

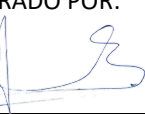

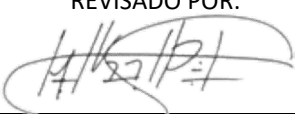
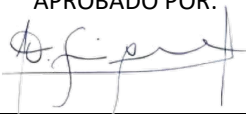


POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:
ADMINISTRACIÓN DE ACTIVOS DE INFORMACIÓN
SUBSECRETARÍA DE ENERGÍA

CONTROL NORMA ISO 27001:2022 / 27002:2022

- 5.9. Inventario de información y otros activos asociados
- 5.11 Devolución de activos
- 5.12 Clasificación de la información

REVISIONES DE LA POLÍTICA				
N.º Versión	Fecha	Motivo de la revisión	Detalle del cambio	Preparado por
1	15-12-2016	Aprobación de Política por CSI	Creación de la política	Encargado de Seguridad de la Información
2	04-12-2017	Nuevos requisitos de la Red de Expertos	Se consideran los siguientes controles NORMA ISO 27001:2013 y 27002:2013, A.08.01.01 Inventario de activos, A.08.01.02 Propiedad de los activos, A.08.01.04 Devolución de activos y A.08.02.01 Clasificación de información	Encargado de Seguridad de la Información
3	06-09-2019	Revisión de Política de Seguridad Organización de la Seguridad	Se revisan los siguientes controles NORMA ISO 27001:2013 y 27002:2013, A.08.01.01 Inventario de activos, A.08.01.02 Propiedad de los activos, A.08.01.04 Devolución de activos y A.08.02.01 Clasificación de información	Encargado de Seguridad de la Información
4	01-10-2024	Actualización del documento	Actualización de controles y normativa vigente a ISO27001:2022 / ISO27002:2022	Encargado de Seguridad de la Información

ELABORADO POR:  	REVISADO POR: 	APROBADO POR: 
Gonzalo Aravena Bravo Encargado Seguridad de la Información	Manuel Vásquez Representante del Departamento de Tecnologías	Oscar Fuentes Mondaca Jefa División Administración y Finanzas

	de la Información	
--	-------------------	--

Contenido

1. OBJETIVO3

2. ALCANCE3

3. ROLES Y RESPONSABILIDADES.....3

4. DEFINICIONES.....4

5. DESCRIPCIÓN DE LOS CONTROLES ASOCIADOS A LA POLÍTICA.....8

5.1. INVENTARIO DE ACTIVOS DE INFORMACIÓN8

5.2. PROPIEDAD DE LOS ACTIVOS9

5.3. ENTREGA DE ACTIVOS.....9

5.4. DEVOLUCIÓN DE ACTIVOS.....9

5.5. CLASIFICACIÓN DE LA INFORMACIÓN 10

6. DIFUSIÓN DE LA POLÍTICA..... 11

7. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN..... 11

1. **OBJETIVO**

Para lograr niveles adecuados de integridad, confidencialidad y disponibilidad de los activos de información de la Subsecretaría, se determinaron como objetivos de esta política, los siguientes:

- Identificar los activos críticos que sustentan el correcto desarrollo de los procesos de provisión de la Subsecretaría.
- Definir los diferentes responsables o custodios que se asignan a los activos de información en la Subsecretaría de Energía.
- Establecer las evaluaciones de riesgo para identificar amenazas y vulnerabilidades potenciales que podrían afectar los activos de información.
- Establecer los controles adecuados por cada activo de información.
- Definir los procesos de gestión y cambios correspondiente a los activos de información.
- Definir el uso aceptable del activo de la información tanto como a los/as funcionarios/as como a las partes interesadas.

2. **ALCANCE**

Esta política aplica a todos los activos de información críticos que serán indicados por las jefaturas de cada área en la Subsecretaría, correspondientes a los procesos de provisión definidos en la institución en la matriz de riesgo institucional, abordando el dominio de seguridad “Administración de Activos de Información”.

Los controles de la normativa NCh-ISO 27002:2022 / 27002:2022 cubiertos por esta política son los siguientes:

ISO/IEC 27001:2013	ISO/IEC 27001:2022	Nombre de Control
A. 8.1.1, 8.1.2	5.9	Inventario de información y otros activos asociados
A. 8.1.4	5.11	Devolución de activos
A. 8.2.1	5.12	Clasificación de la información

3. **ROLES Y RESPONSABILIDADES.**

Responsable de la administración de los activos.

- Cuyo deber es mantener, actualizar y custodiar el Inventario de Activos de Información institucional.

Comité de Seguridad de la Información.

