insultante, injurioso, amenazador, ofensivo, obsceno, racista o sexista o participar en chat o en foros relacionados con más materias señaladas y en general aquellas que sean ajenas a las funciones que les correspondan.
- Si un funcionario requiere del acceso a algún sitio que se encuentre limitado en las instalaciones de la CNR, lo deberá solicitar siguiendo los conductos regulares correspondientes.
- Evitar visitar sitios y/o abrir archivos sospechosos, aunque vengan de direcciones de correo conocidas, dado que muchos virus, malware y spyware roban direcciones de correo válidas para propagarse.
- Los funcionarios no están autorizados a instalar software en los PCs y notebooks de la CNR, dado que se aumentan las probabilidades de introducción de virus, malware o spyware que podrían comprometer las plataformas y servicios tecnológicos existentes en la CNR.
- Los programas o servicios de transferencia e intercambio de archivos o descarga (como DropBox, WeTransfer, Kazaa, eMule, eDonkey, Ares, Imesh, Sharezaa, Mega.nz, BitTorrent, etc.) están estrictamente prohibidos, ya que suelen 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.

Procedimientos de operación de documentados: Al respecto en la CNR se preparan procedimientos documentados para las actividades operacionales asociadas con las instalaciones de procesamiento de datos y los servicios tecnológicos existentes en la CNR.

Gestión de Cambios: En la CNR se controlarán los cambios realizados sobre las instalaciones de procesamiento de información, los sistemas y servicios tecnológicos que afectan a la seguridad de la información considerando elementos como:

- La identificación y registro de cambios significativos
- La planificación y pruebas de cambios
- La evaluación de los posibles impactos, incluidos los impactos de seguridad en la información, de dichos cambios.
- Un procedimiento de aprobación formal para los cambios propuestos
- Verificación de que se han cumplido los requisitos de seguridad
- La comunicación de los detalles de los cambios a todas las personas pertinentes
- Una indicación de la operación de retroceso (vuelta atrás) para abortar y recuperar los cambios incorrectos y los eventos inesperados.

Control contra código malicioso: En la CNR se tomarán las precauciones necesarias para proteger la red local de datos previniendo, detectando, aislando y recuperándose de la introducción de software malicioso como son Virus, Gusanos, Spyware, Código móvil, Keylogger, Ransomware, Phishing, otras variantes y bombas lógicas en los computadores y Servidores, previniendo de esta manera que todos los activos de información digitales vigentes, en uso y relacionados con tecnología de la información tales como servidores, estaciones de trabajo y el software perteneciente a la CNR estén protegidos mediante herramientas y software de seguridad como firewall, antivirus, anti spam, antispyware y otras aplicaciones que brinden protección contra código malicioso.

Lo anterior en concordancia a los lineamientos establecido en la Política Específica de Seguridad de la información denominada “Política de Protección Contra Código Malicioso “existente en la CNR.

Respaldo de Información: En la CNR se tomarán las medidas y precauciones necesarias para proteger la información digital y sus sistemas críticos en producción ante posibles daños, por lo cual frecuentemente deberán realizarse respaldos asegurando su proceso de recuperación considerando la implementación de soluciones de respaldo para programas, bases de datos e información considerada como crítica para la institución.

Lo anterior en concordancia a los lineamientos establecidos en la política específica de Seguridad de la información denominada “Política Respaldo de la información” existente en la CNR.

Sincronización de Relojes: En la CNR los sistemas informáticos se sincronizarán con una fuente de tiempo de referencia única. Para ello, la Unidad de Tecnología de la Información y la Comunicación (Utic) de la CNR vela por que la sincronización de los relojes de los sistemas de procesamiento de información tenga una fuente única de referencia horaria. En este mismo sentido, se realizarán las configuraciones necesarias y aplicarán parches para los diferentes sistemas operativos para asegurar la debida sincronización de estaciones de trabajo mediante al Active Directory existente en la CNR.

En el caso de la sincronización de servidores, se deberá utilizar el servidor de tiempo NTP que para el caso de Chile corresponde al servicio ntp.shoa.cl perteneciente al Servicio Hidrográfico y Oceanográfico de la Armada (SHOA).

Instalación de software operacional: En la CNR se controlará la instalación de software en sistemas operacionales. Para el caso de aquellos sistemas que son provistos, administrados y soportados directamente por proveedores externos como son el caso de los sistemas CeroPapel, Docal, Cege, Ungasoft, SED, ESIIR, entre otros y que son coordinados directamente por las respectivas contrapartes administradoras de los centros de responsabilidad existentes en la CNR, incluyendo el Sistema Ley de Fomento al Riego (Ley 18.450) que es administrado y soportado directamente por la Unidad Utic, es necesario que estas contrapartes, controlen y aseguren la actualización del software operacional, las aplicaciones y las bibliotecas de programas lo cual podrá ser realizado solo por los respectivos administradores capacitados.

Los sistemas y el software de sistema operativo solo se podrán implementar en producción después de realizar pruebas exhaustivas y exitosas, considerando la capacidad de uso, la seguridad, el impacto que podría generar sobre otros sistemas y la facilidad de uso para los usuarios.

Antes de la aplicación de los cambios en los sistemas, se retendrán las versiones anteriores del software de aplicación como medida de contingencia (vuelta atrás). La CNR considerará los riesgos de utilizar software sin soporte.

Cualquier decisión de actualizar a una nueva versión de software y sistemas, deberá considerar los requisitos del negocio para el cambio y la seguridad de la información. Se deberían aplicar parches de software cuando puedan ayudar a eliminar o reducir las debilidades de la seguridad de la información.

En la CNR solo deberá permitirse el acceso físico o lógico a los proveedores para fines de soporte o mantenimiento cuando sea necesario y con la aprobación de las jefaturas correspondientes, y para lo cual los respectivos Administradores de los Sistemas de Información de los centros de responsabilidad serán los responsables de monitorear las actividades de dichos proveedores.

Registro de eventos: En la CNR, los eventos de seguridad de la información se registrarán y en el Sistema de Servicios Generales (SSG) generando evidencias de estos, considerando detalles de los eventos claves, Los registros de eventos establecerán las bases para los sistemas de monitoreo para generar informes y alertas consolidadas sobre la seguridad del sistema.

Los administradores de los sistemas o servicios no podrán tener permisos para borrar o desactivar los registros de sus actividades.

Separación de entornos de desarrollo, pruebas y operacionales: En la CNR, se garantizarán las operaciones correctas y seguras de las instalaciones de procesamiento de información.

Los entornos de desarrollo, pruebas y explotación deberán estar separados para reducir los riesgos del acceso o cambios no autorizados al entorno operacional., considerando los siguientes elementos:

- El software de desarrollo y de explotación se ejecutarán en distintos sistemas o procesadores y en distintos dominios y directorios.
- Los cambios a los sistemas y aplicaciones se probarán en un entorno de pruebas o etapas antes de aplicarlos a los sistemas en explotación.
- Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no podrán estar accesibles desde los sistemas en explotación.
- Los usuarios utilizarán distintos perfiles de usuario para los sistemas en explotación y de pruebas y se mostrarán mensajes de identificación adecuados para reducir el riesgo de errores.
- Los datos sensibles no se copiarán en el entorno del sistema de pruebas a menos que se entreguen controles equivalentes para el sistema de pruebas.

Registro de evento: En la CNR, se registrarán los eventos de seguridad en el Sistema de Servicios Generales (SSG), generando evidencias de los incidentes y los eventos de fallas que impacten sobre los activos de información.

Dichos registros deben describir las actividades, fechas, horas y detalles de los eventos.

Registros del administrador y el operador: En la CNR, las actividades del administrador y del operador del sistema se controlarán y registrarán.

Gestión de las vulnerabilidades técnicas: En la CNR se deben gestionar y remediar las vulnerabilidades técnicas de los sistemas de información en uso, tomando

cuánto antes las medidas apropiadas y oportunas en respuesta a su remediación.
Debe existir un inventario detallado y preciso de activos de software y plataforma TI, el cual debe incluir el proveedor de software, nombre del software, números de versión, estado actual de implementación y la(s) persona(s) dentro de la organización responsable del software y otras tecnologías, por lo que se deberá:

1. Exigir a los proveedores de sistemas de información que remedien y aseguren las vulnerabilidades identificadas.
2. Usar herramientas de identificación de vulnerabilidades para identificar vulnerabilidades.
3. Realizar pruebas de penetración o evaluaciones de vulnerabilidad planificadas, repetibles para apoyar la identificación de vulnerabilidades
4. Verificar que las actividades de respuesta y remediación han sido aplicadas.
5. Implementar un proceso de administración de actualizaciones de software para garantizar la aprobación más actualizada.
6. Instalan parches y actualizaciones de aplicaciones para todo el software autorizado considerando que todos los cambios deben ser completamente probados y documentados.
7. La remediación de las vulnerabilidades técnicas se deberá llevar a cabo de acuerdo con los controles relacionados con la gestión del cambio siguiendo los procedimientos de respuesta a incidentes de seguridad.
8. Utilizar únicamente actualizaciones de software de fuentes legítimas (que pueden ser internas o externas a la organización).
9. Probar y evaluar las actualizaciones antes de instalarlas para garantizar que sean efectivas y no resultar en efectos secundarios que no se pueden tolerar.
10. Aplicar actualizaciones o parches de seguridad de software de manera regular y preventiva considerando controles de cambio y pruebas previas en ambientes no productivos para no afectar la disponibilidad de los servicios digitales entregados por la CNR.
11. Realizar pruebas para confirmar si la remediación o mitigación es efectiva.
12. Proporcionar mecanismos y evidencias para verificar la autenticidad y la efectividad de la remediación.

Consideraciones a tener presente:
Si no existen actualizaciones disponibles o las actualizaciones no se puede instalar, considere otros controles, tales como:

1. Aplicar cualquier solución alternativa sugerida por el proveedor de software u otras fuentes relevantes;
2. Apagar servicios o capacidades relacionadas con la vulnerabilidad;
3. Adaptar o agregar controles de acceso (por ejemplo, reglas en firewalls) en los límites de la red.
4. Proteger sistemas, dispositivos o aplicaciones vulnerables de ataques mediante el despliegue de filtros de tráfico adecuados (llamados parches virtuales).
5. Aumentar el monitoreo para detectar ataques reales.
6. Para el software adquirido, si los proveedores publican regularmente información sobre actualizaciones de seguridad para sus softwares y proporcionar una instalación para instalar dichas actualizaciones automáticamente, la organización debe decidir si usar la actualización automática o no.
7. Se debe mantener un registro de auditoría para todos los pasos realizados en la gestión de remediación de vulnerabilidades técnicas.
8. El proceso de gestión de vulnerabilidades técnicas debe ser monitoreado y evaluado regularmente para asegurar su eficacia y eficiencia.
9. Debe existir un procedimiento técnico a realizar en caso de incidencia.
10. Cuando la organización utiliza servicios proporcionados por un proveedor de servicios en la nube (plataforma externa a CNR), el servicio en la nube debe garantizar la gestión de vulnerabilidades de los recursos del proveedor de servicios.
11. Las responsabilidades del proveedor de servicios en la nube para la gestión de vulnerabilidades técnicas deben ser parte del acuerdo de servicio en la nube y esto debe incluir procesos para informar el servicio en la nube acciones del proveedor relacionadas con vulnerabilidades técnicas. Para algunos servicios en la nube, hay responsabilidades respectivas para el proveedor de servicios en la nube y el cliente del servicio en la nube.
12. La gestión de las vulnerabilidades técnicas puede verse como una subfunción de la gestión del cambio y como tales pueden aprovechar los procesos y procedimientos de gestión de cambios.
13. La organización debe cuidar en la revisión y actuación sobre los informes de vulnerabilidad.
14. Se debe considerar también que, los softwares o sistemas suministrados por partes interesadas pueden tener vulnerabilidades de seguridad de la información que podrían comprometer los activos de información existentes en la CNR y los servicios que son ofrecidos.

Restricciones en la instalación de software: En la CNR, para evitar la explotación de vulnerabilidades técnicas se implementarán reglas y pautas que rijan para la instalación de software por parte de los usuarios, debiéndose aplicar el principio de los menores privilegios.
Separación de entornos de desarrollo, pruebas y operacionales: En la CNR, los entornos de desarrollo, pruebas y explotación (o producción), estarán separados para reducir los riesgos del acceso o cambios no autorizados al entorno operacional, implementando el nivel de separación entre los entornos de explotación (o producción), de prueba y desarrollo necesario para evitar los problemas operacionales.
Instrumento de formalización

- Políticas específicas de seguridad de la información por dominio
- PD-UTIC-01 Desarrollo de Módulos de Software
- PD-UTIC-02 Continuidad Operacional de Tecnología
- Instructivos Utic

POLÍTICA SEGURIDAD EN LAS COMUNICACIONES

La presente política declara su aplicabilidad para el control definido en la Norma NCh-ISO27.001:Of2013, más particularmente en sus controles:

- A-13.01.01 Control de Redes
- A-13.01.02 Seguridad de los servicios de Red
- A-13.01.03 Segregación de Redes
- 5.14 Transferencia de Información (ISO 27002:2022)

Declaración institucional

La presente política se enmarca dentro de la POLÍTICA General de Seguridad de la información de la CNR junto con la normativa respectiva vigente y en este sentido, en la CNR 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 el alcance, lineamientos, actores, responsabilidades y los procedimientos necesarios para velar por el cumplimiento de medidas y desarrollar la gestión y operación en materias relacionadas con la Seguridad en las Comunicaciones a través del Sistema de Seguridad de la Información implementado en la CNR.

Objetivo de la política de seguridad de las comunicaciones

Garantizar la protección de la información en las redes de comunicaciones existentes en la CNR y en sus instalaciones de procesamiento de información, considerando:

- Administrar y controlar las redes para proteger la información en los sistemas y aplicaciones.
- Segregar los grupos de servicios de información, usuarios y sistemas de información en las redes.

Alcance y/o ámbito de aplicación

El alcance de la presente política se extiende a los servicios de redes de comunicaciones e instalaciones relativas al procesamiento de datos existentes en la CNR.
Esta política es aplicable a todos los funcionarios/as, la suplencia y el personal a honorarios que en la facultad de sus funciones le ha sido asignado funciones de administración de redes y comunicaciones y de la infraestructura tecnológica existentes en la CNR.

Responsabilidades específicas

Administradores de los Sistemas de Información de los respectivos centros de responsabilidad

- Para el caso de aquellos sistemas que son provistos, administrados y soportados directamente por proveedores externos como son el caso de los sistemas CeroPapel, Docal, Cege, Ungasoft, SED, ESIIR, entre otros que son coordinados directamente por las respectivas contrapartes administradoras de los centros de responsabilidad existentes en la CNR, dichas contrapartes controlarán y se asegurarán que los accesos realizados por los proveedores de los respectivos Sistemas de Información a su cargo sean realizados a través de conexión de redes privadas virtuales (VPN), debiendo establecer las responsabilidades y procedimientos para la administración de los accesos a equipos de redes.
- Velar por que ninguna persona pueda acceder, modificar ni utilizar activos sin autorización estableciendo controles especiales para resguardar la confidencialidad y la integridad de los datos que se transmiten a través de redes públicas o de redes inalámbricas y para proteger a los sistemas y aplicaciones.
- Asegurar que los respectivos Sistemas de Información a su cargo contengan autenticación para el acceso de los usuarios/as a la red, debiendo además restringir la conexión de los sistemas a la red.
- Satisfacer los requerimientos de seguridad de la información establecidos para la operación, administración y comunicación de los sistemas de información y que tienen a su cargo en la CNR.

