



POLÍTICA DE SEGURIDAD PARA EL CONTROL DEL ACCESO  
Código: SGSI-POL-04  
Página: 1 de 11  
Versión: 4  
Nivel de Confidencialidad: Interno - Confidencial  
Fecha Versión: 31-01-2024

## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:

### CONTROL DEL ACCESO

#### SUBSECRETARÍA DE ENERGÍA


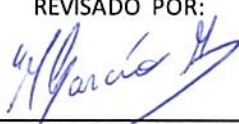
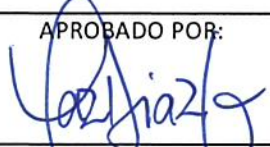
CONTROL NORMA ISO 27001:2022 / 27002:2022

- 5.15 Control de acceso
- 5.17 Autenticación de información
- 8.2 Derechos de acceso privilegiado
- 8.3 Restricción de acceso a la información
- 8.5 Autenticación segura

#### REVISIONES DE LA POLÍTICA

Nº Versión	Fecha	Motivo de la revisión	Detalle del cambio	Preparado por
1	12-12-2016	Aprobación de Política por CSI	Creación de la política	Encargado de Seguridad de la Información.
2	04-12-2017	Actualización del documento	Ajuste de formato según lo indicado por la Red de Expertos. Incorporación de los siguientes controles de la Nch ISO 27001:2013: A.9.2.3, A.12.1.1, A.12.3.1, A.12.6.1	Encargado de Seguridad de la Información.
3	06-09-2019	Revisión de Política de Seguridad Organización de la Seguridad	Se consideran los siguientes controles NORMA ISO 27001:2013 / 27002:2013, A.09.01.01 Política de control de acceso, A.09.01.02 Acceso a redes y servicios de red A.09.02.03 Gestión de derechos de acceso privilegiados, A.09.04.01 Restricción de acceso a la información, A.09.04.02 Procedimientos de inicio de sesión seguro y A.09.04.03 Sistema de gestión de contraseñas	Encargado de Seguridad de la Información.
4	31-01-2024	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/a Seguridad de la Información	Mario García Antipa Representante del Departamento de Tecnologías de la Información	Paz Díaz Godoy Jefa División Administración y Finanzas (S)

## Contenido

1. OBJETIVOS .....	3
2. ALCANCE.....	3
3. ROLES Y RESPONSABILIDADES .....	4
4. DEFINICIONES.....	4
5. DESCRIPCIÓN DE LOS CONTROLES ASOCIADOS A LA POLÍTICA .....	7
5.1. CONTROL DE ACCESO LÓGICO .....	7
5.2. CONTROL DE ACCESO FÍSICO .....	8
5.3. IDENTIFICACIÓN Y CONTRASEÑAS REQUERIDAS .....	8
5.4. TIPOS DE CUENTAS .....	8
5.5. CENTRALIZACIÓN DE LAS CUENTAS .....	9
5.6. PROTECCIÓN DE ESTACIONES DE TRABAJO .....	9
5.6.1.CAMBIO PERIÓDICO Y CARACTERÍSTICAS DE LAS CONTRASEÑAS .....	10
5.6.2.ASIGNACIÓN DE CONTRASEÑAS EXPIRADAS Y REASIGNACIÓN DE CONTRASEÑAS .....	10
5.6.3.LÍMITE A INTENTOS FALLIDOS DE INGRESO .....	10
5.6.4.REGLAS GENERALES DE LAS CONTRASEÑAS .....	11
5.7. ADMINISTRACIÓN DE DERECHOS PRIVILEGIADOS .....	11
6. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN.....	11
7. DIFUSIÓN DE LA POLÍTICA.....	11



## 1. OBJETIVOS

- Definir los lineamientos para el adecuado resguardo de la información soportada en la plataforma tecnológica de la Subsecretaría de Energía.
- Establecer la normativa para el acceso autorizado a la información clasificada tanto para el ambiente lógico como físico de la institución.
- Establecer los requerimientos de seguridad para la adecuada administración, implementación y diseño de las redes de comunicación informática en la Subsecretaría de Energía.
- Definir una normativa alineada con las buenas prácticas de seguridad para la información administrada por los/as funcionarios/as desde sus estaciones de trabajo.
- Establecer como norma las prácticas destinadas a la adecuada ubicación del equipamiento, junto con el mantenimiento periódico del mismo para resguardar su disponibilidad e integridad.
- Establecer la definición de áreas restringidas en virtud de la confidencialidad y criticidad de la información contenida en ellas.
- Disponer los lineamientos para la adecuada protección del equipamiento y zonas restringidas en virtud de la continuidad operacional de la Subsecretaría de Energía.
- Definir la forma y periodos de evaluación y/o auditoría para la verificación de todos los registros de accesos de los perfiles de los/as usuarios/as.