- Responsable del ciclo de vida de las políticas de seguridad de la Subsecretaría de Energía, en conformidad a lo dispuesto en la Política General de Seguridad de la Información de la misma.
- Participa en la revisión de la presente política.

Jefatura División Administración y Finanzas.

- Revisión y aprobación de la presente política.

Encargado de Seguridad de la Información.

- Velar por el cumplimiento de la presente política en la plataforma tecnológica de la Subsecretaría de Energía.
- Podrán delegársele otras responsabilidades según lo que establezca el Comité de Seguridad de la Información, en conformidad a lo dispuesto en la Política General de Seguridad de la Información de la Subsecretaría de Energía.

Jefaturas de División, Gabinete, Oficinas, SEREMIS, Departamentos o Unidades, según corresponda:

- Tienen el rol de determinar y clasificar (Confidencialidad, integridad y disponibilidad) los activos de información críticos o relevantes de su área, estos serán identificados como los responsables de los activos.
- Responsable de apoyar a las jefaturas en la clasificación de la información según su confidencialidad, integridad y disponibilidad a partir del debido análisis normativo.

Departamento de Gestión y Desarrollo de Personas.

- Son los responsables de recibir la devolución al egreso de los funcionarios, conservando debido registro de entrega, registro de devolución y/o inventario de los activos físicos que fueron entregados a los/as funcionarios/as para la ejecución de sus labores.

Departamento de Tecnologías de la información.

- Son los responsables de implementar los controles tecnológicos para los activos de información.
- Supervisar y auditar de manera periódica el buen uso de los diferentes activos de información.

Funcionarios/as:

- Todo/as quienes formen parte del personal de la Subsecretaría quienes deberán velar por mantener la integridad, confidencialidad y disponibilidad de los activos de información que estén a su cargo, cuidando de su buen uso y realizando su correcta devolución una vez terminada la relación laboral con la institución.

4. DEFINICIONES

1. **Activo informático:** Toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.
2. **Agencia:** La Agencia Nacional de Ciberseguridad, que se conocerá en forma abreviada como ANCI.
3. **Auditorías de seguridad:** Procesos de control destinados a revisar el cumplimiento de las políticas y procedimientos que se derivan del Sistema de Gestión de la Seguridad de la Información.

4. **Autenticación:** Propiedad de la información que da cuenta de su origen legítimo.
5. **Ciberataque:** Intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.
6. **Ciberseguridad:** Preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.
7. **Confidencialidad:** Propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.
8. **Disponibilidad:** Propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.
9. **Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT:** Centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.
10. **Incidente de ciberseguridad:** Todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.
11. **Integridad:** Propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.
12. **Red y sistema informático:** Conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.
13. **Resiliencia:** Capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.
14. **Riesgo:** Posibilidad de ocurrencia de un incidente de ciberseguridad; la magnitud de un riesgo es cuantificada en términos de la probabilidad de ocurrencia del incidente y del impacto de las consecuencias del mismo.
15. **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.
16. **Amenaza:** Causa potencial de un incidente no-deseado por el cual puede resultar dañado un sistema u organización. A modo ejemplar, se consideran como tales: terremotos, inundaciones, sabotajes, amenazas de bombas, negligencias humanas y cortes eléctricos, fallas en sala de servidores, entre otras.

17. **Análisis del riesgo:** El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que los riesgos puedan ocurrir. Consecuencia y probabilidad se combinan para producir un nivel estimado de riesgo según la definición de la organización. Adicionalmente, se debe identificar y analizar los controles mitigantes existentes.
18. **Evaluación del riesgo:** Comparar los niveles de riesgo encontrados contra los criterios de riesgo preestablecidos (si es que han sido establecidos por la dirección) considerando el balance entre los beneficios potenciales y resultados adversos. Ordenar y priorizar mediante un ranking los riesgos analizados.
19. **Proceso:** Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entradas en resultados.
20. **Procedimiento:** Forma específica para llevar a cabo una actividad o un proceso. Los procedimientos pueden estar documentados o no.
21. **Sistema:** Conjunto integrado y coordinado de personas, conocimiento, habilidades, equipos, maquinaria, métodos, procesos, actividades.
22. **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.
23. **Servicio:** El resultado generado por actividades en la interfaz entre el proveedor y el cliente y por actividades internas del proveedor para satisfacer las necesidades del cliente.
24. **Seguridad:** Estado en el cual el riesgo de daño a personas o daños materiales está limitado a nivel aceptable.
25. **Seguridad de funcionamiento:** Término colectivo utilizado para describir el desempeño de la disponibilidad y los factores que la influyen; desempeño de la confiabilidad, de la capacidad de mantenimiento y del mantenimiento de apoyo.
26. **Evento de seguridad de la información:** La ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la Política de Seguridad o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.
27. **Gestión del riesgo**¹: Es un proceso para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un

¹ La gestión del riesgo normalmente incluye la evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo.

aseguramiento razonable respecto del alcance de los objetivos de la organización; (Doc. Técnico N° 70).