Analista de Redes y Comunicaciones

- Administrar, gestionar y controlar las redes y comunicaciones existentes en la CNR para proteger la información y garantizar la disponibilidad de los servicios de comunicaciones existentes en la CNR.
- Cautelar y velar por los activos de información a cargo de la Unidad de Tecnología de la Información y la Comunicación (Utic) asegurando el cumplimiento de los controles del sistema de seguridad de la información.
- Implementar controles para garantizar la seguridad de la información en las redes y las comunicaciones para la protección de los servicios conectados de accesos no autorizado que pudieran comprometer los servicios y la plataforma tecnológica de la CNR.
- Establecer controles especiales y realizar el monitoreo continuo para resguardar la confidencialidad y la integridad de los datos que se transmiten por las redes públicas o a través de redes inalámbricas.
- Garantizar que los sistemas sean autenticados en la red.
- Restringir la conexión de los sistemas a la red, segregando los grupos de servicios de información, usuarios y sistemas de información en las redes y servicios de comunicaciones existentes, en la CNR.
- Emitir reportes periódicos con los registros de análisis del estado de las redes existentes en la CNR.

Lineamientos

En la CNR, las redes de comunicaciones estarán interconectadas a la Red de Conectividad del Estado (RCE) y operarán basadas en protocolos y estándares abiertos para redes de paquetes, debiendo ser compatibles con las normas y estándares de Internet Protocol (IP) o aquellas que le reemplacen.
Los usuarios/as de la CNR sólo podrán tener acceso a las redes de datos internas y a los sistemas o servicios a los que les está permitido, además del servicio de red de conectividad y comunicaciones provistos por la Red de Conectividad del Estado (RCE) de conformidad al DS.83 12/01/2005 - Art33.
Junto con lo anterior, se tomarán las precauciones necesarias para garantizar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo de conformidad a las siguientes normativas:

Control de Redes

- Se establecerán las responsabilidades para la administración de los equipos de redes.
- En la CNR las redes de comunicaciones se administrarán y controlarán para proteger la información de los sistemas y aplicaciones. Para ello se implementan controles adecuados para garantizar la seguridad de la información en las redes de comunicaciones y la protección de los servicios conectados del acceso no autorizado.
- Se establecerán controles especiales para resguardar la confidencialidad y la integridad de los datos que se pasan a redes públicas o a través de redes inalámbricas y para proteger a los sistemas y aplicaciones.
- Se aplicarán mecanismos de monitoreo adecuados para permitir el registro y la detección de acciones que pueden afectar o comprometer los servicios de comunicaciones que son entregados por la CNR.
- Los usuarios/as tienen por obligación autenticarse para acceder a los sistemas de la red.
- Se controlará y restringirá la conexión a los sistemas, los servicios y a las redes de comunicaciones existentes en la CNR, establecer controles de gestión y procedimientos para proteger el acceso a las conexiones de la red y servicios de red.

Seguridad de los servicios de Red: En la CNR se garantizará la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo, determinando y monitoreando de manera regular la capacidad de los proveedores de los servicios de red para administrarlos de manera segura.
Segregación de Redes: En la CNR serán segregados los grupos de servicios de información, usuarios, sistemas y sistemas de información en las redes a través de dominios de “acceso público”, “acceso visitas”, acceso proveedores), “redes de datos”, ”red de servidores”, “unidades organizacionales (Por ejemplo, Gestión de Personas, Área de Fomento, Estudios y Desarrollo de Políticas, Administración y Finanzas, Gestión Estratégica, Secretaría Ejecutiva,..). Dicha segregación se podrá realizar mediante redes con diferencias físicas o mediante el uso de distintas redes lógicas definiendo el perímetro de cada una de ellas.
En la CNR, se permitirá el acceso entre dominios controlando su perímetro mediante un firewall o enrutador de filtrado.
Respecto de las redes inalámbricas existentes en la CNR, se considerarán controles para la segregación de los accesos para las conexiones internas y externas.
El control de acceso de nivel de usuario a las redes inalámbricas existentes en la CNR deberá ser a través de autenticación y cifrado.

Transferencia de Información (ISO 27002:2022 – Ctrl.5.14)

En la CNR deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de transferencia para mantener la seguridad de la información transferida dentro de una organización y con cualquier parte interesada y proteger la información en tránsito.

Cuando la información se transfiere información entre la CNR y terceros, los acuerdos de transferencia (incluida la autenticación del destinatario) deben ser establecidos y mantenido para proteger la información en todas sus formas en tránsito.

La transferencia de información puede ocurrir a través de transferencia electrónica, transferencia de medios de almacenamiento físico y transferencia verbal.
Para todo tipo de transferencia de información, las reglas, procedimientos y acuerdos deben incluirse:

1. Controles diseñados para proteger la información transferida de intercepción, acceso no autorizado, copia, modificación, enrutamiento erróneo, destrucción y

denegación de servicio, incluidos los niveles de acceso control acorde con la clasificación de la información involucrada y cualquier control especial que se requieren para proteger la información confidencial, como el uso de técnicas criptográficas.
2. Controles para garantizar la trazabilidad y el no repudio, incluido el mantenimiento de una cadena de custodia para información en tránsito.
3. Identificación de los contactos apropiados relacionados con la transferencia.
   d) Responsabilidades y obligaciones en caso de incidentes de seguridad de la información, como la pérdida de medios de almacenamiento o datos;
4. Uso de un sistema de etiquetado acordado para información sensible o crítica, asegurando que el significado de las etiquetas se comprenda de inmediato y que la información esté debidamente protegida.

Fiabilidad y disponibilidad del servicio de traslado

1. Pautas de retención y eliminación para todos los registros, incluidos los mensajes;
2. La consideración de cualquier requisito legal, estatutario, reglamentario y contractual pertinente relacionados con la transferencia de información (por ejemplo, requisitos para

firmas).

Transferencia electrónica

También deben tener en cuenta los siguientes elementos cuando se utilicen medios electrónicos facilidades de comunicación para la transferencia de información:
a) Detección y protección contra malware que puede transmitirse mediante el uso de dispositivos electrónicos comunicaciones.
b) Protección de la información electrónica sensible comunicada que se encuentra en forma de archivo adjunto.
c) Prevención contra el envío de documentos y mensajes en las comunicaciones a la dirección equivocada o número.
d) Obtener aprobación antes de usar servicios públicos externos como mensajería instantánea, redes sociales redes, intercambio de archivos o almacenamiento en la nube
e) Niveles más fuertes de autenticación al transferir información a través de redes de acceso público;
f) Restricciones asociadas con las instalaciones de comunicación electrónica (p. ej., prevención de reenvío de correo electrónico a direcciones de correo externas);

Transferencia de medios de almacenamiento físico

Al transferir medios físicos de almacenamiento (incluido el papel), las reglas, los procedimientos y los acuerdos deben también incluir:
a) Responsabilidades de control y notificación de la transmisión, despacho y recepción;
b) Asegurar el correcto direccionamiento y transporte del mensaje;
c) Embalaje que protege el contenido de cualquier daño físico que pueda surgir durante el tránsito y de acuerdo con las especificaciones de cualquier fabricante.
d) Verificar la identificación de los mensajeros;
e) Mantener registros para identificar el contenido de los medios de almacenamiento, la protección aplicada, así como registrar la lista de destinatarios autorizados, los tiempos de transferencia a los custodios de tránsito y recibo en destino.

Instrumento de formalización

- Políticas específicas de seguridad de la información por dominio
- PD-UTIC-02 Continuidad Operacional de Tecnología
- Instructivos Utic

POLÍTICA RELACIONES CON LOS PROVEEDORES Y USO DE SERVICIOS CLOUD

La presente política declara su aplicabilidad para los controles definidos en la norma NCh-ISO27.001:Of2013, más particularmente en su control:

- 5.19 Seguridad de la Información en servicios de proveedores (ISO – 27002:2022)
  (A-15.01.01 Política de Seguridad de la Información para las relaciones con los proveedores)
- 5.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores (ISO – 27002:2022)
  (A-15.02.01 Monitoreo y revisión de los servicios del proveedor)
- 5.23 Seguridad de la información en el uso de servicios Cloud (ISO – 27002:2022)

Declaración institucional

La presente política se enmarca dentro de la Política General de Seguridad de la información de la CNR junto con la normativa respectiva vigente y en este sentido, en la CNR 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 el alcance, lineamientos, actores, responsabilidades y los procedimientos y medidas necesarias para velar por el cumplimiento de medidas y desarrollar la gestión y operación en materias relacionadas con las Relaciones con los Proveedores a través del Sistema de Seguridad de la Información implementado en la CNR, definiendo e implementarse procesos y procedimientos para gestionar la seguridad de la información y los riesgos asociados con el uso de los productos o servicios del proveedor.

Objetivo de la política de relaciones con los proveedores

Establecer los requisitos de seguridad de la información para cuando se realice la contratación de servicios externos, asociados al acceso de proveedores a los activos de información de la Comisión Nacional de Riego, incluido todo el personal externo que trabaja para la Institución y que, en el desarrollo de sus funciones, pueda tener acceso a información crítica, con el fin de proteger la confidencialidad, integridad y disponibilidad de ésta.

Mantener un nivel acordado de seguridad de la información en las relaciones con los proveedores y en la prestación de servicios en línea con los acuerdos establecidos.

Garantizar que en los procesos de adquisición, uso, gestión y finalización de los servicios en la nube se establecen acuerdos con los requisitos de seguridad de la información de la organización, especificando y administrando la seguridad de la información para el uso de servicios en la nube.

Alcance y/o ámbito de aplicación

El alcance de la presente política se extiende y aplica a todas las actividades desarrolladas por proveedores y personal externo que presta servicios para la CNR y que pertenecen a empresas proveedoras de servicios vinculadas a través de contratos vigentes.

Responsabilidades especificas

División Jurídica y Departamento de Administración y Finanzas

- Dar cumplimiento a lo establecido en esta Política.
- Dar cumplimiento a lo establecido en el Manual de Compras.
- Incluir en los contratos las respectivas cláusulas de confidencialidad según sea el caso.

Proveedores

- Dar estricto cumplimiento a las directrices y normas de seguridad descritas en la presente Política de Seguridad de la Información.
- Asegurarse de que el proveedor mantenga suficiente capacidad de servicio junto con planes viables diseñado para garantizar que los niveles de continuidad del servicio acordados se mantengan después de un servicio principal fallas o desastres.
- Informarse de la Política de Seguridad de la Información vigente de la CNR, la cual es difundida a través de la página WEB www.cnr .gob.cl.

De los Administradores de los Sistemas de Información y Servicios digitales de la Áreas y Unidades

- Gestionar las relaciones con los proveedores
- Monitorear el cumplimiento de los requisitos de seguridad de la información establecidos para cada proveedor y tipo de acceso, incluida la revisión de terceros y la validación del producto;
- Gestionar los incidentes y contingencias asociados con los productos y servicios del proveedor, incluyendo responsabilidades tanto de la organización como de los proveedores;
- Evaluar y gestionar los riesgos de seguridad de la información asociados con mal funcionamiento o vulnerabilidades de los productos (incluidos los componentes de software y sub-componentes utilizados en estos productos) o servicios prestados por los proveedores;
- Tomar las acciones apropiadas cuando se observen deficiencias en la prestación de los servicios

Lineamientos

Proveedores

- Todo personal externo que desarrolle labores para la Comisión Nacional de Riego deberá tomar conocimiento de la Política General de Seguridad de la Información, disponible en el sitio WEB www.cnr.gob.cl, observando sus directrices y colaborando en su aplicación dentro del su ámbito de acción. Para estos efectos, el trabajo o proyectos realizados por el proveedor deben ser compatibles con los estándares de seguridad de la información establecidos en CNR.
- Los proveedores sólo podrán desarrollar para CNR aquellas actividades con el personal perteneciente a sus empresas proveedoras y acuerdo a lo establecido en las correspondientes bases y contratos de provisión de servicios.
- De acuerdo con lo establecido en las cláusulas asociadas al contrato de provisión de servicio, todo el personal externo que desarrolle labores para la CNR deberá cumplir con las directrices definidas en el presente documento. En caso de incumplimiento de cualquiera de estas obligaciones, CNR se reserva el derecho de veto sobre el personal que haya cometido la infracción, así como las sanciones que se consideren pertinentes en la relación a la empresa o persona contratada y la aplicación de multas según corresponda.
- Cualquier intercambio de registros de información que se produzca entre CNR y los proveedores, deberá estar debidamente autorizada se entenderá que se ha realizado dentro del marco establecido por el contrato de provisión de servicios correspondiente, de modo que dicha información no podrá ser utilizada en ningún caso fuera de dicho marco, para fines diferentes a los asociados a dicho contrato.
- Ninguna persona, tanto interna como externa, debe ocultar o manipular su identidad en ninguna circunstancia.

Confidencialidad de la Información

- El personal externo que tenga acceso a información de CNR se obliga a considerar que dicha información, por defecto, tiene el carácter de confidencial.
- Se podrá considerar como información no confidencial solo aquella con la cual el proveedor tuvo acceso a través de medios de difusión pública, dispuesto por CNR.
- Queda prohibido para los proveedores revelar, modificar, destruir o hacer mal uso de la información, cualquiera sea el soporte en que se encuentre contenida.
- El proveedor deberá resguardar por tiempo indefinido la confidencialidad y no podrá difundir la información a la que tiene acceso, salvo que esté debidamente autorizado por el responsable de ella.
- Ningún proveedor dará usos no propios de su responsabilidad, a ningún material o información propia o confiada por CNR.
- En el caso de que motivos directamente relacionados con el puesto de trabajo o los accesos entregados, el personal externo de la empresa proveedora que tome conocimiento de dicha información confidencial contenida en cualquier soporte, deberá considerar dicha información como confidencial y se verá en la obligación de no difundirla por ningún medio. Asimismo, el personal externo deberá devolver el o los soportes mencionados, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos.
- Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para CNR.
- El incumplimiento de estas obligaciones será sancionado en los términos establecidos por las leyes vigentes.

Propiedad Intelectual

- El personal externo está obligado a garantizar el cumplimiento de las restricciones legales al uso material protegido por las normas de propiedad intelectual.
- Queda estrictamente prohibido el uso de programas informáticos que no cuenten con su respectiva licencia.
- 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.

Intercambio de Información

En el marco del contrato con proveedores, se considerarán como no autorizadas las siguientes actividades:

- Transmisión o recepción de material protegido por Copyright infringiendo la ley de protección intelectual.
- Transmisión o recepción de toda clase de material pornográfico, mensajes o de una naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Transferencia de archivos a terceras partes no autorizadas de material de CNR.
- Transmisión o recepción de archivos que infrinjan la Ley de Protección de Datos de Carácter Personal (Ley N° 19.628) o directrices de CNR.
- Quienes trabajen en conjunto con CNR, no deben divulgar información sobre los procesos internos de éste.
- Toda salida de información que contenga datos de carácter personal (tanto en soportes digitales como en papel o por correo electrónico) solo podrá ser realizada por personal autorizado y con la debida autorización del responsable de esta información.
- Si el tratamiento de datos de carácter personal se llevase a cabo fuera de las instalaciones de CNR, dicho tratamiento deberá ser autorizado expresamente por el dueño y responsable de esa información y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de información tratado.