## 2. ALCANCE

Todos los recursos computacionales de la Subsecretaría de Energía y cualquier usuario/a que necesite tener acceso a los recursos de la red.

Los/as usuarios/as, operadores/as y administradores/as de la Subsecretaría de Energía.

Los/as usuarios/as externos/as que deban acceder a algún recurso de la Subsecretaría de Energía.

Los siguientes dominios de seguridad de la norma Nch ISO 27001:2022 / 27002:2022:

ISO/IEC 27001:2013	ISO/IEC 27001:2022	Nombre de Control
A.9.1.1, A.9.1.2	5.15	Control de acceso
A.9.2.4, A.9.3.1, A.9.4.3	5.17	Autenticación de información
A.9.2.3	8.2	Derechos de acceso privilegiado
A.9.4.1	8.3	Restricción de acceso a la información
A. 9.4.2	8.5	Autenticación segura





### **3. ROLES Y RESPONSABILIDADES**

Para un eficaz funcionamiento de la presente Política, se han definido los siguientes roles relevantes aparejados de las siguientes responsabilidades:

#### **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 Operaciones y Ciberseguridad.**

- Responsable de la implementación de controles de seguridad en la plataforma tecnológica de la Subsecretaría de Energía y administrar los controles de acceso lógico a los sistemas de información, teniendo a cargo las altas y bajas de cuentas de usuario/a.

#### **Departamento de Gestión y Desarrollo de Personas.**

- Administrar los controles de acceso físico, teniendo a cargo las altas y bajas del usuario/a.
- Son los responsables de solicitar los accesos lógicos a los/as funcionarios/as y administrar los controles de acceso físico, teniendo a cargo las altas y bajas del usuario/a.

#### **Encargado de Seguridad de la Información.**

- Velar por el cumplimiento de la presente política en la plataforma tecnológica de la Subsecretaría de Energía.
- Podrán delegarse 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.

#### **Funcionarios/as**

- Seguir todas las directrices establecidas en la política.

### **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<sup>1</sup>:** Es un proceso para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un 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. **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.
32. **Información clasificada:** Datos o material que ha sido designado con un nivel de clasificación específico debido a su sensibilidad y que requiere protección especial en el ámbito de la seguridad de la información. Estos niveles de clasificación indican el grado de confidencialidad y la necesidad de controlar el acceso a dicha información para evitar divulgaciones no autorizadas.

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

### 5.1. CONTROL DE ACCESO LÓGICO

Para todo sistema computacional de la Subsecretaría de Energía, el/la usuario/a deberá señalar quién es (identificación) y luego deberá comprobar que es quién dice ser (autenticación). La identificación se realizará normalmente por un Username, Usuario/a o "Código de Usuario".

---

<sup>1</sup> La gestión del riesgo normalmente incluye la evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo.





El acceso para todos/as los/as usuarios/as de la Subsecretaría de Energía será solicitado a través del Departamento de Gestión y Desarrollo de Personas al Departamento de Tecnologías de la Información y este debe establecer el perfil de acceso que va a tener dicho usuario/a según el cargo que este ocupa.

En caso del acceso (frecuente o temporal) de partes interesadas se deberá establecer la misma metodología aplicada a los/as funcionarios/as con previa solicitud, evaluación y autorización por parte del área que contrata sus servicios y el departamento de gestión y desarrollo de personas. En todo caso debe existir entre la subsecretaría y en las partes interesadas un contrato y/o convenio que estipule los convenios de confidencialidad (DNA).

## 5.2. CONTROL DE ACCESO FISICO

Para garantizar la seguridad en todas las instalaciones de la Subsecretaría de Energía, se ha implementado un riguroso sistema de control de acceso físico. Este proceso es gestionado por el departamento de gestión y desarrollo de personas, la cual se encarga de generar la configuración de acceso físico según el perfil correspondiente al cargo de cada funcionario/a.