28. **Incidente de seguridad de la información:** Corresponde a un evento con probabilidad significativa de comprometer las operaciones institucionales y amenazar la seguridad de la información.
29. **Medios de procesamiento de la información:** Cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan.
30. **Seguridad de la información:** Preservación de confidencialidad, integridad y disponibilidad de la información; además, puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudio y confiabilidad.
31. **Uso aceptable:** Es la utilización de manera autorizada y en estricta conformidad con las políticas y normativas de seguridad de la institución, con el fin de preservar la integridad, confidencialidad y disponibilidad de la información.
32. **Propietario del activo de información:** Corresponde al responsable de tomar decisiones respecto del activo. Esto no implica necesariamente derecho de propiedad sobre el activo de información.
33. **Custodio:** Corresponde al rol o cargo de la(s) persona(s) autorizada(s) para usar el activo de información, ya sea modificándolo, actualizándolo, trasladándolo o limpiándolo.
34. **Datos sensibles:** Aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
35. **Terceras partes:** Se definirá como terceras partes en la presente Política de Seguridad a:
 - Proveedores de servicios y de red;
 - Servicios de asesoría de seguridad;
 - Sociedad Civil;
 - Outsourcing de instalaciones y/o operaciones;
 - Consultores gerenciales y de negocios;
 - Auditores externos;
 - Proveedores de productos de software y servicios de información;
 - Servicio de limpieza, cafetería y otros servicios de apoyo externo;
 - Personal temporal, estudiantes en práctica u otros contratados para la ejecución de una labor determinada durante un acotado período de tiempo.

5. DESCRIPCIÓN DE LOS CONTROLES ASOCIADOS A LA POLÍTICA

5.1. INVENTARIO DE ACTIVOS DE INFORMACIÓN

La Subsecretaría de Energía como propietaria de la información física y lógica, así como de la información generada, procesada, almacenada y transmitida por sus plataformas tecnológicas, otorgará responsabilidad a sus distintas áreas sobre los activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de los mismos.

La información, archivos físicos y lógicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, internet, correo electrónico, herramientas de acceso remoto, aplicaciones y teléfonos, entre otros) propiedad de la Subsecretaría, son activos de la institución y se proporcionan a los/as funcionarios/as y terceros autorizados, para cumplir con los propósitos del Servicio.

Toda la información sensible, así como los activos donde ésta se almacena y se procesa, deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios señalados en la presente política. Los dueños o responsables de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos y áreas.

El levantamiento de activos de información debe consolidarse en un inventario, el cual debe incluir la siguiente información referente a cada uno de los activos identificados:

- **Nombre del activo de información:** En este campo debe incluirse todos los activos de información identificados para la etapa, independiente de su medio de soporte y sus características.
- **ID:** Identificador único asociado a un activo de información dentro de un sistema de gestión de seguridad de la información.
- **Tipo de activo,** estos pueden ser:
 - Documento: Corresponde a un escrito que refleja el resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella. Este puede ser físico o electrónico.
 - Base de Datos: Es la información sistematizada y organizada.
 - Software: Programa computacional empaquetado producido por una empresa que lo comercializa.
 - Sistema: Programa computacional a medida, desarrollado por la institución o por un externo, cuyo objetivo es apoyar un proceso de negocio.
 - Equipos: Objetos o dispositivos que realizan o apoyan la realización de una función.
 - Infraestructura Física: Estructura que permite almacenar y/o custodiar activos de información del proceso, tales como: Data Center, oficinas de partes, bodegas, caja fuerte, etc.
 - Expediente: Conjunto de documentos y formularios dispuestos en estricto orden de ocurrencia, de ingreso o egreso. Este puede ser físico o electrónico.

- Personas: Individuos que tienen acceso, manejan o de alguna manera interactúan con la información dentro de la Subsecretaría de Energía. Estas personas pueden incluir funcionarios, contratistas, socios comerciales, alta dirección u otras partes interesadas que participan en las operaciones de la Subsecretaría de Energía.
- Ubicación: Corresponde al lugar físico o lógico donde se encuentra el activo mientras es utilizado en el proceso, esta descripción debe ser lo suficientemente detallada como para determinar a partir de esta información las condiciones de seguridad física en las que se encuentra el activo.
- Responsable/Dueño: Corresponde al rol o cargo de la persona autorizada para tomar decisiones respecto del activo. Esto no implica necesariamente derecho de propiedad sobre el activo.
- Persona autorizada para manipular: Corresponde al rol o cargo de la(s) persona(s) autorizada(s) para usar el activo de información, ya sea modificándolo, actualizándolo, trasladándolo o limpiándolo.