Monitoreo y revisión de los servicios del proveedor:
La CNR monitorea, revisa, evaluar y gestionar periódicamente los cambios en la información del proveedor, prácticas de seguridad y prestación de servicios.
El seguimiento, la revisión y la gestión de cambios de los servicios del proveedor deben garantizar que la información se cumplen los términos y condiciones de seguridad de los acuerdos, que los incidentes de seguridad y los problemas se gestionan correctamente y los cambios en los servicios del proveedor o el estado comercial no afectan prestación de servicios.
Lo anterior involucra un proceso de relación administrativa de servicios entre la CNR y el proveedor para:
a) Monitorear los niveles de desempeño del servicio para verificar el cumplimiento de los acuerdos;
b) Controlar los cambios realizados por los proveedores, incluidos:
1) mejoras a los servicios actuales ofrecidos;
2) desarrollo de nuevas aplicaciones y sistemas;
3) modificaciones o actualizaciones de las políticas y procedimientos del proveedor;
4) controles nuevos o modificados para resolver incidentes de seguridad de la información y mejorar la información seguridad;
c) Monitorear los cambios en los servicios del proveedor, incluidos;
1) cambios y mejoras a las redes;
2) uso de nuevas tecnologías;
3) adopción de nuevos productos o versiones o lanzamientos más nuevos;
4) nuevas herramientas y entornos de desarrollo;
5) cambios en la ubicación física de las instalaciones de servicio;
6) cambio de subproveedores;
7) subcontratación a otro proveedor;
d) Revisar los informes de servicio producidos por el proveedor y organizar reuniones regulares de progreso según sea necesario por los acuerdos;
e) Realizar auditorías de proveedores y subproveedores, junto con la revisión de los auditores independientes informes, si están disponibles, y seguimiento de los problemas identificados;
f) Proporcionar información sobre incidentes de seguridad de la información y revisar esta información según sea necesario por los acuerdos y cualquier guía y procedimiento de apoyo;
g) Revisar las pistas de auditoría de los proveedores y los registros de eventos de seguridad de la información, problemas operativos, fallas, rastreo de fallas e interrupciones relacionadas con el servicio entregado;
h) Responder y gestionar cualquier evento o incidente de seguridad de la información identificado;
i) Identificar vulnerabilidades de seguridad de la información y gestionarlas;
j) Revisar los aspectos de seguridad de la información de las relaciones del proveedor con sus propios proveedores;
k) Asegurarse de que el proveedor mantenga suficiente capacidad de servicio junto con planes viables diseñado para garantizar que los niveles de continuidad del servicio acordados se mantengan después de un servicio principal fallas o desastres.
l) Asegurar que los proveedores asignen responsabilidades para revisar el cumplimiento y hacer cumplir los requisitos de los acuerdos;
m) Evaluar periódicamente que los proveedores mantienen niveles adecuados de seguridad de la información.
Además, en la CNR se identifican e implementar procesos y procedimientos para abordar los riesgos de seguridad asociados con el uso de productos y servicios proporcionados por los proveedores. Esto también debería aplicarse a al uso que hace la organización de los recursos de los proveedores de servicios en la nube. Estos procesos y procedimientos deben incluyen aquellas que serán implementadas por la organización, así como aquellas que la organización requiere proveedor a implementar para el comienzo del uso de los productos o servicios de un proveedor o para la terminación del uso de los productos y servicios de un proveedor, tales como:
a) Evaluar y seleccionar los productos o servicios del proveedor que cuenten con la seguridad de la información adecuada, controles y la revisión de los mismos; en particular, la exactitud e integridad de los controles implementados por el proveedor que asegure la integridad de la información del proveedor y el procesamiento de la información y de ahí la seguridad de la información de la organización.
b) Definir la información de la organización, los servicios TIC y la infraestructura física que los proveedores puede acceder, monitorear, controlar o usar.
c) Definir los tipos de componentes y servicios de infraestructura de TIC proporcionados por los proveedores que pueden afectar la confidencialidad, integridad y disponibilidad de la información de la organización.
d) Evaluar y gestionar los riesgos de seguridad de la información asociados con mal funcionamiento o vulnerabilidades de los productos (incluidos los componentes de software y sub-componentes utilizados en estos productos) o servicios prestados por los proveedores;
e) Monitorear el cumplimiento de los requisitos de seguridad de la información establecidos para cada proveedor y tipo de acceso, incluida la revisión de terceros y la validación del producto;
f) El manejo de incidentes y contingencias asociados con los productos y servicios del proveedor, incluyendo responsabilidades tanto de la organización como de los proveedores;
g) medidas de resiliencia y, en su caso, de recuperación y contingencia para asegurar la disponibilidad de la información del proveedor y el procesamiento de la información y, por lo tanto, la disponibilidad de los recursos de la organización. información;
h) sensibilización y formación del personal de la organización que interactúa con el personal del proveedor con respecto a las reglas apropiadas de participación, políticas, procesos y procedimientos específicos del tema y comportamiento basado en el tipo de proveedor y el nivel de acceso del proveedor a la organización sistemas e información.
En la CNR también se deberá garantizar una terminación segura de la relación con el proveedor, incluidos:
1) desaprovisionamiento de derechos de acceso;
2) manejo de la información;
3) determinar la propiedad de la propiedad intelectual desarrollada durante el compromiso;
4) portabilidad de la información en caso de cambio de proveedor o internalización;
5) gestión de registros;
6) devolución de bienes;
7) eliminación segura de información y otros activos asociados;
8) establecer requisitos continuos de confidencialidad;
9) nivel de seguridad del personal y seguridad física que se espera del personal y las instalaciones del proveedor.

Los procedimientos para continuar con el procesamiento de la información en caso de que el proveedor no pueda suministrar sus productos o servicios (por ejemplo, debido a un incidente, porque el proveedor ya no está en el negocio, o ya no proporciona algunos componentes debido a los avances tecnológicos) debe considerarse evitar cualquier retraso en la organización de productos o servicios de reemplazo (por ejemplo, identificar un proveedor alternativo con antelación o siempre utilizando proveedores alternativos).

Seguridad de la información en el uso de servicios Cloud (ISO 27002:2022 – Crtl.5.23)
En la CNR, el uso de servicios en la nube implica una responsabilidad compartida por la colaboración y el esfuerzo entre el proveedor de servicios en la nube y la organización que actúa como cliente del servicio en la nube, por lo cual es fundamental que las responsabilidades tanto del proveedor de servicios en la nube como de la organización, actuando como el cliente del servicio en la nube, se definen e implementan adecuadamente.
En función de lo anterior, la CNR debe definir:
a) En cada contrato los requisitos de seguridad de la información pertinentes asociados con el uso de los servicios en la nube.
b) Criterios de selección de contratación de servicios en la nube y alcance del uso del servicio.
c) Las funciones y responsabilidades relacionadas con el uso y la gestión de los servicios en la nube;
d) Los controles de seguridad gestiona el proveedor de servicios en la nube y los que son gestionado por la organización como cliente del servicio en la nube.
e) Las garantías sobre los controles de seguridad implementados por los proveedores de servicios en la nube.
f) Cómo se administran controles, interfaces y cambios en los servicios cuando se utilizan múltiples servicios en la nube.

g) El monitoreo, revisión y evaluación del uso continuo de los servicios en la nube para administrar riesgos de seguridad de la información;
h) Cómo cambiar o detener el uso de los servicios en la nube, incluidas las estrategias de salida para los servicios en la nube,
La CNR debe revisar los acuerdos de servicios en la nube con los proveedores de servicios considerando la confidencialidad, integridad, disponibilidad y manejo de la información requisitos de la organización, con objetivos de nivel de servicio en la nube apropiados y servicios en la nube objetivos cualitativos.
El servicio debe estar claramente identificado y aceptado por la dirección.

Los acuerdos entre el proveedor de servicios en la nube y la CNR, debe incluir las siguientes disposiciones para la protección de los datos de la organización y disponibilidad de servicios:
a) Proporcionar soluciones basadas en estándares aceptados por la industria para la arquitectura y la infraestructura;
b) Administrar los controles de acceso del servicio en la nube para cumplir con los requisitos de la organización;
c) Implementar soluciones de protección y monitoreo de malware;
d) Procesar y almacenar la información confidencial de la organización en ubicaciones aprobadas (p. país o región en particular) o dentro o sujeto a una jurisdicción en particular;
e) Brindar soporte dedicado en caso de un incidente de seguridad de la información en el servicio en la nube ambiente;
f) Garantizar que se cumplan los requisitos de seguridad de la información de la organización en caso de nube los servicios se subcontratan aún más a un proveedor externo (o se prohíben los servicios en la nube de ser subcontratado);
g) Apoyar a la organización en la recopilación de evidencia digital, teniendo en cuenta las leyes y regulaciones para evidencia digital en diferentes jurisdicciones;
h) Proporcionar apoyo apropiado y disponibilidad de servicios durante un período de tiempo apropiado cuando la organización quiere salir del servicio en la nube;
i) Proporcionar la copia de seguridad necesaria de los datos y la información de configuración y gestionar las copias de seguridad de forma segura según corresponda, en función de las capacidades del proveedor de servicios en la nube utilizado por la organización, actuar como cliente del servicio en la nube
j) Proporcionar y devolver información como archivos de configuración, código fuente y datos que son propiedad de la organización, actuando como el cliente del servicio en la nube, cuando se le solicite durante la prestación del servicio o al término del servicio.
La CNR, actuando como cliente del servicio en la nube, debe considerar si el acuerdo debe exigir a los proveedores de servicios en la nube que proporcionen una notificación previa antes de cualquier cambio sustancial impactante que se va a realizar, incluyendo:
a) Cambios en la infraestructura técnica (por ejemplo, reubicación, reconfiguración o cambios en el hardware o software) que afectan o cambian la oferta de servicios en la nube;
b) Procesar o almacenar información en una nueva jurisdicción geográfica o legal;
c) Uso de proveedores de servicios en la nube similares u otros subcontratistas.
Instrumento de formalización

- Políticas específicas de seguridad de la información por dominio
- PD-UTIC-02 Continuidad Operacional de Tecnología
- Instructivos Utic
- PD-CCP-03 Compras y Contrataciones

Inteligencia de Amenazas

Inteligencia de Amenazas (ISO – 27002:2022 – Crtl. 5.7)
Declaración institucional
En la CNR, la información relacionada con las amenazas a la seguridad de la información se recopila y analiza para generar inteligencia de amenazas y proporcionar conciencia del entorno de amenazas de la organización para realizar la mitigación apropiada.
Lineamientos
La información sobre amenazas existentes o emergentes se recopila y a menudo es proporcionada por proveedores, organismos gubernamentales o grupos colaborativos de inteligencia de amenazas.
En la CNR las actividades de inteligencia de amenazas deben incluir
a) Identificar, examinar y seleccionar las fuentes de información internas y externas que sean necesarias y apropiado para proporcionar la información requerida para la producción de inteligencia de amenazas.
b) Recopilar información de fuentes seleccionadas, que pueden ser internas y externas.
c) Procesar la información recopilada para prepararla para el análisis (por ejemplo, traduciendo, formateando o información corroborante).
d) Analizar la información para comprender cómo se relaciona y es significativa para la organización.
e) Las amenazas se comunican y comparten con personas relevantes e interesadas en la CNR
f) Controles técnicos preventivos y de detección como cortafuegos, detección de intrusos sistema o soluciones antimalware.
g) La CNR se compromete a compartir información sobre amenazas con otras organizaciones de manera mutua para mejorar la inteligencia general sobre amenazas.
Instrumento de formalización

- Informe técnico de Eventos de Ciberseguridad

POLÍTICA ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La presente política declara su aplicabilidad en los controles definidos en la Norma NCh-ISO27.001:Of2013, más particularmente en sus controles:

- A-16.01.01 Responsabilidades y Procedimientos
- A-16.01.02 Informe de Eventos de Seguridad de la Información
- A-16.01.03 Informe de las debilidades de Seguridad de la Información

Declaración institucional

La presente política se enmarca dentro de la Política General de Seguridad de la Información de la CNR junto con la normativa respectiva vigente y en este sentido, en la CNR 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 el alcance, lineamientos, actores, responsabilidades y los procedimientos y medidas necesarias para velar por el cumplimiento de medidas y desarrollar la gestión y operación en materias relacionadas con la Administración de Incidentes de Seguridad de la Información a través del Sistema de Seguridad de la Información implementado en la CNR.

Objetivo de la política de 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.

Alcance y/o ámbito de aplicación

El alcance de la presente política se extiende a todas las instalaciones que contengan activos de información catalogados como críticos para la Comisión Nacional de Riego.

La presente política es aplicable a todos los funcionarios/as, la suplencia y el personal a honorarios, además de personal externo y contratistas.

Responsabilidades específicas

Encargado de Seguridad de la Información

Revisar y Analizar los eventos de seguridad de la información reportados.

Coordinador de Unidad de Tecnología de la Información y la Comunicación (Utic):

- Administrar los incidentes de seguridad de la información, incluida la comunicación sobre los eventos e incidentes, garantizando que los activos de información no se vean afectados por eventos o incidentes que pudieran afectar la integridad, disponibilidad, confidencialidad y la seguridad de estos.
- En el más mínimo plazo dar respuesta y solución a los incidentes o eventos que pudieran estar afectando a los activos de la información.
- Analizar y emitir informes de debilidades que pudieran generar eventos o incidentes.
- Elaborar periódicamente informes de eventos o incidentes ocurridos en la Plataforma tecnológica y los servicios existentes en la CNR.
- Asegurar que la administración de incidentes de seguridad de la información sea comunicada y acordada con los proveedores u otros asociados a materias de tecnología.

Administradores de los Sistemas de Información de los respectivos centros de responsabilidad

- Analizar, gestionar y dar remediación a los incidentes de seguridad que tengan relación con fallas ocurridas en los sistemas de información y que tienen a su cargo en la CNR.
- Garantizar que el software informático suministrado de manera externa y que está a su cargo, sea monitoreado y controlado para evitar cambios no autorizados y que pueden introducir falencias o incidentes que podrían afectar o comprometer los activos de información de la CNR.

Encargado de la Infraestructura TI y del Encargado de Comunicaciones:

- Analizar, gestionar y dar solución a incidentes de seguridad que tengan relación con fallas de hardware, software y las comunicaciones.
- Velar por el cumplimiento de las disposiciones de seguridad física que pudieran afectar el centro de procesamiento de datos de la CNR
- Controlar y validar los cambios que se pudieran realizar sobre las instalaciones; sistemas a nivel y las comunicaciones, además de mantener actualizadas las plataformas tecnológicas con los respectivos parches de seguridad para evitar comprometer la continuidad de los servicios producto del impacto de incidentes.

Administrador de Bases de Datos:

- Cautelar los activos digitales de información del tipo Bases de Datos, velando por el cumplimiento de las normativas señaladas en esta Política de Administración de Incidentes de Seguridad de la Información.
- Analizar, gestionar y dar solución a incidentes de seguridad que tengan relación con fallas en las Bases de Datos.
- Controlar y validar los cambios que se pudieran realizar sobre los sistemas a nivel de Bases de Datos , además de mantener actualizadas las bases de datos existentes con los respectivos parches de seguridad para evitar comprometer la continuidad de los servicios producto del impacto de incidentes.

Lineamientos

En la CNR se tomarán las precauciones necesarias para establecer las responsabilidades y procedimientos para asegurar la debida administración de incidentes de seguridad de la información registrándose y gestionándose los eventos o incidentes de seguridad de la información.

En la CNR se desarrolla un procedimiento para el tratamiento de los incidentes de seguridad de la información, considerando:

- La detección, el registro, la comunicación y el análisis del evento o Incidente.
- Determinar las causas y sus cuestiones correctivas/preventivas.

Para estos efectos, deberá existir el personal competente para que el manejo y la resolución de los incidentes de seguridad de la información sea efectivo.

Responsabilidades y Procedimientos: En la CNR se establecen las responsabilidades y los procedimientos necesarios para garantizar una respuesta rápida, eficaz y ordenada frente a los incidentes de seguridad de la información considerando:

- La detección, el analizar, el monitoreo e informar sobre eventos e incidentes de seguridad.
- El registro de actividades de administración de incidentes.
- La evaluación de las debilidades en la seguridad de la información.

En la CNR, el manejo y la resolución de incidentes relacionados con la Seguridad de la Información son manejados por el personal competente, manteniendo los contactos correspondientes con las autoridades, proveedores, grupos de interés externo o foros que manejen y puedan apoyar en la resolución de problemas relacionados con los incidentes de seguridad de la información.

Informe de eventos de seguridad de la información: En la CNR, los eventos o incidentes de seguridad de la información serán gestionados controlados e informados a través del de los Sistema de Servicios Generales (SSG) existente en la CNR por los respectivos custodios de los activos de información debiendo ser informado al Encargado de Seguridad de la información en el menor tiempo posible.

