POLITICA

CONTROL DE ACCESO

REVISIONES DE LA POLÍTICA			
Nº Versión	**Fecha**	**Motivo de la revisión**	**Paginas elaboradas o modificadas**
0 (cero)	09.08.2012	Elaboración Inicial	Todas
1 (uno)	14.11.2016	Se agrega evaluación, revisión, formalización y difusión de la política de Control de Acceso. Se agregan roles y responsables. Se agregan referencias. Se actualiza el Modo de Operación de la Política de Control de Acceso. Se agrega instrucciones de trabajo. Se agregan registros y/o evidencias.	Todas
2 (dos)	11.09.2019	Se eliminan los siguientes controles: A.09.02.02 - A.09.02.04 - A.09.04.01 - A.13.01.02 - A.14.01.02. Se agregan los siguientes controles: A.09.03.01 - A.12.04.01 - A.12.04.03. Ajuste de forma y fondo, de acuerdo a instrucciones red de expertos PMG/MEI - SSI 2019.	Todas

CONTROLES NCh ISO 27001:2013	A.09.01.01 A.09.01.02 A.09.03.01 A.12.04.01 A.12.04.03

ELABORADO POR	REVISADO POR	APROBADO POR
Jaime García Sepúlveda Encargado Seguridad de la Información Comisión Nacional de Energía	**María Angélica Jiménez O.** Encargada de Ciberseguridad Comisión Nacional de Energía	**José Venegas Maluenda** Secretario Ejecutivo Comisión Nacional de Energía

COMISIÓN NACIONAL DE ENERGÍA CHILE
Ma. ANGELICA JIMENEZ
Encargada de Ciberseguridad

REPUBLICA DE CHILE
SECRETARIO EJECUTIVO
Comisión Nacional de Energía

POLÍTICA

CONTROL DE ACCESO

TABLA DE CONTENIDOS

1. Objetivo

El propósito de esta política es delimitar el acceso y uso aceptable de todo el equipamiento computacional, servicios y sistemas de información, así como de las redes de datos de la Comisión Nacional de Energía. Estas reglas están orientadas a proteger a los funcionarios y a la Institución sobre el uso inapropiado de la información, los servicios de red y equipos informáticos.

2. Alcance

La presente Política de Control de Acceso de la información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información y los sistemas informáticos de la CNE.

Esta Política es aplicable a todo el personal de la Comisión Nacional de Energía, independiente de su calidad contractual. De la misma forma, aplica a todo aquel personal vinculado a tareas de apoyo o asesoría externa a la CNE.

3. Referencias

- Norma NCh-ISO 27001:2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.
- Norma NCh-ISO 27002:2013 Tecnología de la Información – Código de prácticas para la gestión de la seguridad de la información.
- DS. 83 aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.

4. Definiciones

Derechos privilegiados	Conjunto de permiso o atributos dados a un usuario, quien de acuerdo con sus funciones y/o tareas encomendadas, puede acceder a un determinado recurso.
Restricciones de acceso	Delimitar el acceso de los usuarios a determinados recursos.

5. Roles y Responsables

Roles	Responsabilidades
Encargado de Seguridad de la Información	Ejecutar labores de coordinación para una adecuada elaboración, revisión e implementación de esta política y las materias que ella comprende.

Comité de Seguridad de la Información	Asegurar que las materias abordadas en esta política se ejecutan y se cumplen, identificar como se manejan los no cumplimientos, promover la difusión y sensibilización de las materias abordadas en este documento, revisar periódicamente la política detectando y proponiendo mejoras.
Jefe Subdepartamento de Tecnologías de la Información	Evaluar e implementar en caso de ser factible las propuestas de mejora establecidas por el Comité de Seguridad de la Información. Además de revisar periódicamente la política detectando y proponiendo mejoras. Tiene a cargo el otorgamiento de acceso a los recursos de red. Encargado de recepcionar, evaluar y configurar las solicitudes de registro de usuarios, permisos de acceso, perfiles y accesos privilegiados a los servicios y sistemas de información.
Personal / Funcionarios CNE	Cumplir cabalmente con las disposiciones y requerimientos establecidos en la presente política. Cada usuario de la información, equipos informáticos y de los servicios de red de la CNE deberá velar por la correcta implementación de las normas de control de acceso promovidas por la CNE dentro de sus áreas de responsabilidad, así como del cumplimiento por parte de su equipo de trabajo.

6. Modo de Operación

Con el objetivo de proteger la información de la institución previniendo el acceso no autorizado a los equipos y sistemas de la CNE, los usuarios de los sistemas de información de la institución deben poseer una cuenta personal que lo identifique. La identificación se realizará normalmente por un nombre de usuario único (Username).

En el presente documento se abordan las siguientes temáticas:

- Política de control de acceso a los sistemas de información.
- Acceso a las redes y a los servicios de la red.
- Uso de información de autenticación secreta.
- Registro de eventos.
- Registros de actividad del administrador y operador del sistema.

6.1 Política de control de acceso a los sistemas de información - (Control A.9.1.1 NCh ISO 27001:2013)

Todos los funcionarios de la CNE, incluso terceros, deben tener acceso sólo a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de la institución. La asignación de privilegios y acceso a los activos de información (correo electrónico institucional, software, aplicaciones, carpetas compartidas, etc.) deben estar basados en las necesidades de las áreas y aprobados por el propietario de los activos.

