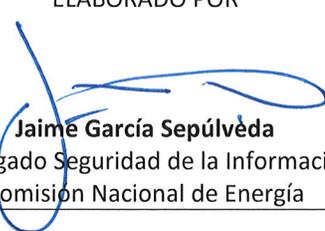


**POLITICA**  
  
**DESARROLLO SEGURO**

REVISIONES DE LA POLÍTICA			
Nº Versión	Fecha	Motivo de la revisión	Paginas elaboradas o modificadas
0 (cero)	15.10.2018	Elaboración Inicial	Todas
1 (uno)	04.09.2019	Ajuste en forma y fondo, de acuerdo a instrucciones red de expertos PMG/MEI – SSI 2019	Todas

CONTROLES NCh ISO 27001:2013	A.12.1.4 A.14.1.2 A.14.2.1 A.14.2.6 A.14.2.8 A.14.2.9
---------------------------------	--

ELABORADO POR   <b>Jaime García Sepúlveda</b> Encargado Seguridad de la Información Comisión Nacional de Energía	 PREVISADO POR <b>María Angélica Jiménez O.</b> Encargada de Ciberseguridad Comisión Nacional de Energía	APROBADO POR   <b>José Venegas Maluenda</b> Secretario Ejecutivo Comisión Nacional de Energía
--	---	---

## POLÍTICA

### DESARROLLO SEGURO

#### TABLA DE CONTENIDOS

1. Objetivo .....	3
2. Alcance .....	3
3. Referencias .....	3
4. Definiciones .....	3
5. Roles y Responsables.....	4
6. Modo de Operación .....	4
6.1. Política de desarrollo seguro - (Control A.14.2.1 NCh ISO 27001:2013) .....	4
6.2. Protección de servicios de aplicación en redes públicas - (Control A.14.1.2 NCh ISO 27001:2013).....	5
6.3. Entorno de Desarrollo Seguro - (Control A.14.2.6 NCh ISO 27001:2013) .....	5
6.4. Pruebas de seguridad del sistema - (Control A.14.2.8 NCh ISO 27001:2013).....	6
6.5. Pruebas de aprobación del sistema - (Control A.14.2.9 NCh ISO 27001:2013).....	7
6.6. Separación de entornos de desarrollo, prueba y operacionales - (Control A.12.1.4 NCh ISO 27001:2013).....	7
7. Periodicidad de evaluación y revisión .....	7
8. Difusión .....	8

## 1. Objetivo

El propósito de esta política es garantizar la seguridad de la información como parte integral del ciclo de vida de los sistemas de información institucionales, el cual incluye las fases de adquisición, desarrollo y mantenimiento de software y sistemas. Esta política considera un conjunto de reglas y prácticas orientadas a proteger el uso inapropiado de la información, por parte de los funcionarios institucionales o de personal externo a la institución.

## 2. Alcance

La presente Política de Desarrollo Seguro 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 debe ser conocida por todos los funcionarios de la Comisión, sean éstos en calidad de Planta, Contrata o personal a honorario que cumplan sus funciones en dependencia de la CNE. De la misma forma todo aquel personal vinculado a tareas de apoyo o asesoría externa a la CNE.

## 3. Referencias

- Norma Chilena ISO 27001:2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos.
- Norma Chilena ISO 27002:2013 Tecnologías de la Información – Técnicas de Seguridad - Código de prácticas para los controles de 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

<b>Desarrollo Seguro</b>	Requisito para generar un servicio, arquitectura, software y sistema seguro, desde la perspectiva del resguardo de la información.
<b>Vulnerabilidades</b>	Se refiere a alguna condición de debilidad o fragilidad que se encuentra presente en el activo identificado. Usualmente se traduce en una debilidad o ausencia de control, que posibilita la ocurrencia de un incidente y que pueden afectar a uno o más activos de información.
<b>Equipo de Desarrollo</b>	Corresponde a los funcionarios institucionales o personal externo que forman parte del grupo a cargo de analizar y programar las funcionalidades de proyectos de desarrollo de software y sistemas.

	<p>Política          Desarrollo Seguro          Página: 4 de 8          Versión: 1          Fecha Versión: 04 de septiembre de 2019</p>
--	---

## 5. Roles y Responsables

Roles	Responsabilidades
<b>Encargado de Seguridad de la Información</b>	Ejecutar labores de coordinación para una adecuada elaboración, revisión e implementación de esta política y las materias que ella comprende.
<b>Comité de Seguridad de la Información</b>	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.
<b>Jefe Subdepartamento de Tecnologías de la Información</b>	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.
<b>Personal / Funcionarios CNE</b>	Cumplir cabalmente con las disposiciones y requerimientos establecidos en la presente política. Cada funcionario de la CNE deberá velar por la correcta implementación de las normas de desarrollo seguro de sistemas promovidos por la CNE dentro de sus áreas de responsabilidad, así como del cumplimiento por parte de su equipo de trabajo.
<b>Personal Externo</b>	Cumplir cabalmente con las disposiciones y requerimientos establecidos en la presente política.

## 6. Modo de Operación

### 6.1. Política de desarrollo seguro - (Control A.14.2.1 NCh ISO 27001:2013)

La Política de Desarrollo Seguro de la CNE comprende las reglas para el desarrollo de software y sistemas dentro de la organización. Para esto, se establecen los siguientes lineamientos:

- Se deberán utilizar técnicas de programación seguras tanto para los desarrollos nuevos como en las situaciones de reutilización de códigos donde es posible que no se conozcan las normas que se aplican al desarrollo o donde no sean coherentes con las buenas prácticas actuales. Lo anterior, tanto para el desarrollo interno como externo.
- Se debe estandarizar el ciclo de vida del desarrollo de software en la CNE, logrando con ello los siguientes objetivos:
  - Definir actividades a llevarse a cabo en un proyecto de desarrollo de software.
  - Unificar criterios en la organización para el desarrollo de software.
  - Proporcionar puntos de control y revisión.