Las situaciones y/o causales de eventos o incidentes de seguridad consideran:

- Cambios no controlados en el sistema.
- Fallas en el software o hardware.
- Errores humanos.
- Incumplimientos en las disposiciones de seguridad física.
- El control de seguridad ineficaz
- El incumplimiento de la integridad, la confidencialidad o las expectativas de disponibilidad de la información.

Informe de las debilidades de la seguridad de la información: En la CNR, se requiere que los funcionarios/as y proveedores, que utilizan los sistemas y servicios de información de la organización, tomen nota e informen sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios.

Todos los funcionarios/as y proveedores deberán informar lo más rápido posible estas debilidades al Encargado de Seguridad de la Información para poder evitar futuros incidentes de seguridad de la información.

Los funcionarios/as y los proveedores no deben intentar indagar en debilidades de seguridad sospechosas salvo con la debida autorización del Encargado de Seguridad de la Información y del Dueño del Activo de información, o bien por el rol asociado a Ciberseguridad quien por su naturaleza de actividades podría realizar dichas pruebas e indagaciones de seguridad.

La realización de prueba(s) de debilidades será considerada como uso indebido que podría provocar daños a los sistemas o servicios de información, generando una responsabilidad legal para la persona que realiza la prueba.

Terminología asociada

Seguridad de la Información: La acción sobre todo proceso, actividad o disponibilidad física o digital de los activos de información declarados en la CNR.

Activos de Información: Todos aquel o aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. **Amenaza**: Evento que puede desencadenar un incidente en la organización, produciendo eventualmente daños materiales, o

pérdidas inmateriales en sus activos.
Disponibilidad: Garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
Evento: Una ocurrencia identificada en un sistema, servicio, o cualquier otro elemento. Es una posible brecha de cumplimiento de las políticas/normas/procedimientos o fallas en las medidas de seguridad ya implementadas.
Impacto: Efecto causado en los objetivos de la institución.
Incidente: Está indicado por un simple o múltiples eventos esperados. Esto tiene una alta probabilidad de comprometer continuidad de las operaciones de la misión institucional.

Instrumento de formalización

- Políticas específicas de seguridad de la información por dominio
- PD-UTIC-02 Continuidad Operacional de Tecnología
- Instructivos Utic

POLÍTICA DE CUMPLIMIENTO

La presente política declara su aplicabilidad para el control definido en la norma NCh-ISO27.001:2013, más particularmente en sus controles:

- A.18.01.01 Identificación de la legislación vigente y los requisitos contractuales
- A.18.02.01 Revisión independiente de la seguridad de la información
- A.18.02.02 Cumplimiento con las políticas y normas de seguridad
- A.18.02.03 Verificación del cumplimiento técnico

Declaración institucional
La Comisión Nacional de Riego (CNR), se compromete a evitar incumplimientos normativos, estatutarios, regulatorios y contractuales relacionados con la seguridad de la información, además de garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas, con la normativa vigentes y los procedimientos establecidos en la CNR.
En este sentido, se desarrollan e implementan continuamente las medidas necesarias y tendientes a asegurar el cumplimiento de la norma relativa a la seguridad de la información y para ello son definidos lineamientos, procedimientos, actores y responsables de velar por el cumplimiento en materias de identificación de legislación vigente y requisitos contractuales de la institución a través de los controles dispuestos en el Sistema de Seguridad de la Información implementado en la CNR
Objetivos
Identificar, aplicar y hacer cumplir los requisitos normativos, legales o contractuales que se aplican a la CNR, con el objeto de evitar incumplimientos en este tipo de obligaciones, sin importar el rango jurídico de las mismas, y que digan relación con la seguridad de la información.
Alcance y/o ámbito de aplicación
La presente política está sujeta a las normativas relacionadas con la seguridad de la información y es aplicable a todos los funcionarios/as, ya quienes trabajan en la CNR en calidad de honorarios.
Responsabilidades específicas
Funcionarios/as CNR y personal a honorarios.
Dar cumplimiento a la presente política e identificar cualquier tipo de cuerpo normativo relacionado que se aplique directa o indirectamente a la CNR, respecto de la seguridad de la información, independiente del cargo o función que desempeñen y la situación contractual. Cada uno es responsable de identificar y hacer cumplir la normativa atingente a la seguridad de la información o a cualquier otro tipo de requisito de seguridad.
Todo funcionario o persona que trabaje para la CNR, sin importar su calidad jurídica deberá cuidar que no se duplique, convierta a otro formato libros, artículos, informes o cualquier otro documento, en su totalidad o en parte, salvo que sean permitidos por la Ley de Propiedad Intelectual. Igual criterio debe aplicarse respecto a la duplicación o conversión a diferentes formatos o extracción de grabaciones audiovisuales comerciales.
Departamento de Administración y Finanzas .
La CNR provee los recursos necesarios para que, en cumplimiento a la ley de Propiedad Intelectual y Derechos de Autor, se adquiera cualquier tipo de software licenciado, los que además deben ser adquiridos a proveedores autorizados y confiables, dejando estrictamente prohibido la adquisición y uso de software sin licencia o pirata, y el uso de estos últimos será considerado falta grave y se aplicaran las medidas disciplinarias correspondientes a quien se sorprenda en esta falta o a quienes hubiesen autorizado su adquisición.
División Jurídica
Identificar y revisar la Política General de Seguridad de la Información, sus normativas de cualquier naturaleza jurídica que se aplique directa o indirectamente en la seguridad de la información en la CNR.

Instrumento de formalización

- Resol.Política SSI
- PD-UTIC-02 Continuidad Operacional de Tecnología
- Instructivos Utic
- PD-UTIC-01 Desarrollo de Módulos de Software
- PD-GP-01 Selección, Contratación e Inducción
- PD-CCP-03 Compras y Contrataciones

POLÍTICA PROTECCIÓN DE LOS REGISTROS Y PRIVACIDAD, PROTECCIÓN DE LA INFORMACIÓN DE IDENTIFICACIÓN PERSONAL

Se monitoreará la ejecución de respaldos y se abordarán las fallas de los respaldos programados para garantizar su integridad de acuerdo con la política de respaldos. La presente política declara su aplicabilidad para el control definido en la norma NCh-ISO27.001:2013, más particularmente en sus controles:

- A.18.01.03 Protección de los registros
- A.18.01.04 Privacidad y protección de la información de identificación personal.

Declaración Institucional

La Comisión Nacional de Riego, se compromete a custodiar y proteger sus registros e información de identificación personal de modo tal de proteger contra uso indebido, pérdida, destrucción, falsificación, acceso sin autorización, 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 el resguardo de los registros y la información sensible contenida en ellos, para ello se define lineamientos, procedimientos, actores y responsables de velar por el cumplimiento en materias de resguardo de registros e información de la institución a través de los controles dispuestos en el Sistema de Seguridad de la Información implementado en la CNR

Objetivo de la política de protección de los registros y protección de la información de identificación personal

Aplicar y hacer 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.

Alcance y/o ámbito de aplicación

La presente política aplica a la protección de los registros o información de identificación personal existentes y que son manejados en la CNR.

Esta política es aplicable a todos los funcionarios/as quienes trabajan en la CNR independiente de su calidad jurídica.

Responsabilidades específicas

Departamento de Administración y Finanzas .

Incluir en los contratos de terceras cláusulas de confidencialidad y resguardo de la información, tanto de la información de identificación personal, como de cualquier registro a que tenga acceso por motivo del contrato específico.

Unidad de Personas.

Incluir en los contratos a honorarios cláusulas de confidencialidad y resguardo de la información.

División Jurídica

Identificar y difundir las normativas que definen la protección y privacidad de la información personal y velar por su estricto cumplimiento.

Unidad de Tecnología de la Información y la Comunicación (Utic)

Velar por la protección de la privacidad y la protección de la información personal identificable según se requiere en la legislación y las normativas pertinentes, garantizando los principios de privacidad implementando las medidas técnicas adecuadas para proteger la información personal identificable.

Realizar respaldos de la información asegurando su proceso de recuperación considerando la implementación de soluciones de respaldo sistemas, programas, configuraciones, bases de datos e información considerada como crítica para la institución.

Probar de manera regular los medios de recuperación de respaldos para garantizar que se puede confiar en ellos frente a su uso ante emergencias.

Funcionarios/as CNR y personal a honorarios.

Dar cumplimiento a la presente política, y a los cuerpos normativos relacionados, independiente del cargo o función que desempeñen y la situación contractual. Cada uno es responsable de salvaguardar la información que recibe, crea o controla.

Lineamientos

Todos quienes trabajan en la CNR, están en la obligación de tomar las medidas y precauciones necesarias para proteger los registros o información de identificación personal, sin importar el soporte en que se encuentren contenidos y sus sistemas críticos en producción ante posibles daños.

A nivel de la plataforma tecnológica existente en la CNR, se garantizará la disponibilidad de la infraestructura adecuada y en operación para la realización de procesos de resguardos de registros digitales y la información contenida en ellos, asegurando que estos estén disponibles incluso después de la falla de algún control creado para tales efectos.

El tratamiento de datos personales sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas señaladas en la ley de Protección de datos Personales y Sensibles, ley 19.628.

El responsable de los registros o bases de datos donde se almacenen datos personales, con posterioridad a su recolección, deberá velar por el cuidado de ellos con la debida diligencia, haciéndose responsable de los daños que su pudieran generar.

Dada la capacidad limitada de recursos y tiempos de procesamiento de respaldos, todo registro digital a resguardar será todo aquellos que los dueños de los activos de información hayan especificado como activo de información crítico.

La CNR establecerá un plan de ejecución de respaldos de conformidad a los lineamientos señalados en la política de Respaldos de Información, que, en cumplimiento al resguardo de los registros y la información contenida en ellos, considerará los siguientes elementos:

Procedimientos de respaldos documentados y producir registros precisos y completos de las copias de respaldo en base a una programación de procesos de respaldo.

El tipo de respaldo a realizar (completo o incremental) y la frecuencia de los respaldos deberían reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la criticidad de la información para la operación continúa de la organización.

Las piezas de los respaldos realizados se almacenarán en una ubicación remota, a una distancia suficiente para evitar cualquier daño ante desastres en la ubicación principal, debiendo además tener un nivel de protección física y ambiental adecuada.

Los medios de respaldo se deberán probar de manera regular para garantizar que se puede confiar en ellos frente a su uso ante emergencias.

Instrumento de formalización

- PD-UTIC-02 Continuidad Operacional de Tecnología
- Instructivos Utic

POLÍTICA SEGURIDAD EN ESCRITORIO Y PANTALLA DESPEJADOS

La presente política declara su aplicabilidad para el control definido en la Norma NCh-ISO27.001:Of2013, más particularmente en su control:

- A-11.02.09 Política de escritorio y pantalla despejados

Declaración institucional

La presente política se enmarca dentro de la Política General de Seguridad de la información de la CNR junto con la normativa respectiva vigente y en este sentido, en la CNR 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 el alcance, lineamientos, actores, responsabilidades y los procedimientos necesarias para velar por el cumplimiento de medidas en materias relacionadas con la seguridad de escritorio y pantalla despejados a través del Sistema de Seguridad de la Información implementado en la CNR.

Objetivo de la política de escritorio y pantalla despejados

Adoptar en la CNR una política de escritorio despejado para los papeles y para los medios de almacenamiento extraíbles y una política de pantalla despejada para las instalaciones de procesamiento de información para evitar la pérdida, los daños, el robo o el compromiso de activos 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.

Alcance y/o ámbito de aplicación

El alcance de la presente política se extiende a todos los Usuarios de la CNR, ya sean funcionarios/as de planta, contrata, honorarios, asesores, consultores, practicantes y otros trabajadores, incluyendo las empresas que prestan servicios a CNR.

Responsabilidades específicas

Jefaturas de Áreas y Unidades de los respectivos centros de responsabilidad

- Velar por la adopción de la política de escritorio y pantalla despejados para evitar la pérdida, los daños, el robo o el compromiso de activos 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.
- Coordinar revisiones periódicas en el cumplimiento de esta política.

Encargado de la Infraestructura TI

- Aplicar medidas y reglas automáticas de seguridad en los equipos computacionales de los usuarios/as para que estos se mantengan desconectados o protegidos con algún mecanismo de bloqueo de pantalla y teclado mediante una contraseña u otro mecanismo de autenticación de usuario similar cuando se dejan sin supervisar y se debería proteger con bloqueos de tecla, contraseñas u otros controles cuando no está en uso.

Usuarios/as internos de CNR

- Los funcionarios/as de la CNR deben conocer la Política de Escritorio y Pantalla Despejados y los riesgos relacionados con el tratamiento de la seguridad de los activos de información entendiendo su contenido, su alcance y comprometiéndose a cumplirlas
- Los medios que contienen información sensible o clasificada se deben extraer de las impresoras inmediatamente.

Lineamientos
En la CNR se gestiona la práctica de escritorio y pantalla despejada considerando que:

- La información sensible o crítica para la CNR almacenada en medios electrónicos o papel, se mantendrá custodiada bajo llave cuando no se necesite, especialmente cuando en el lugar de almacenaje esté desocupada de personas.
- Los computadores se deberán mantener desconectados o protegidos con algún mecanismo de bloqueo de pantalla y teclado mediante una contraseña u otro mecanismo de autenticación de usuario similar cuando se dejan sin supervisar y se debería proteger con bloqueos de tecla, contraseñas u otros controles cuando no está en uso.
- En forma complementaria, para un equipo desatendido se deberá controlar el cierre de sesión y la limitación del tiempo de conexión por inactividad/consumo de energía.
- Los medios que contienen información sensible o clasificada se deberían extraer de las impresoras inmediatamente.
- Para evitar el daño en la integridad de los activos de información principalmente en aquellos disponibles en formato papel no se deberán consumir alimentos en los puestos de trabajo.

Instrumento de formalización

- Políticas específicas de seguridad de la información por dominio
- PD-UTIC-02 Continuidad Operacional de Tecnología
- Instructivos Utic

POLÍTICA RESPALDO DE LA INFORMACIÓN

La presente política declara su aplicabilidad para el control definido en la norma NCh-ISO27.001:Of2013, más particularmente en su control:

- A.12.03.01 Respaldo de la Información

Declaración institucional

La Comisión Nacional de Riego (CNR), 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, procedimientos, actores y responsables de velar por el cumplimiento en materias de respaldo de información de la institución a través de los controles dispuestos en el Sistema de Seguridad de la Información implementado en la CNR, para proteger los datos y software, así como los dispositivos digitales que lo soportan, almacenan y distribuyen.

Objetivo de la política de 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 ante riesgos que pudieran afectar la integridad y disponibilidad de los activos de información digitales existentes en la infraestructura central de la CNR, a través de mecanismos que permitan garantizar la realización de copias de seguridad y restauración de los servicios, servidores e información de la CNR.

Alcance y/o ámbito de aplicación

La presente política aplica al resguardo de la información, las configuraciones y el software oficial localizado en servidores existentes en el centro del procesamiento de datos de la CNR y aquellos disponibles y localizados en servicios Cloud contratados por la institución.

Esta política es aplicable a todos los funcionarios/as, la suplencia y el personal a honorarios que en la facultad de sus funciones le han sido asignadas las tareas de administrar la infraestructura TI existente en la CNR.

Responsabilidades específicas

Coordinador de la Unidad de Tecnología de la Información y la Comunicación (Utic)

- Garantizar la realización de respaldos de la información asegurando su proceso de recuperación considerando la implementación de soluciones de respaldo sistemas, programas, configuraciones, bases de datos e información considerada como crítica para la institución.
- Designar al personal para la administración, operación y manejo de los aspectos relativos a las operaciones de respaldo y recuperación de la información.