## 5.3. IDENTIFICACIÓN Y CONTRASEÑAS REQUERIDAS

La identificación y contraseña serán requeridas antes de tener acceso a cualquier recurso de la red, debiendo los/as usuarios/as ser identificados positivamente mediante una cuenta de usuario/a y su contraseña.

El/la Usuario/a y la Contraseña son individuales y de uso personal. En este sentido, está prohibido el uso de un nombre de otro usuario/a o facilitar los datos antes referidos a un tercero.

Todo/a nuevo/a funcionario/a requiere de una credencial de autenticación para el ingreso a su estación de trabajo, correo institucional, sistemas institucionales, acceso a recursos compartidos, acceso remoto y wifi.

De igual manera no está permitido tener credenciales de acceso visibles en lugares de trabajo de los/as funcionarios/as.

En caso del acceso (frecuente o temporal) de partes interesadas se deberá establecer la misma metodología aplicada a los/as funcionarios/as con previa solicitud, evaluación y autorización por parte del área que contrata sus servicios y el departamento de gestión y desarrollo de personas. En todo caso debe existir entre la subsecretaría por un acto administrativo o en el contrato como tal.

## 5.4. TIPOS DE CUENTAS

Se reconocen 4 niveles globales de cuentas de usuario/a:

- Nivel Usuario/a Externo o Temporal (Auditoría externas o practicantes)
- Nivel Usuario/a Perfilado, de acuerdo con sus funciones específicas dentro de los sistemas.





- Nivel Administrador/a, en las plataformas o sistemas que lo permitan.
- Nivel Cuentas de servicios TI, existen plataformas que requieren cuentas de servicio para su integración con Active directory o accesos pertinentes a otros recursos.

Los diferentes tipos de cuentas de usuario/a antes mencionados, definen sus propios niveles de acceso y privilegios en el sistema de información de la Subsecretaría de Energía. Su función primordial es establecer perfiles propios para cada nivel básico, los que serán usados como perfil por omisión si no se especifican otras características.

#### 5.5. CENTRALIZACIÓN DE LAS CUENTAS

Para todo/a nuevo/a funcionario/a que se cree como usuario/a, éste deberá ser definido por el Departamento de gestión y desarrollo de personas, de acuerdo al procedimiento de creación de cuentas de usuarios/as correspondiente, y el departamento de tecnologías de la información es quien se encarga de monitorear, gestionar las altas y bajas y mantener actualizada la base de datos correspondiente a los/as usuarios/as y perfiles de acceso según directrices emanadas por parte del departamento de gestión y desarrollo de personas.

La modificación de una cuenta de usuario/a por cambio de división o unidad deberá ser informado por el Departamento de Gestión y Desarrollo de Personas mediante a un ticket.

Cualquier solicitud de cambio de privilegios asignados a una cuenta deberá ser solicitada desde la Jefatura correspondiente y será evaluada por el departamento de gestión y desarrollo de personas para finalmente realizar la solicitud de los cambios al departamento de tecnologías de la información, y este último deberá actualizar la base de datos correspondientes.

En caso de cambio de unidad del usuario/a, se deberá además validar la eliminación de privilegios anteriores por el/la Jefe/a de la unidad anterior.

#### 5.6. PROTECCIÓN DE ESTACIONES DE TRABAJO

Las estaciones de trabajo deberán tener una contraseña de ingreso y un protector de pantalla (screensaver) con contraseña y activación máxima de 10 minutos.

Toda información física que sea clasificada dentro de la subsecretaría como información confidencial o secreta no deberá permanecer sobre los escritorios de los/as funcionarios/as, estos deberán estar en un sobre cerrado y en cajones con acceso bajo llave.

Todo/a funcionario/a que se levante de su estación deberá hacer cierre de su sesión de trabajo.

En aquellos puntos de impresión se deberá establecer función de autenticación de modo que los/as funcionarios/as sean los/as únicos/as que puedan obtener sus impresiones solo cuando estén ubicados en dichos puntos.

Todo información confidencial o secreta no debe quedar escrita en pizarra u otro tipo de pantallas cuando no requiera de estas.



### 5.6.1. CAMBIO PERIÓDICO Y CARACTERÍSTICAS DE LAS CONTRASEÑAS

Los/as usuarios/as deberán cambiar su contraseña cada 90 días.