- Se deben estandarizar, los criterios de seguridad y calidad, que serán considerados, durante cada fase del proceso de desarrollo de sistemas de información.
- En cuanto al desarrollo de sistemas por terceros, se deben celebrar contratos, con las empresas proveedoras, que contengan cláusulas, que resguarden la propiedad intelectual para la CNE, y asimismo, aseguren, los niveles de confidencialidad de la información, en el proyecto respectivo.
- Se debe diferenciar, entre el encargado de celebrar y autorizar los contratos con terceros, de los que deben fiscalizar su cumplimiento.

## **6.2. Protección de servicios de aplicación en redes públicas - (Control A.14.1.2 NCh ISO 27001:2013)**

La información involucrada en los servicios de aplicación que pasan a través de redes públicas, se deberá proteger contra la actividad fraudulenta, la disputa de contratos y la información y modificación no autorizada.

El software, datos y otra información que requiera un alto nivel de integridad y que estén accesibles públicamente se deben proteger por mecanismos adecuados. Los sistemas accesibles públicamente, se deben probar contra debilidades y fallas antes que la información esté disponible.

Debe haber un proceso de aprobación formal antes que la información esté accesible públicamente. Además, toda la entrada proveniente del exterior al sistema deberá ser verificada y aprobada.

Los sistemas electrónicos de edición, sobre todo aquellos que permiten la retroalimentación y el ingreso directo de información, se deben controlar con cuidado de modo que:

- La información se obtenga en cumplimiento con toda la legislación sobre protección de datos.
- El ingreso de la información a, y el procesamiento por, el sistema de edición será procesado completamente y con exactitud de manera oportuna.
- La información sensible será protegida durante la recolección, procesamiento y almacenamiento.
- El acceso al sistema de edición no debe permitir el acceso no planeado a redes las cuales se conecta el sistema.

## **6.3. Entorno de Desarrollo Seguro - (Control A.14.2.6 NCh ISO 27001:2013)**

	Política Desarrollo Seguro Página: 6 de 8 Versión: 1 Fecha Versión: 04 de septiembre de 2019
---	--

El Entorno de Desarrollo Seguro en la CNE considera los aspectos de seguridad de la información en:

- La fase de diseño de los proyectos de desarrollo de software y sistemas.
- El entorno de desarrollo, identificado como el conjunto de procesos y herramientas que se utilizan para desarrollar un código fuente o programa.
- El ciclo de desarrollo de software, en particular:
  - Seguridad en la metodología de desarrollo de software.
  - Pautas de codificación segura para cada lenguaje de programación que se utiliza.
- El establecimiento de puntos de verificación de seguridad dentro de los hitos de los proyectos de desarrollo de software y sistemas.
- Los repositorios de información asociados a los proyectos de desarrollo de software y sistemas.
- El manejo del control de versiones de los proyectos de desarrollo de software y sistemas.
- La capacidad del equipo de desarrollo para:
  - Conocer las condiciones de seguridad de las aplicaciones desarrolladas.
  - Evitar, encontrar y resolver las vulnerabilidades de los desarrollos de software y sistemas.
- Los desarrollos ejecutados por personal externo y las condiciones contractuales con las empresas prestadoras de este servicio.

#### **6.4. Pruebas de seguridad del sistema - (Control A.14.2.8 NCh ISO 27001:2013)**

Todos los sistemas de información, durante su fase de desarrollo, se someterán a pruebas y verificaciones de seguridad, incluyendo un programa de actividades detallado, entradas de pruebas y los resultados esperados bajo una variedad de condiciones.

Se recomienda, que las pruebas del sistema, incluyan, entre otros aspectos; instalación, volumen, rendimiento, almacenamiento, configuración, funcionalidad, seguridad, recuperación ante errores, como mínimo.

Dentro de lo posible, las pruebas, deben ser realizadas, almacenando criterios y datos de pruebas en archivos, de modo de permitir la verificación rápida y repetitiva.

#### **6.5. Pruebas de aprobación del sistema - (Control A.14.2.9 NCh ISO 27001:2013)**

Las pruebas de aceptación de sistemas, se deberán realizar en un entorno de prueba (QA), de tal forma que permita, garantizar que el sistema no introducirá vulnerabilidades al entorno de la organización. Asimismo, se debe asegurar, que las pruebas sean confiables.

Para realizar las pruebas de aceptación de sistemas, se podrán utilizar las herramientas automatizadas disponibles en el mercado, como las herramientas de análisis de códigos o los escáneres de vulnerabilidad y debería verificar la remediación de los defectos relacionados con la seguridad.

#### **6.6. Separación de entornos de desarrollo, prueba y operacionales - (Control A.12.1.4 NCh ISO 27001:2013)**

Los ambientes de desarrollo, prueba y producción, estarán separados preferentemente en forma física.

Para el caso de los desarrollos externalizados, se definirán y documentarán en los Términos de Referencia, detalladamente, las reglas y pasos para la transferencia de software, desde el estado de desarrollo hacia el estado productivo. Estas reglas deben considerar al menos los siguientes lineamientos:

- Ambiente de Desarrollo (Proveedor)
- Ambiente de Pruebas (Proveedor)
- Ambiente Pre-Producción (CNE)
- Ambiente Producción (CNE)

Al final del proyecto, se debe hacer traspaso del repositorio del proyecto a la CNE.

En el caso de los desarrollos internos se debe considerar:

- Ambiente de Desarrollo (Local)
- Ambiente Pre-Producción (CNE)
- Ambiente Producción (CNE)

### **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.