Encargado de la Infraestructura TI

- Definir el estándar de respaldo de los servidores y equipos de hardware, que detalle los respaldos de software básico, de las aplicaciones, configuraciones de servicios y de los datos en los ambientes de productivos, autorizar las solicitudes de respaldo especiales.
- Desarrollar y ejecutar los procedimientos/instructivos documentados para las actividades operacionales asociadas con las operaciones de Respaldo y Recuperación de la Información velando y controlando el cumplimiento de ellos.
- Realizar las configuraciones y la administración necesarias, velando por el cumplimiento de las tareas de respaldo y restauración de información.
- Deberá coordinar, ejecutar, validar y velar por la correcta realización de las pruebas y restauración de las copias de respaldo efectuadas utilizando las herramientas pertinentes para tales efectos.
- Mantener un inventario de los activos de información TI sobre los que se realiza copia de seguridad.
- Comprobar de manera regular los medios de recuperación de respaldos para garantizar que se puede confiar en ellos frente a su uso ante emergencias.

Usuarios/as internos de CNR

- Almacenar en algún servidor central de la CNR toda información institucional que es relevante para el quehacer de la CNR.

Lineamientos

En la CNR se tomarán las medidas y precauciones necesarias para proteger la información digital y sus sistemas críticos en producción ante posibles daños, por lo cual frecuentemente deberán realizarse respaldos asegurando su proceso de recuperación considerando la implementación de soluciones de respaldo para programas, bases de datos e información considerada como crítica para la institución.

A nivel de plataforma central, la CNR deberá garantizarse la disponibilidad de la infraestructura adecuada y en operación para la realización de procesos de respaldos en base a una programación de ellos, asegurando que estos estén disponibles incluso después de alguna falla de algún componente.

Toda la información institucional para respaldar será aquella cuyos registros digitales estén almacenados en algún servidor central de la CNR, por lo cual se deberán realizar la programación de copias de la información, del software y de las imágenes del sistema, garantizando su comprobación mediante procesos de restauración de manera regular.

Información que no es propia de la naturaleza y/o actividades asociadas de la Comisión Nacional de Riego y no relevante para el quehacer de la CNR o aquella que resida en las estaciones de trabajo, NO será respaldada.

En la CNR se establece un programa de ejecución de respaldos y restauración de la información, considerando los siguientes elementos:

- Procedimientos de respaldos documentados y producir registros precisos y completos de las copias de respaldo.
- El tipo de respaldo a realizar (completo o incremental) y la frecuencia de los respaldos debería reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la criticidad de la información para la operación continua de la organización.
- Las piezas de los respaldos realizados se almacenarán en una ubicación remota, a una distancia suficiente para evitar cualquier daño ante desastres en la ubicación principal, debiendo además tener un nivel de protección física y ambiental adecuada.
- Los medios de respaldo se comprobarán de manera regular para garantizar que se puede confiar en ellos frente a su uso ante emergencias o catástrofes.
- Se monitorea la ejecución de respaldos y se remediaran las fallas de ejecución de estos para garantizar su integridad de acuerdo con la política de respaldos.

En la CNR la programación de los respaldos considerará Respaldo Completo (Full Copy) acompañado de copias de respaldos incrementales diarios con una retención de a lo más mensual considerando archivar copias de seguridad en algún medio magnético externo cada dos semanas.

Terminología

Activos de Información: Todos aquel o aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.

Respaldo completo o "Full Copy": Copia directa y completa de los archivos y directorios. Este proceso puede durar horas dependiendo del tamaño de los archivos o directorios a copiar, por lo que este proceso normalmente se ejecuta la primera vez o cada cierto tiempo.

Copia de respaldo incremental: La copia incremental únicamente copia los ficheros creados o modificados desde el último respaldo de dato realizado, ya sea de una copia completa o incremental, reduciendo de este modo los archivos a copiar y el tiempo empleado en el proceso de respaldos.

Instrumento de formalización

- Políticas específicas de seguridad de la información por dominio
- PD-UTIC-02 Continuidad Operacional de Tecnología
- Instructivos Utic

POLÍTICA PROTECCIÓN CONTRA CÓDIGO MALICIOSO

La presente política declara su aplicabilidad para el control definido en la Norma NCh-ISO27.001:Of2013, más particularmente en sus controles:

- A.12.02.01 Controles contra código malicioso.
- A.12.06.02 Restricciones en la instalación de software

Declaración institucional

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 en materias de protección contra código malicioso, procedimientos, actores y responsables de velar por el cumplimiento de estas medidas de protección y los controles dispuestos a través del Sistema de Seguridad de la Información implementado en la CNR.

Objetivo de la política de 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 que pudieran atentar contra la integridad y disponibilidad de los activos de información digitales almacenados en servidores, estaciones de trabajo y cualquier otro medio magnético en uso y perteneciente a la CNR.

Alcance y/o ámbito de aplicación

La presente política aplica a la protección de información y software oficial localizado en servidores y estaciones de trabajo sean estacionarias o portátiles pertenecientes al inventario de activos y que se conecten a la red de datos de la CNR de forma local o remota.

Esta política es aplicable a todos los funcionarios/as, la suplencia y el personal a honorarios que en la facultad de sus funciones le ha sido asignado estaciones de trabajo y/o administren la infraestructura TI existente en la CNR.

Responsabilidades específicas

Coordinador de la Unidad de Tecnología de la Información y la Comunicación (Utic)

- Desarrollar los procedimientos o instructivos documentados para el control de las actividades de Protección contra Código Malicioso velando por el cumplimiento de ellos.
- Designar al personal para la administración, operación y manejo de los aspectos relativos a la Protección contra Código Malicioso.
- En el más mínimo plazo dar respuesta y solución a los incidentes o eventos de seguridad de la información que pudieran estar afectando a los activos de la información producto de la acción de código malicioso.

Encargado de la Infraestructura TI:

- Cautelar los activos de información, velando por el cumplimiento de las normativas señaladas en esta Política de Protección Contra Código Malicioso de la CNR.
- Instalar, configurar y dar soporte a la herramienta de protección contra software malicioso, manteniendo operativa y actualizada una plataforma de hardware y software de control de antivirus, phishing y firewall para la red de servidores y computadores de la CNR evitando la propagación de código malicioso, virus y sus variantes a través de redes internas y estaciones de trabajo existentes en la CNR.
- Implantar controles de detección, prevención y recuperación.
- Realizar las configuraciones necesarias para detectar, bloquear y eliminar los códigos maliciosos a partir de reglas internas propias del servidor antivirus y las implementadas en la administración del servicio de antivirus.
- Emitir reportes periódicos con los registros de análisis de vulnerabilidades y amenazas recibidas tanto en estaciones de trabajo con en la red interna de datos de la CNR.

Usuarios/as internos de CNR

- Los/as usuarios/as y dueños de los activos de información son responsables de cautelar el cumplimiento de las normativas señaladas en esta Política de Protección Contra Código Malicioso.
- Cada vez que algún usuario/a detecta actividad anormal, sospechosa o producto de alarmas locales producidas en sus estaciones de trabajo, deberán reportar el incidente en el Sistema de Servicios Generales (Mesa de Ayuda de Informática).
- Deberán abstenerse de recibir por correo y/o ejecutar programas o documentos con contenido ejecutable cuya procedencia no sea conocida o sea sospechosa, dado que pueden ser archivos que contienen virus. Asimismo, queda prohibido enviar este tipo de contenidos.
- Evitar visitar sitios y/o abrir archivos sospechosos, aunque vengan de direcciones de correo conocidas, dado que muchos virus y spyware roban direcciones de correo válidas para propagarse.
- Los funcionarios/as no están autorizados a instalar software en los computadores y notebooks de la CNR, dado que se aumentan las probabilidades de introducción de virus o spyware.
- Los funcionarios no están autorizados para descargar ni instalar software no autorizado ni aplicaciones desde Internet.

Lineamientos

En la CNR se tomarán las precauciones necesarias para proteger la red local de datos previniendo, detectando, aislando y recuperándose de la introducción de software malicioso como son Virus, Gusanos, Spyware, Código móvil, Keylogger, Ransomware, Phishing, otras variantes y bombas lógicas en las PC´s y Servidores, previniendo de esta manera que todos los activos de información digitales vigentes, en uso y relacionados con tecnología de la información tales como servidores, estaciones de trabajo y el software perteneciente a la CNR estén protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brinden protección contra código malicioso.

Toda estación de trabajo perteneciente a la CNR contará con una herramienta de protección contra software malicioso instalado y estará permanentemente actualizado (tanto en su versión de software como en su base de amenazas).

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

Protección en equipos computacionales: La(s) herramientas de seguridad instaladas en los servidores y estaciones de trabajos cumplirán con las siguientes directrices:

- Permanecerán siempre activa desde el inicio sesión del dispositivo.
- Permitirán analizar los equipos en búsqueda de amenazas.
- Permitirán realizar análisis en tiempo real en busca de amenazas provenientes de cualquier medio removible conectado al equipo (pendrive, discos externos, etc.), notificando en forma inmediata ante la detección de un código malicioso, sea notificada automáticamente.
- Permitirán la programación automática de busca de bases de nuevas amenazas, escaneo y actualización en los equipos donde se encuentra instalado.

Protección a nivel de Red de Datos (LAN): Se garantizará que la infraestructura de comunicaciones de la CNR cuente con un servicio de seguridad de antivirus y código malicioso que otorgue la protección necesaria ante amenazas, inspeccionando y controlando el tráfico de entrada y de salida para cada una de las LAN de la red. Dicho servicio permitirá:

- La generación de filtrado de contenidos y control de uso de internet.
- El análisis de tráfico.
- Controlar las aplicaciones de los usuarios.
- Protección ante correos spam.
- Detección de amenazas.
- Acceso seguro vía redes privadas virtuales VPN
- Controlar el uso de sitios web desconocidos o que se sospecha son maliciosos (es decir, la elaboración de una lista negra)

Equipos Personales: En la CNR no se permitirá que los equipos personales se conecten a la red interna de datos institucional habilitando a nivel de infraestructura TI las reglas, las configuraciones necesarias para su control y el resguardo y la protección de la información existente en CNR y los sistemas y servicios que son entregados por la institución.

El servicio de seguridad de antivirus y código malicioso que se implemente en la institución tendrá carácter de corporativo y por ende será obligatoria su instalación y uso en todo el equipamiento computacional sean estos servidores físicos, virtuales, servidores provistos por servicios Cloud contratados, estaciones de trabajo, notebooks y otros dispositivos. Cualquier equipo que no cuente con esta protección de antivirus, no podrá ser conectado a la red de datos local de la CNR. En función de las materias antes indicadas, en la CNR NO está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por la CNR

- Instalar y ejecutar programas obtenidos a través de internet, correo u otro medio, en los equipos de la Institución sin la debida autorización del Encargado de Seguridad de la Información de la CNR con la previa evaluación técnica de la Unidad de Tecnología de la Información y la Comunicación (Utic).
- Efectuar cambios en el software, en los parámetros, en la configuración o deshabilitar la(s) herramienta(s) de protección contra software malicioso.
- El uso de cualquier tipo de herramienta que impida o bloquee el normal funcionamiento de la(s) herramienta(s) de protección contra software malicioso.
- Conectar equipos a la red de datos de la CNR, que no cuenten con una herramienta de protección contra software malicioso.
- Generar, propagar, ejecutar o intentar introducir cualquier código de programación que pudiera replicarse, dañar o poner en riesgo la integridad y la disponibilidad de los equipos o la infraestructura tecnológica existente en la CNR.
- Copiar o descargar archivos de medios de almacenamiento externos (pendrive, discos duros, celulares, etc.), sin antes analizarlos con la(s) herramienta(s) de protección contra software malicioso.

Además, en la CNR la plataforma de control Antivirus y Código Malicioso cumplirá con:

- Disponer de una consola de administración y monitoreo centralizada
- Actualizar sus bases de datos de antivirus de forma permanente y centralizada.
- Permitir la distribuir las actualizaciones de forma automática en las estaciones de trabajo.
- Tener la capacidad de alto grado de detección
- No impactar en los tiempos de respuesta de las estaciones de trabajo de los usuarios/as.
- Proteger todos los computadores y servidores en uso existentes en la red de la CNR.
- Permitir realizar el análisis de búsqueda de virus y código malicioso en forma silenciosa en los equipos informáticos, evitar la propagación de estos.

Cada vez que se detecte equipamiento que se vea afectado por la presencia de código malicioso o virus cualquiera sea su variante, este equipamiento será aislado en forma inmediata de la red de datos, evitando con ello facilitar su propagación en la red interna de la CNR.
En caso de que surja un problema con virus u otro código malicioso en alguno de los equipos computacionales, deberán realizarse las operaciones para la eliminación de Código Malicioso.
Terminología:
Activos de Información: Todos aquel o aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.
Amenaza: Evento que puede desencadenar un incidente en la organización, produciendo eventualmente daños materiales, o pérdidas inmateriales en sus activos.
Disponibilidad: Garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
Evento: Una ocurrencia identificada en un sistema, servicio, o cualquier otro elemento. Es una posible brecha de cumplimiento de las políticas/normas/procedimientos o fallas en las medidas de seguridad ya implementadas.
Impacto: Efecto causado en los objetivos de la institución.
Incidente: Está indicado por un simple o múltiples eventos esperados. Esto tiene una alta probabilidad de comprometer continuidad de las operaciones de la misión institucional.
Virus: Programas maliciosos **(**malwares) que “infectan" a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior del archivo “víctima" (normalmente un ejecutable) de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y, por tanto, una nueva fuente de infección.
Gusanos: Son un subconjunto de malware. Su principal diferencia con los virus radica en que no necesitan de un archivo anfitrión para seguir vivos. Los gusanos pueden reproducirse utilizando diferentes medios de comunicación como las redes locales, el correo electrónico, los programas de mensajería instantánea, redes P2P, dispositivos USBs y las Redes sociales.
Código Móvil: Software de transferencia entre sistemas, por ejemplo, transferidas a través de una red o mediante una unidad flash USB, y ejecutado en un sistema local sin necesidad de instalación o ejecución explícita por parte del beneficiario. Ejemplos de código móvil incluyen secuencias de comandos (JavaScript, VBScript), Java applets, controles ActiveX, animaciones Flash, películas Shockwave (y Xtras), y macros incrustadas en documentos de Office.
Spyware: El spyware o software espía es una aplicación que recopila información sobre una persona u organización sin su conocimiento ni consentimiento. El objetivo más común es distribuirlo a empresas publicitarias u otras organizaciones interesadas.
Keylogger: Aplicaciones encargadas de almacenar en un archivo todo lo que el usuario ingrese por el teclado (capturadores de teclado). Son ingresados por muchos troyanos para robar contraseñas e información de los equipos en los que están instalados.
Ransomware: Es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.
Phishing: Consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza. De esta forma, el usuario cree ingresar los datos en un sitio de confianza cuando, en realidad, estos son enviados directamente al atacante.

Instrumento de formalización

- Políticas específicas de seguridad de la información por dominio
- PD-UTIC-02 Continuidad Operacional de Tecnología
- Instructivos Utic

POLÍTICA DE LA CONTINUIDAD DEL NEGOCIO

El presente ámbito de Ciberseguridad declara su aplicabilidad en las directrices y orientaciones definidas en la Norma NCh-ISO27.001 y NCh-ISO27.002, más particularmente en su control:

- A.17.01.01 Planificación de la continuidad de la seguridad de la información

Declaración institucional

La CNR requiere establecer e identificar de forma continua sus requisitos para la seguridad de la información ante situaciones adversas, es decir, durante una crisis o desastre, así como también es necesario planificar la continuidad operacional y la recuperación ante desastres a objeto de reducir el tiempo y el esfuerzo en el análisis y la recuperación ante un impacto en el negocio, en la CNR es formulada la administración de la continuidad operacional para responder y direccionar de manera controlada la gestión de incidentes, teniendo presente:

Que, los equipos, sistemas y servicios informáticos tienen un gran valor para la institución, que necesitan ser protegidos de manera apropiada, a fin de asegurar la continuidad de las operaciones, reduciendo al mínimo las consecuencias derivadas de situaciones de emergencia, incluyendo los medios de almacenamiento de información, de una manera adecuada y segura.

Que, la institución debe procurar un ambiente seguro y controlado para que los equipos informáticos puedan operar adecuadamente.