Los sistemas de información de la Subsecretaría de Energía deberán ocultar la contraseña al momento de ser ingresada por el/la usuario/a. La clave de acceso deberá tener un largo mínimo de 8 caracteres y ser alfanumérica, es decir, letras, números y opcionalmente algún signo especial ("\_", "-", "@", ".", "").

### 5.6.2. ASIGNACIÓN DE CONTRASEÑAS EXPIRADAS Y REASIGNACIÓN DE CONTRASEÑAS

La contraseña asignada a una nueva cuenta obligará al usuario/a a cambiarla durante su primera conexión.

La solicitud de cambio de contraseña por olvido se deberá efectuar al Departamento de Tecnologías de la Información por sistema de ticket, previa identificación positiva del usuario/a que lo solicita.

Toda reasignación de contraseñas será registrada en la bitácora (log) del sistema y deberá notificarse al usuario/a de la cuenta, a su casilla de correo registrada al crear la cuenta asociada. Esto tiene como finalidad detectar casos de suplantación de identidad.

El Departamento de Tecnologías de la Información dispondrá de herramientas que eviten posibles tácticas de suplantación de identidad de usuarios/as u otros artilugios para obtener información a la cual no tiene acceso normalmente <sup>2</sup>.

### 5.6.3. LÍMITE A INTENTOS FALLIDOS DE INGRESO

Todos los eventos de ingreso fallido y satisfactorio a los sistemas de información de la Subsecretaría de Energía serán registrados en Logs.

Para prevenir ingresos mediante la prueba de varias posibles contraseñas, se limita la aceptación de 10 intentos consecutivos de ingreso, configurado como estándar de la Subsecretaría de Energía.

Después de los 10 intentos fallidos, la cuenta de usuario/a será deshabilitada. Para efectos de habilitarla nuevamente, el/la usuario/a deberá notificar vía sistema de ticket en horario laboral al Departamento de Tecnologías de la Información, el que habilitará la cuenta previa verificando la identidad del usuario/a, generando el informe de atención respectivo.

En caso de partes interesadas sólo podrá ser reactivado el acceso por consentimiento del departamento responsable al momento de crear la cuenta del usuario/a.

---

<sup>2</sup> Se denomina Ingeniería Social en el campo de la Seguridad de la Información.





#### **5.6.4. REGLAS GENERALES DE LAS CONTRASEÑAS**

La Subsecretaría de Energía restringirá el acceso a los datos de autenticación. Los datos de autenticación deberán ser protegidos con controles de acceso y encriptación para evitar que personas no autorizadas logren obtención de los datos.

Para evitar transmitir contraseñas de forma insegura en la red, en sistemas que manejen información sensible o clasificada como confidencial, serán empleados mecanismos de cifrado.

Las credenciales (usuario/a y claves) no deberán ser incluidas en aplicaciones donde puedan quedar expuestas (macros de planillas o documentos o programas de tipo script).

La clave no puede contener el nombre de usuario/a o parte del nombre del funcionario/a.

Para evitar ataques de fuerza bruta, una función de bloqueo de intrusos será implementado en cada sistema, suspendiendo temporalmente la cuenta después de 10 intentos de inicio de sesión no válidos. La reactivación de las cuentas bloqueadas deberá realizarse en conformidad a lo señalado en el numeral 5.6.3, anterior.

#### **5.7. ADMINISTRACIÓN DE DERECHOS PRIVILEGIADOS**

La asignación y uso de accesos privilegiados en los sistemas deberá ser restringido y controlado.

Se deberá asignar derechos de acceso privilegiado a una cuenta de usuario/a distinta a las que se utiliza para sus actividades normales, los que deberán ser asociados a cada sistema y a los/as usuarios/as a quienes se les debería asignar.

El acceso privilegiado a los sistemas deberá ser debidamente autorizado, por la Jefatura directa y la Jefatura del Departamento de Tecnologías de Información. Para las cuentas de administración genéricas de los sistemas, las contraseñas se deberán cambiar regularmente, estas serán guardadas en un sistema para su resguardo.

#### **6. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN.**

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

#### **7. DIFUSIÓN DE LA POLÍTICA.**

La presente política debe ser conocida por todos/as los/as funcionarios/as de la Subsecretaría de Energía, por lo que es necesario contar con una adecuada difusión, la cual se realizará comunicando la política vía correo electrónico a todos/as los/as funcionarios/as y publicándola en la intranet institucional.