5.2. RESPONSABLE DE LOS ACTIVOS

Los activos mantenidos en el inventario deben tener asignado un responsable o propietario/a, quien es responsable de la administración correcta de un activo durante todo su ciclo de vida.

Entre las funciones y responsabilidades de los responsables de los activos de información se encuentran las siguientes:

- Velar para que se realice un inventario de todos los activos que tiene a su cargo.
- Asegurarse de que los activos de información se protejan y se clasifiquen de acuerdo a su grado de confidencialidad, integridad y disponibilidad.
- Definir y revisar periódicamente las restricciones de acceso y clasificaciones para los activos críticos, considerando las políticas de control de acceso pertinentes.
- Asegurarse de un manejo adecuado cuando se elimine o destruya un activo.
- Responsable de que se implementen los controles tecnológicos adecuados a todos los activos que están bajo su cargo.

Se pueden delegar las tareas rutinarias a un custodio que resguarde los activos diariamente, pero la responsabilidad sigue siendo el propietario o responsable del activo de información.

En sistemas de información complejos, se puede asignar grupos de activos que actúen en conjunto para brindar un servicio en particular. En este caso el dueño o responsable de este servicio está a cargo de la entrega del servicio, incluida la operación de sus activos.

5.3. ENTREGA DE ACTIVOS

Será responsabilidad del departamento de desarrollo y gestión de personas realizar las solicitudes al departamento de tecnologías de la información respecto a la preparación de los activos específicos a los/as funcionarios/as de acuerdo con la función que estos cumplan

dentro de la institución. Dicha entrega deberá generar un documento de entrega de activos, el cual debe ir acompañado de la presente política junto con los siguientes documentos: **SGSI-POL-15-Dispositivos móviles.pdf** y **A.08.01.01_PROC_ACTIVOS_DE_INFORMACION**.

5.4. DEVOLUCIÓN DE ACTIVOS

Todos/as los/as funcionarios/as y usuarios/as externos/as deben devolver los activos de información institucionales al departamento de desarrollo y gestión de personas que estén en el poder del funcionario/a al finalizar su empleo, contrato o acuerdo. Para ello se deberán cumplir los procedimientos específicos de acuerdo al rol que tienen las distintas áreas en el proceso de egreso de un/a funcionario/a.

5.5. CLASIFICACIÓN DE LA INFORMACIÓN

Los/as responsables/as de los activos de información son los responsables de clasificar sus activos, de acuerdo a las condiciones de confidencialidad, integridad y disponibilidad que ellos presentan. Los activos de clasificarán según su porcentaje y categorías:

CLASIFICACIÓN DE LA INFORMACIÓN	Porcentaje %
Confidencialidad	40%
Integridad	20%
Disponibilidad	40%

- **Confidencialidad:**

- 1) Baja (Pública): Activo de información que no tiene restricciones de acceso.
- 2) Media (Interna): Activo de información que cuyo acceso es exclusivo de los/as funcionarios/as de la Subsecretaría de Energía.
- 3) Alta (Reservada): Activo de información cuyo acceso no autorizado tiene impacto para la institución o terceros.

- **Integridad:**

- 1) Baja: Activo de información cuya modificación no deseada tiene consecuencias con impacto leve para la institución o terceros.
- 2) Media: Activo de información cuya modificación no deseada tiene consecuencias con impacto significativo para la institución o terceros.
- 3) Alta: Activo de información cuya modificación no deseada tiene consecuencias con impacto grave para la institución o terceros.

- **Disponibilidad:**

- 1) Baja: Activo de información cuya inaccesibilidad, tiene impacto leve para la institución o terceros.
- 2) Media: Activo de información cuya inaccesibilidad, tiene impacto significativo para la institución o terceros.
- 3) Alta: Activo de información cuya inaccesibilidad, tiene impacto grave para la institución o terceros.



6. DIFUSIÓN DE LA POLÍTICA.

La política sobre Administración de Activos de Información deberá ser conocida por todos/as los/as funcionarios/as de la Subsecretaría y contar con una adecuada difusión. Para estos efectos, la presente política será comunicada vía correo electrónico a todos/as los/as funcionarios/as y se publicará en la intranet institucional.

7. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN.

Para garantizar la idoneidad, adecuación y efectividad continua de la presente política, se deberá revisar/evaluar al menos cada 2 años o cuando ocurra algún cambio significativo en el entorno organizacional, las circunstancias comerciales, condiciones legales o normativas o el entorno tecnológico, considerando además los resultados de las auditorías al sistema, las cuales se realizarán de acuerdo con la planificación interna del Ministerio.