Que, la institución debe contar con un instrumento que gestione adecuadamente el buen manejo de las Tecnologías de la Información y las Comunicaciones una vez producida la emergencia, así como los recursos humanos y tecnológicos disponibles para enfrentarla.

Que, los funcionarios pertenecientes a UTIC deberán proceder según los lineamientos establecidos en dicho plan para cada situación de emergencia en particular, así como también, mejorar y/o actualizar dicho procedimiento permanentemente.

Para realizar una gestión eficiente y eficaz de la operación de los activos de CNR de los eventos tanto preventivo como reactivos, se genera este instructivo para formalizar y definir también en una compilación de procesos que permiten identificar y evaluar los riesgos potenciales que podrían interrumpir la actividad normal en la organización sirviendo para proponer las medidas oportunas a tomar para minimizar los impactos de negocio de los riesgos identificados y sometidos a evaluación. Así, con la adecuada implementación del Plan de Continuidad del Negocio podrán conseguir los siguientes objetivos: garantizar la continuidad operativa del negocio; establecer prioridades y ajustar los mecanismos de prevención, monitoreo y recuperación ante una falla o desastre; establecer una estrategia de tecnología vinculada a la estrategia de negocio para minimizar daños en caso de incidencia.

Lineamientos

En la CNR, la continuidad de la seguridad de la información se integra en los sistemas de administración de continuidad del negocio a través de la planificación de la continuidad de la seguridad en la información.

Para ello se hace necesario determinar sus requisitos para la seguridad de la información y la continuidad de la administración de la seguridad de la información ante situaciones adversas, es decir, durante una crisis y la recuperación ante desastres.

En la ausencia de una continuidad del negocio formal y una planificación de recuperación ante desastres. la administración de seguridad de la información deberá suponer que los requisitos de seguridad de la información seguirán siendo los mismos ante situaciones adversas, en comparación con las condiciones operacionales normales.

Instrumento de formalización

- Resolución Plan de Continuidad de Seguridad de la Información

POLÍTICA DE CIBERSEGURIDAD

El presente ámbito de Ciberseguridad declara su aplicabilidad en las directrices y orientaciones definidas en la Norma NCh-ISO27.001 y NCh-ISO27.002, más particularmente en sus controles:

- A-12.02.01 Controles contra código malicioso.
- A-12.04.01 Registro de evento
- A-12.04.03 Registros del administrador y el operador
- 8.8 Gestión de vulnerabilidades técnicas *(ISO 27002:2022)*

(A-12.06.01 Gestión de las vulnerabilidades técnicas)

- A-12.06.02 Restricciones en la instalación de software
- A-12.01.04 Separación de entornos de desarrollo, pruebas y operacionales
- A-13.01.02 Seguridad de los servicios de red
- A-14.02.02 Procedimientos de control de cambios
- A-14.02.05 Principios de ingeniería de sistema seguro
- A-14.02.08 Prueba de seguridad del sistema
- A-14.02.09 Prueba de aprobación del sistema
- 8.11 Enmascaramiento de datos (ISO 27002:2022)
- A-16.01.05 Respuesta ante incidentes de seguridad de la información

La masificación en el uso de tecnologías de información y comunicaciones (TIC), junto con servir al desarrollo del país, conlleva riesgos que pueden provenir de múltiples fuentes afectando la seguridad pública, los servicios críticos y los derechos de las personas (actividades de espionaje, sabotaje, fraudes, ciberataques, entre otros), lo que es posible constatar la considerable evolución doctrinaria, técnica y normativa en los más diversos organismos y foros internacionales.

Por lo anterior es de vital importancia la adopción de los lineamientos y directrices señalados en la Política Nacional de Ciberseguridad, los cuales orientan las acciones del país en materia de ciberseguridad, junto con implementar y poner en marcha las medidas que sean necesarias para proteger la seguridad de los usuarios del ciberespacio, considerando estrategias educativas orientadas al autocuidado y prevención en ambiente digital, cumpliendo además con el programa de Gobierno, que propone “desarrollar una estrategia de seguridad digital que proteja a los usuarios privados y públicos”. para alcanzar el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente.

Lineamientos

En la CNR se desarrollan las 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.

Para favorecer el buen cumplimiento de requisitos de seguridad, en la CNR se da a conocer e implementan medidas de prevención conducentes a aumentar los niveles de seguridad de los Servicios Tecnológicos existentes con el objetivo de disminuir los riesgos de Ciberseguridad.

Lo anterior, previniendo un eventual incremento de acciones que pudieran afectar y comprometer a las redes, plataformas, sistemas informáticos y servicios que la CNR pone a disposición de la ciudadanía y sus funcionarios, resulta vital y urgente adoptar las medidas necesarias para asegurar la continuidad de dichos servicios.

Además, se obtiene información sobre las vulnerabilidades técnicas de los sistemas de información en uso y se evalúa la exposición de la organización a tales vulnerabilidades para tomar las medidas apropiadas y para prevenir la explotación de vulnerabilidades técnicas.

Dichas medidas permiten la incorporación de buenas prácticas en el uso de los servicios tecnológicos institucionales (web, redes, PC, Notebook, entre otros) garantizando el resguardo y la protección de los activos de información de la CNR. Las medidas que implementan son las siguientes:

- Se habilita un control que restringirá la instalación de software por parte de los funcionarios. Solo los administradores en UTIC podrán instalar software permitidos.
- Los softwares autorizados son todos aquellos que poseen una licencia vigente y adquiridas por CNR.
- En la pantalla principal no habrá documentos o carpetas para lograr dar cumplimiento a la Política Seguridad de Información en la CNR, Escritorio Limpio.
- Las carpetas compartidas estarán disponibles únicamente en Google Drive (Google WorkSpace).
- Se habilitarán mecanismos para fortalecer las contraseñas de acceso a la red cada 90 días y así dar cumplimiento con la normativa vigente, que solicita claves "robustas".
- Bloqueo de pantalla por inactividad cada 30 minutos, solicitando contraseñas para la reanudación de la sesión.
- Computadores y equipos se apagan de forma automática después de las 21:00 hrs.
- Todo equipo tecnológico que se conecte a la red institucional deberá cumplir con las Políticas de Seguridad de Información e ingresar con usuario y clave.
- Serán eliminados automáticamente los archivos localizados en la papelera cada 30 días.

- Se habilitará el Bloqueo de software no permitidos y las conexiones vía acceso remoto no autorizadas.
- Se sensibiliza respecto de los riesgos de uso de pendrive, equipos telefónicos y otros dispositivos móviles conectados a puertos USB durante 60 días, y luego, se restringirá el uso de estos.
- Se restringirá el tiempo máximo de conexión de las WIFI de visitas.
- La navegación web tendrá como página de inicio la Intranet de CNR.
- En el escritorio estará disponible como acceso directo la intranet institucional la que contiene los accesos a servicios como Mesa de Servicios (SSG), SEP, CEROPAPEL, Portal CNR, Autoconsulta. entre otros.

Todas estas medidas y buenas prácticas serán aplicadas con el objetivo de minimizar los riesgos de fallas o pérdida de los activos de información de la CNR.

Gestión de Vulnerabilidades técnicas (ISO 27002:2022 – Ctrl. 8.8)

La CNR debe contar con un inventario preciso de activos el que incluye el proveedor de software, nombre del software, números de versión, estado actual de implementación y la(s) persona(s) dentro de la organización responsable del software.

Para identificar vulnerabilidades técnicas, la CNR considera definir y establecer los roles y responsabilidades asociados a la vulnerabilidad técnicas, incluido el seguimiento de la vulnerabilidad, la evaluación del riesgo de la vulnerabilidad, la actualización, el seguimiento y cualquier responsabilidad de coordinación requerida;

Los Administradores de los Sistemas de Información y Servicios digitales deberán exigir a los proveedores de los sistemas de información (incluidos sus componentes) y servicios que aseguren la remediación de vulnerabilidades incluidos los requisitos en los contratos aplicables.

Se podrán utilizar herramientas de escaneo de vulnerabilidades adecuadas para las tecnologías en uso para identificar vulnerabilidades y para verificar si el parcheo de vulnerabilidades fue exitoso.

Se podrá rastrear el uso de bibliotecas de terceros y código fuente en busca de vulnerabilidades.

Dependiendo de la urgencia con la que se deba abordar una vulnerabilidad técnica, se debe gestionar la acción de acuerdo con los controles relacionados con la gestión de respuesta a incidentes de seguridad.

Se deberán utilizar únicamente actualizaciones de fuentes legítimas, además de probar y evaluar antes de instalarlas para garantizar que sean efectivas y no resultar en efectos secundarios que no se pueden tolerar.

Se debe mantener un registro de auditoría para todos los pasos realizados en la gestión de remediación de vulnerabilidades técnicas.

Enmascaramiento de datos (ISO 27002:2022 – Ctrl. 8.11)

En la CNR se deben limitar la exposición de datos confidenciales para cumplir con las normas legales, estatutarias, reglamentarias y los requisitos contractuales.

Cuando la protección de datos confidenciales es una preocupación, la CNR debe considerar ocultar dichos datos mediante el uso de técnicas como el enmascaramiento de datos, el enmascaramiento o la anonimización.

Las técnicas de enmascaramiento o anonimización pueden ocultar o disfrazar la verdadera identidad u otra información confidencial resguardando información sensible.

Cuando se utilicen técnicas de enmascaramiento o anonimización, se debe verificar que los datos hayan sido adecuadamente enmascaramiento o anonimizados.

La anonimización de datos debe considerar todos los elementos de la información sensible para que sea eficaz.

Las técnicas adicionales para el enmascaramiento de datos incluyen:

a) Encriptación (que requiere que los usuarios autorizados tengan una clave).
b) Anular o eliminar caracteres (evitar que los usuarios no autorizados vean los mensajes completos).
c) Números y fechas variables.
d) Sustitución (cambiar un valor por otro para ocultar datos sensibles).
e) Reemplazar valores con su hash.

Se debe considerar lo siguiente al implementar técnicas de enmascaramiento de datos:

a) No otorgar a todos los usuarios acceso a todos los datos, por lo tanto, se deben diseñar consultas y máscaras para mostrar solo los datos mínimos requeridos al usuario.
b) Hay casos en los que algunos datos no deberían ser visibles para el usuario para algunos registros de un conjunto de datos; en este caso, se debe diseñar e implementar un mecanismo de ofuscación de datos.
c) Cualquier requisito legal o reglamentario.

Se debe tener en cuenta lo siguiente al utilizar el enmascaramiento de datos:

a) Nivel de fuerza del enmascaramiento de datos, enmascaramiento o anonimización de acuerdo con el uso de los datos procesados.
b) Controles de acceso a los datos procesados.
c) Acuerdos o restricciones en el uso de los datos procesados.
d) Hacer un seguimiento del suministro y la recepción de los datos procesados.

Prevención de fuga de datos (ISO 27002:2022 – Ctrl. 8.12).

En la CNR, las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y cualquier otro dispositivo que procesar, almacenar o transmitir información sensible para detectar y prevenir la divulgación y extracción no autorizada de información por parte de individuos o sistemas.

Se deberá considerar lo siguiente para reducir el riesgo de fuga de datos:

a) Identificar y clasificar la información para protegerla contra fugas (por ejemplo, información personal, modelos de precios y diseños de productos).
b) Canales de monitoreo de fuga de datos (por ejemplo, correo electrónico, transferencias de archivos, dispositivos móviles y almacenamiento dispositivos portátiles.
c) Actuar para evitar que se filtre información (p. ej., correos electrónicos en cuarentena).

Las herramientas de prevención de fuga de datos deben utilizarse para:

a) Identificar y controlar la información sensible en riesgo de divulgación no autorizada (por ejemplo, en datos en el sistema de un usuario).
b) Detectar la divulgación de información confidencial (por ejemplo, cuando la información se carga en servicios en la nube de terceros o enviados por correo electrónico);
c) Bloquear las acciones de los usuarios o las transmisiones de la red que expongan información confidencial (Por ejemplo, copia de las entradas de la base de datos en una hoja de cálculo)

La CNR debe determinar si es necesario restringir la capacidad de un usuario para copiar y pegar o cargar datos a servicios, dispositivos y medios de almacenamiento fuera de la organización, si ese es el caso, la organización debe implementar tecnología como herramientas de prevención de fuga de datos o la configuración de herramientas existentes que permiten a los usuarios ver y manipular datos almacenados de forma remota pero evitan copiar y pegar fuera del control de la organización.

Si se requiere la exportación de datos, se requerirá que el propietario de los datos apruebe la exportación y retenga a los usuarios responsable de sus actos.

Cuando se realiza una copia de seguridad de los datos, se debe tener cuidado para garantizar que la información confidencial esté protegida mediante medidas como el cifrado, el control de acceso y la protección física de los medios de almacenamiento que contienen los respaldos.

También se debe considerar la prevención de fugas de datos para proteger contra las acciones de inteligencia de un adversario obtenga información confidencial o secreta que puede ser de interés para el espionaje o puede ser crítico para la comunidad.

Gestión de eventos (Log) (ISO 27002:2022 – Ctrl.8.15)

Con el objetivo de registrar y recopilar eventos, generar y conservar evidencia, asegurar la integridad de la información de registro, prevenir contra acceso no autorizado, identificar eventos de seguridad de la información que pueden conducir a un incidente de seguridad de la información y para apoyar las investigaciones, en la CRN se deben producir, almacenar y almacenar registros que registren actividades, excepciones, fallas, errores y otros eventos para ser analizados.

Es importante que todos los sistemas tengan fuentes de tiempo sincronizadas

Los registros de eventos deben incluir para cada evento, según corresponda:

a) ID de usuario.
b) Actividades del sistema.
c) Fechas, horas y detalles de eventos relevantes (por ejemplo, inicio y cierre de sesión).
d) Identidad del dispositivo, identificador del sistema y ubicación.
e) Direcciones de red y protocolos.

Los siguientes eventos deben ser considerados para el registro:

a) Intentos de acceso al sistema exitosos y rechazados.
b) Datos exitosos y rechazados y otros intentos de acceso a recursos.
c) Cambios en la configuración del sistema.
d) Uso de privilegios.
e) Uso de programas de utilidad y aplicaciones.
f) Los archivos a los que se accedió y el tipo de acceso, incluida la eliminación de archivos de datos importantes.
g) Alarmas generadas por el sistema de control de acceso.
h) Activación y desactivación de sistemas de seguridad, como sistemas antivirus y detección de intrusos sistemas u otros.
i) Creación, modificación o eliminación de identidad.
j) Transacciones ejecutadas por los usuarios en las aplicaciones.