Estas necesidades de acceso deben ser determinadas por las respetivas jefaturas, en función de las tareas asignadas al cargo del funcionario.

Para todo medio de procesamiento de información al que se necesite conceder accesos (por ejemplo: servidores, aplicaciones, carpetas compartidas, base de datos, etc.), el dueño de la información en conjunto con el Subdepartamento de Tecnologías de la Información, debe asignar un responsable del medio, quién será encargado de autorizar los permisos de acceso y solicitar los espacios necesarios.

Sólo se pueden conceder accesos a externos a la institución, previa autorización del dueño del medio de procesamiento de información y el dueño de la información. Las cuentas de acceso a terceros deben tener especificado un tiempo de expiración, el que debe ser controlado por el Subdepartamento de Tecnologías de la Información, según corresponda.

Cualquier intento de acceso no autorizado a los equipos, carpetas compartidas, sistemas de información será considerado un incidente grave, por lo que debe reportarse de inmediato al Encargado de Seguridad de la Información.

6.2 Acceso a las redes y a los servicios de la red - (Control A.9.1.2 NCh ISO 27001:2013)

El acceso a los sistemas y servicios de red de la Institución es otorgado sólo a usuarios identificados y autentificados. Para todo sistema de información de la CNE, el usuario deberá señalar quién es (identificación) y luego deberá comprobar que es quién dice ser (autenticación). La identificación se realizará con una cuenta de usuario asignada a cada funcionario y la autenticación se realizará con una contraseña secreta.

Los usuarios deben tener acceso a la red y a los servicios de la red para los que han sido autorizados específicamente, lo cual debe quedar establecido en la asignación de privilegios correspondiente.

Los requisitos de autenticación de la CNE son:

- Antes de tener acceso a cualquier sistema o recurso de la red, todos los usuarios deben ser identificados positivamente mediante su cuenta de usuario y su contraseña.
- La cuenta de usuario y la contraseña deben ser individuales.
- La autenticación en sistemas por parte de funcionarios y administradores deben ser registrados en Logs para actividades de auditoria y eventuales análisis forenses.

6.3 Uso de información de autenticación secreta - (Control A.9.3.1 NCh ISO 27001:2013)

Los funcionarios y contratistas que desarrollen actividades en la institución deben cumplir las siguientes reglas respecto del uso de la información de autenticación:

- Las cuentas de usuario y las contraseñas son individuales e intransferibles.
- Está prohibido el uso de un nombre de usuario ajeno o facilitar la cuenta de usuario y su contraseña personal a un tercero.

- Queda absolutamente prohibido anotar las contraseñas de acceso en lugares visibles o públicos.
- Las credenciales (usuario y contraseña) no deben ser incluidos en aplicaciones donde puedan quedar expuestas (macros de planillas, documentos o programas de tipo script).
- La composición de las contraseñas debe tener un mínimo de 8 caracteres, alfanumérica, fáciles de recordar, que no se basen en nada que otra persona pueda adivinar u obtener fácilmente mediante la información relacionada con el dueño de la cuenta, que no sean vulnerables a ataques de diccionario (es decir, que no conste de palabras incluidas en los diccionarios).
- El usuario deberá cambiar la información de autenticación secreta cuando exista alguna indicación de su posible compromiso.
- Se recomienda no utilizar las mismas contraseñas para fines laborales y personales.

6.4 Registro de eventos- (Control A.12.4.1 NCh ISO 27001:2013)

- Debe monitorearse el uso de las instalaciones de procesamiento de la información, debiendo generar, mantener y revisar registros de las actividades de los usuarios; excepciones, faltas y eventos de seguridad de la información de manera regular.
- Los registros de eventos deberían considerar, entre otros, los siguientes:
  - ID de usuarios.
  - Actividades del sistema.
  - Fecha, horas y detalles de los eventos clave, es decir, el inicio y finalización de la sesión.
  - Los registros de los intentos exitosos y rechazados de acceso al sistema.
  - Las direcciones y protocolos de redes.
- El Encargado de Seguridad de la Información debe tener acceso a los sistemas y a los registros de actividad, con el objetivo de colaborar en el control y efectuar recomendaciones de mejora.

6.5 Registros de actividad del administrador y operador del sistema - (Control A.12.4.3 NCh ISO 27001:2013)

- Se deben registrar, respaldar, proteger y revisar regularmente, las actividades del administrador y operadores de las distintas plataformas tecnológicas. El Log de actividades debe incluir al menos:
  - Identificación del equipo.
  - Horario de arranque y finalización de los procesos del sistema.
  - Errores del sistema y acciones críticas realizadas.
  - Cuenta del operador que realizó la actividad.

7. Periodicidad de evaluación y revisión

- La presente política debe ser evaluada cada dos años como máximo y sus cambios deben ser aprobados por el Secretario Ejecutivo.
- Su cumplimiento se debe revisar en forma anual, en reunión de Comité de Seguridad, con la finalidad de asegurar su cumplimiento e incorporación de todas las normas y procedimientos necesarios de implementar en el marco de Ciberseguridad y Seguridad de la Información.

8. Difusión

La presente Política entrará en vigencia una vez aprobada por el Secretario Ejecutivo y será difundida mediante correo electrónico a todos los funcionarios de la CNE.