Protección de registros
Los usuarios, incluidos aquellos con derechos de acceso privilegiados, no deben tener permiso para eliminar o desactivar registros de sus propias actividades ya que potencialmente pueden manipular los registros en el procesamiento de la información,
instalaciones bajo su control directo, por lo tanto, es necesario proteger y revisar los registros para mantener responsabilidad de los usuarios privilegiados.
Se habilitarán controles que apunten a la protección contra cambios no autorizados en la información incluidos:
a) Alteraciones en los tipos de mensajes que se registran.
b) Archivos de registro que se editan o eliminan.
c) Fallas en el registro de eventos o sobreescritura de eventos pasados registrados si el medio de almacenamiento mantiene un registro archivo se ha excedido.
Para la protección de los registros, se debe considerar el uso de las siguientes técnicas: hashing criptográfico, grabación en un archivo de solo anexar y de solo lectura, grabación en un archivo de transparencia pública. Para lo cual se deberá disponer de una forma segura de las credenciales de acceso necesarias ante un proceso de auditoría o investigación .
Dado que los registros de eventos pueden contener datos confidenciales e información de identificación personal, se deben tomar medidas de protección a la privacidad, sobre todo cuando se comparte o envíen registros del sistema o de la aplicación a un proveedor para ayudar con la depuración o errores de resolución de problemas, los registros de log se deberán desidentificar utilizando técnicas de enmascaramiento de datos para evitar visibilizar por ejemplo nombres de usuario, direcciones IP, nombres de host u organización nombre, antes de enviar al proveedor.
Análisis de registros
En la CNR debe proveerse de algún mecanismo para cubrir el análisis y la interpretación de los eventos de seguridad de la información, para ayudar a identificar actividad inusual o comportamiento anómalo, que pueden representar indicadores de compromiso o comportamiento anómalo, que incluye:
a) Revisar los intentos exitosos y fallidos de acceder a los recursos protegidos.
b) Verificar los registros de DNS para identificar conexiones de red salientes a servidores maliciosos, como los asociados con servidores de comando y control de botnet.
c) Examinar los informes de uso de los proveedores de servicios en busca de actividad dentro de sistemas y redes (por ejemplo, mediante la revisión de patrones de actividad).
d) Incluir registros de eventos de monitoreo físico como entrada y salida para garantizar una mayor precisión detección y análisis de incidentes.
e) Correlación de registros para permitir un análisis eficiente y altamente preciso.
Deben identificarse los incidentes de seguridad de la información supuestos y reales (por ejemplo, infección de malware o sondeo de cortafuegos) y estar sujeto a una mayor investigación (por ejemplo, como parte de una seguridad de la información proceso de gestión de incidentes).
Filtrado Web (ISO 27002:2022 – Ctrl.8.23)
Con el objetivo de proteger los sistemas contra el malware y evitar el acceso a sitios web no autorizados, en la CNR, el acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso y reducir los riesgos de que sus funcionarios/as accedan a sitios web que contengan información ilegal o se sabe que contienen virus, phishing u otro material malicioso.
Esta protección podrá ser llevada a cabo generando los bloqueos necesarios como direcciones IP, dominios de los sitios web en cuestión, aplicación de reglas de acceso o bien con el apoyo de herramientas y tecnología de inteligencia de amenazas que hacen esto automáticamente o pueden configurarse para hacerlo.
El filtrado web puede incluir una variedad de técnicas que incluyen firmas, heurística, lista de aceptables sitios web o dominios, lista de sitios web o dominios prohibidos y configuración personalizada para ayudar a prevenir software malicioso y otras actividades maliciosas que podrían atacar o comprometer la red, las plataformas tecnológicas, los datos o los sistemas existentes en la CNR.
La CNR debe identificar los tipos de sitios web a los que sus funcionarios deben o no tener acceso, debiendo considerar bloquear el acceso a los siguientes tipos de sitios web:
a) Sitios web que tienen una función de carga de información a menos que esté permitido por razones válidas propias de la institución, las que estará debidamente autorizadas.
b) Sitios web maliciosos conocidos o sospechosos (por ejemplo, aquellos que distribuyen malware o contenido de phishing).
c) Servidores de mando y control.
d) Sitios web maliciosos detectados por sistemas de inteligencia de amenazas.
e) Sitios web que comparten contenido ilegal.
La implementación de este control requerirá establecer reglas para un uso seguro y apropiado de recursos en línea, incluida cualquier restricción a sitios web no deseados o inapropiados y aplicaciones Las reglas deben mantenerse actualizadas.
Se debe capacitar a los funcionarios sobre el uso seguro y apropiado de los recursos en línea, incluidos acceso a la red.
La capacitación debe incluir las reglas de la organización, el punto de contacto para atender inquietudes y procesos de excepción cuando se necesita acceder a recursos web restringidos para fines legítimos.

También se debe capacitar al personal para garantizar que no anulen ningún aviso del navegador que informa que un sitio web no es seguro, pero permite que el usuario continúe.
Instrumento de formalización

- Políticas específicas de seguridad de la información por dominio
- PD-UTIC-01 Desarrollo de Módulos de Software
- PD-UTIC-02 Continuidad Operacional de Tecnología
- Instructivos Utic

PROTOCOLO DE SEGURIDAD PARA EL TRABAJO DISTANCIA

El presente ámbito de Seguridad declara su aplicabilidad en las directrices y orientaciones definidas en la Norma NCh-ISO27.001, NCh-ISO27.002 y ISO 27.002:2022 , más particularmente en su control:

- 6.7 Trabajo Remoto (ISO 27002:2022)
  (A-6.02.02 Teletrabajo)

El trabajo a distancia representa un desafío único, especialmente en circunstancias adversas que demandan la continuidad operativa de los servicios públicos. Este ofrece muchas ventajas, pero no está libre de riesgos de seguridad debido a que no existe un medio ambiente libre de estas amenazas, por lo cual realizar un trabajo remoto seguro significa que debemos tomar algunas medidas para reforzar la seguridad.
Por tal motivo, la CNR elabora el presente protocolo en el que se entregan algunas recomendaciones para que la información que se transmite al realizar un trabajo remoto pueda desarrollarse de la manera más segura posible.
Se entenderá por modalidad de trabajo a distancia aquel pacto que faculta al funcionario a prestar sus servicios total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos por la institución.
Se entenderá por teletrabajo cuando los servicios sean prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones o bien cuando los servicios prestados deban reportarse mediante tales medios.
En función de lo anterior, en la CNR se promueven e instan para los usuarios recomendaciones generales de buenas prácticas sobre esta materia, en todo momento, incluyendo, aquellos momentos de excepción o emergencia, representados en nuestro país por desastres naturales como terremotos tsunamis, fenómenos volcánicos o incendios, u otros fenómenos que pueden afectar la continuidad de los servicios públicos, como procesos de conmoción social, epidemia y pandemia.
Esto quiere decir que una institución debe seguir funcionando a pesar del desastre natural o de la emergencia de salud pública que esté ocurriendo, priorizando y manteniendo un mínimo de medidas fundamentales respecto de los estándares y requisitos de seguridad de la información, implementan medidas que apoyan la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de trabajo a distancia y aquellas que permitan resguardar la información, los sitios y sistemas institucionales.
Para ello en la CNR se hace hincapié en el uso de VPN (Red privada virtual por sus siglas en inglés) en los casos que sea justificado su uso, así como también sus consideraciones de uso y disponibilidad de las VPN las que son tomadas en cuenta por los equipos técnicos de la Unidad Utic quienes habilitan y administrar este servicio de comunicación segura.

Protocolo de seguridad para trabajo a distancia

En la CNR y con la debida autorización de las autoridades las áreas podrán identificar labores que puedan ser realizadas vía trabajo a distancia.
Lo anterior podrá solucionarse coordinando esquemas híbridos de horarios considerando que los principales procesos que debieran abordarse bajo el esquema planteado, con el objetivo de preservar su continuidad, son aquellos críticos, y que en lo posible tengan relación con aquellos productos estratégicos considerados el en formulario A1 de la DIPRES.
Dependiendo de la emergencia también se deben tener en cuenta criterios de priorización, entre los cuales se pueden mencionar: los grupos de riesgo según rango etario, distancias de domicilio respecto de las instalaciones institucionales, nivel de conflictividad en los lugares de traslado de los funcionarios, entre otras variables a definir siempre que estén vinculadas a los procesos y labores críticas o respondan a una política pública mayor.

Directrices y Recomendaciones para trabajar a distancia

En la CNR se implementan medidas de seguridad cuando el personal trabaja de forma remota para proteger la información, el acceso, el procesamiento o almacenamiento fuera de las instalaciones de la organización, garantizando la seguridad de la información cuando el personal trabaja de forma remota.
Además, se establecen recomendaciones para que el ambiente de trabajo remoto pueda replicar las condiciones mínimas de seguridad que ofrece la oficina, las que se indican a continuación:
a) La seguridad física existente o propuesta del lugar de trabajo remoto, teniendo en cuenta la seguridad física del lugar y del entorno local, incluidas las diferentes jurisdicciones dónde se encuentra el personal.
b) Los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas de la organización, la sensibilidad de la información a ser accedida y pasada a través de la enlace de comunicación y la sensibilidad de los sistemas y aplicaciones.
c) El uso de acceso remoto, como acceso vía Red Privada Virtual (VPN).
d) Vigilancia a la amenaza de acceso no autorizado a información o recursos de otras personas en el control remoto lugar de trabajo (por ejemplo, familia y amigos).
e) La amenaza de acceso no autorizado a información o recursos de otras personas en lugares públicos.
f) El uso de redes domiciliarias y redes públicas, y requisitos o restricciones a la configuración de servicios de redes inalámbricas.
g Uso de medidas de seguridad, como firewalls y protección contra malware.
h) Mecanismos seguros para implementar e inicializar sistemas de forma remota.
Las directrices y medidas a considerar:
a) La provisión de equipos y muebles de almacenamiento adecuados para las actividades de trabajo a distancia, cuando el uso de equipo de propiedad privada que no está bajo el control de la organización no está autorizado.
b) La provisión de capacitación para quienes trabajan a distancia y quienes brindan apoyo. Esto debería incluir cómo realizar actividades de manera segura mientras se trabaja de forma remota.
c) La provisión de equipos de comunicación adecuados, incluidos métodos para asegurar el acceso remoto, como requisitos sobre bloqueos de pantalla de dispositivos y temporizadores de inactividad; la habilitación de la ubicación del dispositivo seguimiento; instalación de capacidades de borrado remoto.
d) La provisión de soporte y mantenimiento de hardware y software;
e) Los procedimientos de respaldo y continuidad del negocio;
f) Revocación de autorización y derechos de acceso y devolución de equipos cuando el trabajo a distancia se da por terminadas las actividades.

Respecto a los usuarios de los sistemas

- Deben evitar conectarse a internet desde Wi-Fi público a la red institucional.
- Reforzar a los usuarios permanecer alerta respecto a correos electrónicos fraudulentos y ante cualquier duda o sospecha del funcionario sobre una amenaza, Phishing o malware, este deberá contactarse vía el Sistema de Servicios Generales solicitando soporte al respecto.
- Recalcar a los funcionarios las políticas de seguridad de información interna, como uso de los dispositivos móviles, uso de los equipos personales, borrado de datos y documentación confidencial, así como la política de escritorio limpio.
- Si se utiliza un equipo compartido en el hogar, el funcionario deberá crear un perfil nuevo específico para realizar los trabajos relacionados con la Institución.
- Los equipos con conexión remota fuera de la oficina deberán contener softwares y sistema operativo actualizados.
- Tener equipos de conexión remota fuera de la oficina con software antivirus.

Orientación Institucional

- Utilizar una conexión VPN ya que, a través de ella, se establece una conexión remota segura (encriptada) a la red institucional.
- Velar por la seguridad física existente del sitio de trabajo a distancia, considerando la seguridad física del edificio y del entorno local.
- Establecer canales de comunicación oficiales para la comunicación del equipo de trabajo y jefatura.
- Evitar instalar software corporativo en equipos personales. Se recomienda instalarlos en equipos institucionales o ingresar a través de escritorio remoto por VPN.
- Utilizar equipos institucionales con los resguardos de seguridad correspondientes. De no ser posible, el usuario deberá utilizar su equipo personal y, en conjunto con la institución, deberá verificar que su dispositivo se encuentre en condiciones de seguridad aptas: antivirus reconocido y actualizado, sistema operativo debidamente licenciado y con sus parches al día, y aplicaciones debidamente licenciadas y actualizadas.
- Advertir a los funcionarios que los equipos institucionales y personales utilizados para trabajar de forma remota son susceptibles a auditoría.
- Establecer medidas para evitar el acceso de forma fortuita a información institucional por otros usuarios del equipo del funcionario, como familiares o amigos, limitando el acceso a los recursos estrictamente necesarios
- Utilizar servicios de videoconferencia con niveles de seguridad alto para la sustitución de reuniones presenciales.
- Aplicar la lógica de respaldo de la información en este nuevo escenario.
- Establecer medidas de seguridad como doble factor de autenticación tanto en el correo institucional como en las plataformas que se utilizan para trabajar.
- Verificar los accesos a sistemas o plataformas según el rol que posea cada trabajador.
- Aplicar política de seguridad para la conexión de forma segura de proveedores
- y externos.
- Evaluar la implementación de cifrado de discos en equipos institucionales que se disponibiliza para el trabajo a distancia.
- El material relacionado con la institución generado en la modalidad de trabajo a distancia será de propiedad intelectual de la CNR.
- Establecer requisitos de protección de malware y reglas de firewall (cortafuegos).
- -Establecer una definición del trabajo permitido, las horas de trabajo, la clasificación de información que se puede tener y los sistemas y servicios internos a los que está autoriza el teletrabajador.
- Establecer la revocación de autoridad y derechos de acceso y la devolución de los equipos cuando concluyen las actividades de trabajo a distancia.

- Las conexiones VPN deberán ser restringidas, se recomienda conexión VPN sólo a accesos locales de la institución, sin conexión a internet remota.
- De requerir internet, se recomienda utilizar el mismo túnel VPN y en el caso de necesitar múltiples VPN, se recomienda conexión VPN personalizadas para solo acceder a tomar control remoto del equipo asignado al interior de la institución y utilizar los permisos de acceso ya asignados a dicho equipo.

Esta modalidad de trabajo podrá ser establecida por el Jefe de Servicio a través de la respectiva resolución exenta, dictada para el efecto y fundada en la recomendación presidencial de fomento del trabajo a distancia.
Se deben implementar medidas de seguridad cuando el personal trabaja de forma remota para proteger la información.
accedido, procesado o almacenado fuera de las instalaciones de la organización.

Objetivo

Garantizar la seguridad de la información cuando el personal trabaja de forma remota.

Guía

El trabajo remoto ocurre cuando el personal de la organización trabaja desde una ubicación fuera de las instalaciones de la organización, accediendo a la información ya sea en papel o electrónicamente a través de las TIC equipo. Los entornos de trabajo remoto incluyen los denominados "teletrabajo", "teletrabajo", “lugar de trabajo flexible”, “entornos de trabajo virtuales” y “mantenimiento remoto”.
NOTA: es posible que no todas las recomendaciones de esta guía se puedan aplicar debido a la legislación local y regulaciones en diferentes jurisdicciones,
Las organizaciones que permiten actividades de trabajo remoto deben emitir un tema: política específica sobre el trabajo remoto de trabajo que define las condiciones y restricciones pertinentes. Cuando se considere aplicable, lo siguiente deben tenerse en cuenta los asuntos:
a) la seguridad física existente o propuesta del lugar de trabajo remoto, teniendo en cuenta la seguridad física del lugar y del entorno local, incluidas las diferentes jurisdicciones dónde se encuentra el personal.
b) reglas y mecanismos de seguridad para el entorno físico remoto, como el archivo bajo llave gabinetes, transporte seguro entre ubicaciones y reglas para acceso remoto, escritorio despejado, impresión y disposición de información y otros activos asociados, y reporte de eventos de seguridad de la información.
c) los entornos físicos de trabajo remoto esperados;
d) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas de la organización, la sensibilidad de la información a ser accedida a través de la enlace de comunicación y la sensibilidad de los sistemas y aplicaciones.
e) el uso de acceso remoto, como acceso de escritorio virtual que admita el procesamiento y almacenamiento de información sobre equipos de propiedad privada.
f) la amenaza de acceso no autorizado a información o recursos de otras personas en el control remoto lugar de trabajo (por ejemplo, familia y amigos).
g) la amenaza de acceso no autorizado a información o recursos de otras personas en lugares públicos.
h) el uso de redes domiciliarias y redes públicas, y requisitos o restricciones a la configuración de servicios de redes inalámbricas.
i) uso de medidas de seguridad, como firewalls y protección contra malware.
j) mecanismos seguros para implementar e inicializar sistemas de forma remota.
k) mecanismos seguros de autenticación y habilitación de privilegios de acceso teniendo en consideración la vulnerabilidad de los mecanismos de autenticación de un solo factor donde el acceso remoto a la red de la organización está permitido.
Las directrices y medidas a considerar deben incluir:
a) la provisión de equipos y muebles de almacenamiento adecuados para las actividades de trabajo a distancia, cuando el uso de equipo de propiedad privada que no está bajo el control de la organización no está permitió.
b) una definición del trabajo permitido, la clasificación de la información que puede ser mantenida y la interna sistemas y servicios a los que el trabajador remoto está autorizado a acceder.
c) la provisión de capacitación para quienes trabajan a distancia y quienes brindan apoyo. Esto debería incluir cómo realizar negocios de manera segura mientras se trabaja de forma remota.
d) la provisión de equipos de comunicación adecuados, incluidos métodos para asegurar el acceso remoto, como requisitos sobre bloqueos de pantalla de dispositivos y temporizadores de inactividad; la habilitación de la ubicación del dispositivo seguimiento; instalación de capacidades de borrado remoto.
e) seguridad física.
f) reglas y orientación sobre el acceso de familiares y visitantes a equipos e información.
g) la provisión de soporte y mantenimiento de hardware y software.
h) la provisión de seguros.
i) los procedimientos de respaldo y continuidad del negocio.
j) auditoría y seguimiento de la seguridad.
k) revocación de autorización y derechos de acceso y devolución de los equipos cuando en el trabajo a distancia se dan por terminadas las actividades.

Instrumento de formalización

- Resol.Política SSI
- Políticas específicas de seguridad de la información por dominio
- PD-UTIC-02 Continuidad Operacional de Tecnología
- Instructivos Utic

DOCUMENTOS RELACIONADOS CON LAS POLÍTICAS

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.
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: 2018 Tecnologías de la Información - Técnicas de seguridad - Sistemas de Gestión de la seguridad de la información
Norma Nch ISO 27001:2013 Tecnologías de la Información - Técnicas de seguridad - Sistemas de Gestión de la seguridad de la información - Requisitos.
Norma Nch ISO 27002:2013 Tecnologías de la Información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información.
Norma NCh ISO 9.001, que especifica 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.
Política General de Seguridad de la Información de la Comisión Nacional de Riego
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.

CATÁLOGO DE CONTROLES ASOCIADOS

Dominio: **POLÍTICAS DE SEGURIDAD DE LA iNFORMACIÓN**	**Responsable Implementación**	**Instrumento de formalización**
A.05.01.01 Políticas para la Seguridad de la Información	Encargado SSI	Resol.Política SSI
A.05.01.02 Revisión de las políticas de seguridad de la información	Encargado SSI	
Dominio: **ORGANIZACIÓN DE LA SEGURIDAD DE LA Información**		
A.06.01.01 Roles y responsabilidades de la seguridad de la información	Encargado SSI	
A.06.01.02 Segregación de funciones	Encargado SSI G. Personas	Resol.Política General SSI
A.06.01.03 Contacto con autoridades	Coordinador Adm.	Políticas específicas de seguridad de la información por dominio
A.06.01.04 Contacto con grupos de interés especiales	Encargado SSI	
6.7 Trabajo Remoto *(ISO 27002:2022)*	Coordinador Utic	
Dominio: **SEGURIDAD DE RECURSOS HUMANOS**		
A.07.01.01 Selección	Coordinador G.Personas	Políticas específicas de seguridad de la información por dominio PD-GP-01 Selección, Contratación e Inducción
A.07.02.02 Concientización, educación y capacitación sobre la seguridad de la información	Encargado SSI	
Dominio: **ADMINISTRACIÓN DE ACTIVOS**		
5.9 Inventario de Activos de Información *(ISO 27002:2022)*	Representantes Comité Gestión	Políticas específicas de seguridad de la información por dominio Matriz de Activos de la Información actualizado Manual de Activo Fijo
5.10 Uso aceptable de la información y otros activos asociados (ISO 27002:2022)		
5.12 Clasificación de la Información *(ISO 27002:2022)*		
A.08.01.04 Devolución de activos	Coordinador Adm.	
A.08.03.02 Eliminación de medios	Coordinador Utic	
Dominio: **CONTROL DE ACCESO**		
A.09.01.01 Política de control del acceso	Encargado SSI	
A.09.01.02 Acceso a redes y servicios de red	Coordinador Utic	Políticas específicas de seguridad de la información por dominio PD-UTIC-02 Continuidad Operacional de Tecnología Instructivos Utic
5.16 Administración de identidades *(ISO 27002:2022)*		
A.09.02.03 Gestión de derechos de acceso privilegiados		
A.09.04.01 Restricción de acceso a la información		
A.09.04.02 Procedimiento de inicio de sesión seguro		
5.17 Autenticación de información *(ISO 27002:2022)*		
A.09.04.04 Uso de programas de utilidad privilegiado		
Dominio: **SEGURIDAD FISICA y AMBIENTAL**		
A.11.01.01 Perímetro de seguridad física	Coordinador Adm.	Políticas específicas de seguridad de la información por dominio PD-UTIC-02 Continuidad Operacional de Tecnología
A.11.01.02 Controles de entrada física		
A.11.01.04 Protección contra las amenazas externas y ambientales		
A.11.02.01 Ubicación y Protección del equipamiento	Coordinador Utic	
A.11.02.02 Servicios básicos de apoyo	Coordinador Adm.	
A.11.02.04 Mantenimiento del equipamiento	Coordinador Utic	

A.11.02.05 Retiro de activos	Coordinador Adm.	Instructivos Utic PD-ADM-02 Administración Activo Fijo PD-SSI-02 Seguridad Física y Entorno
7.9 Seguridad de los activos fuera de las instalaciones *(ISO27001:2022*	Coordinador Utic	
A.11.02.7 Eliminación o reutilización segura de equipos	Coordinador Utic	
A.11.02.08 Equipo del usuario desatendido	Coordinador Utic	
A.11.02.09 Política de escritorio y pantalla limpios	Encargado SSI	
Dominio: **SEGURIDAD DE LAS OPERACIONES**		
A.12.01.01 Procedimientos de operación documentados	Coordinador Utic	Políticas específicas de seguridad de la información por dominio PD-UTIC-01 Desarrollo de Módulos de Software PD-UTIC-02 Continuidad Operacional de Tecnología Instructivos Utic
A.12.01.02 Administración de cambios		
A.12.01.04 Separación de entornos de desarrollo, pruebas y operacionales		
A.12.02.01 Controles contra Malware		
A.12.03.01 Respaldo de la información		
A.12.04.01 Registros de Evento		
A.12.04.03 Registros del administrador y el operador		
A.12.04.04 Sincronización de relojes		
A.12.05.01 Instalación del software en sistemas operacionales		
A.12.06.02 Restricciones en la instalación de software		
8.8 Gestión de vulnerabilidades técnicas *(ISO 27002:2022)*	Coordinador Utic Administradores de los Sistemas de Información y Servicios digitales Encargado SSI	Remediación de vulnerabilidades Gestión de remediación con proveedores y partes interesadas Informe gestión vulnerabilidades técnicas
8.12 Prevención de fuga de datos *(ISO 27002:2022)*	Coordinador Utic	Habilitación de controles DLP (Data Loss Prevention) Monitoreo de fuga de datos
8.15 Gestión de eventos (Log) *(ISO 27002:2022)*		Informes de revisión de eventos (logs)
8.23 Filtrado Web		Evidencias de reglas y configuraciones habilitadas para el filtrado web. Capacitación a los funcionarios sobre el uso seguro y apropiado de los recursos en línea, incluidos acceso a la red y navegación.
Dominio: **SEGURIDAD EN LAS COMUNICACIONES**		
A.13.01.01 Controles de red	Coordinador Utic	Políticas específicas de seguridad de la información por dominio PD-UTIC-02 Continuidad Operacional de Tecnología Instructivos Utic
A.13.01.02 Seguridad de los servicios de red		
A.13.01.03 Segregación de redes		
5.14 Transferencia de Información *(ISO 27002:2022)*		
Dominio: **ADQUISICIÓN. DESARROLLO y MANTENIMIENTO DE SISTEMAS**		
A.14.02.02 Procedimientos de control de cambios		Políticas específicas de seguridad de la información PD-UTIC-01 Desarrollo de Módulos de Software PD-UTIC-02 Continuidad Operacional de Tecnología Instructivos UTIC
A.14.02.05 Principios de ingeniería de sistema seguro		
8.11 Enmascaramiento de datos (ISO 27002:2022)		
A.14.02.08 Prueba de seguridad del sistema		
A.14.02.09 Prueba de aprobación del sistema		
Dominio: **RELACIONES CON LOS PROVEEDORES**		
5.19 Seguridad de la Información en servicios de proveedores *(ISO 27002:2022)*	Coordinador Compras.	Políticas específicas de seguridad de la información por dominio PD-UTIC-02 Continuidad Operacional de Tecnología Instructivos Utic PD-CCP-03 Compras y Contrataciones PCG-08 Evaluación de Proveedores
5.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores *(ISO 27002:2022)*	Coordinador Utic Coordinador Adm. Administradores de los Sistemas de Información y Servicios digitales	
5.23 Seguridad de la información en el uso de servicios Cloud *(ISO 27002:2022)*	Coordinador Utic	
5.7 Inteligencia de Amenazas *(ISO 27002:2022)*	Coordinador Utic Administradores de los Sistemas de Información y Servicios digitales Encargado SSI	Informes técnicos de Eventos de Ciberseguridad
Dominio: **ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		
A.16.01.01 Responsabilidades y Procedimientos	Coordinador Utic	Políticas específicas de seguridad de la información por dominio PD-UTIC-02 Continuidad Operacional de Tecnología Instructivos Utic
A.16.01.02 Informe Eventos de Seguridad de la información	Encargado SSI	
A.16.01.03 Informe de Debilidades de la Seguridad de la Información	Encargado SSI	
A.16.01.05 Respuesta ante incidentes de seguridad de la información	Coordinador Utic	
Dominio: **CONTINUIDAD DE LA SEGURIDAD**		
A.17.01.01 Planificación de la continuidad de la seguridad de la información	Encargado SSI	Resolución Plan de Continuidad de Seguridad de la Información
Dominio: **COMPLIMIENTO**		

A.18.01.01 Identificación de la legislación vigente y los requisitos contractuales	Análisis Jurídico	Resol.Política SSI Políticas específicas de seguridad de la información por dominio PD-UTIC-02 Continuidad Operacional de Tecnología Instructivos Utic PD-UTIC-01 Desarrollo de Módulos de Software PD-GP-01 Selección, Contratación e Inducción
A.18.01.03 Protección de los registros	Coordinador Utic	
A.18.01.04 Privacidad y protección de la información de identificación personal	Análisis Jurídico	
A.18.02.01 Revisión independiente de la seguridad de la información	Calidad	
A.18.02.02 Cumplimiento con las Políticas y Normas de Seguridad	Jefaturas CdR	
A.18.02.03 Verificación del cumplimiento técnico	Encargado SSI	
Protocolo de Seguridad para el Trabajo Distancia		
6.7 Trabajo Remoto (ISO 27002:2022) (A-6.02.02 Teletrabajo)	Coordinador Utic	PD-UTIC-02 Continuidad Operacional de Tecnología Instructivos UTIC

DEFINICIONES

Activos de Información: Todo/s aquel o aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución. Los Activos de Información incluyen:
Los registros de información propiamente tal, en sus múltiples formatos (papel o digital, texto, imagen, audio, video, etc.).
Los Equipos/sistemas que soportan la información.
Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.
Responsable o Dueño del Activo de Información: Corresponde al rol o cargo de la persona autorizada para tomar decisiones respecto de un activo de información. Esto no implica necesariamente derecho de propiedad sobre el activo.
Ubicación: Corresponde al lugar físico o lógico donde se encuentra el activo mientras es utilizado en el proceso.
Tiempo de Retención: Corresponde al tiempo en el cual el activo de información debe ser mantenido por la Institución en el medio de almacenamiento.
Amenaza: Evento que puede desencadenar un incidente en la organización, produciendo eventualmente daños materiales, o pérdidas inmateriales en sus activos.
Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor paraevitar suplantación de identidades.
Confidencialidad: Garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
Disponibilidad: Garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma,toda vez que lo requieran.
Documento Electrónico: De acuerdo con la Ley 17 .799, es toda representación de un hecho, imagen o idea que sea creada,enviada, comunicada o recibida por medios electrónicos y almacenados de un modo idóneo para permitir su uso posterior.
CdR: Centro de Responsabilidad existentes en la CNR (Área, departamento y unidades).
Evento: Una ocurrencia identificada en un sistema, servicio, o cualquier otro elemento. Es una posible brecha de cumplimiento de las políticas/normas/procedimientos o fallas en las medidas de Seguridad ya implementadas.
Impacto: Efecto causado en los objetivos de la institución.
Incidente: Está indicado por un simpleo múltiples eventos esperados. Esto tiene una alta probabilidad de comprometer continuidad de las operaciones de la misión institucional.
Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
Seguridad de la información: Todas aquel/as medidas preventivas y reactivas que permitan resguardar y proteger la información buscando mantener la confidencialidad, integridad y disponibilidad de esta.
Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales y que están relacionados con el hardware y software operados por la CNR o por un tercero que procese información en su nombre, para llevar **a** cabo una función propia de la CNR, sin tener en cuenta la tecnología utilizada, ya sea computación de datos, telecomunicaciones u otro tipo.
Tecnología de la Información: Se refiere al hardware y software operados por la CNR o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la CNR, sin tener en cuenta la tecnología utilizada, ya sea computación de datos, telecomunicaciones u otro tipo.
Integridad: Salvaguardar la exactitud y totalidad de la información y los métodos deprocesamiento.
Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las queestá sujeto la CNR.
No repudio: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
Probabilidad: Es la oportunidad de que algo ocurra. Es la medición de la oportunidad.
Protección a la duplicación: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
Riesgo: Materialización de vulnerabilidades identificadas, agrupadas con su probabilidad de ocurrencia, amenazas expuestas, junto con el impacto negativo que podría provocar a las operaciones de la Institución.
Vulnerabilidad: Corresponde a una debilidad que facilita la materialización de una amenaza. La situación generada, dependerá del contexto encontrado.
Análisis de Riesgos: uso sistemático de la información para identificar peligros y estimar los riesgos.
Evaluación de Riesgos: proceso general de análisis y valoración de riesgos.
Estimación de Riesgos: el proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar la importancia del riesgo.
Tratamiento del Riesgo: proceso de selección e implementación de medidas para reducir/compartir el riesgo.
Plan de Contingencia: Instrumento de gestión que contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones del servicio.
Continuidad Operativa: Es el resultado de la aplicación de una metodología diseñada para que en la práctica la Institución pueda recuperar y restaurar sus funciones críticas que se encuentren parcial o totalmente interrumpidas dentro de un tiempo predeterminado, después de la ocurrencia de un incidente.
Ciberseguridad: Conjunto de herramientas, políticas, métodos de gestión de riesgos, prácticas, y tecnologías que pueden utilizarse para proteger los activos de información de la organización y sus usuarios en el entorno digital, buscando garantizar la disponibilidad, integridad y confidencialidad de la información.
Ciberataques: Es un ataque que se monta en contra de equipos, sistemas y servicios digitales a través del ciberespacio.
Protocolo de Seguridad para Trabajo a Distancia : Protocolo en el que se entregan algunas recomendaciones para que la información que se transmite al realizar un trabajo remoto pueda desarrollarse de la manera más segura posible.

ANÓTESE Y COMUNÍQUESE

FIRMA ELECTRÓNICA AVANZADA · COMISIÓN NACIONAL DE RIEGO ·

WILSON URETA PARRAGUEZ
Secretario Ejecutivo
Comisión Nacional De Riego

PLUE/AGJ/LNR/CCA

Distribución:

DIVISIÓN JURÍDICA
ÁREA DE GESTIÓN ESTRATÉGICA
AUDITORÍA INTERNA
UNIDAD DE ANÁLISIS JURÍDICOS Y ASUNTOS LEGALES
UNIDAD DE PERSONAS Y BIENESTAR
UNIDAD DE COMPRAS PÚBLICAS
UNIDAD DE FINANZAS

UNIDAD DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACION
DEPARTAMENTO DE ADMINISTRACIÓN Y FINANZAS
COMISIÓN NACIONAL DE RIEGO