Plan de Ciberseguridad

Septiembre 2019

ÍNDICE

1. Contexto

[1] Contexto [2] Plan de Ciberseguridad

Riesgo de ataques externos

Riesgos Internos – Ingeniería social

Rol Principal del Coordinador

Preservar la seguridad y continuidad del suministro eléctrico - conforme con la normativa vigente.

Riesgo conocido de ciberseguridad

Evento de ciberseguridad podría afectar en forma importante el suministro eléctrico.

Riesgo – falta de gestión de proveedores

Acciones

Mitigar riesgos endógenos – personas, procesos y plataformas tecnológicas del Coordinador.

Mitigar riesgos exógenos – procesos, instalaciones y plataformas externas al Coordinador.

1. Contexto

[1] Contexto [2] Plan de Ciberseguridad

Solicitudes desde la Autoridad a la fecha

Instancias	Alcance
Requerimientos de la SEC	• *Recopilar información pendiente de enviar por parte de Coordinados, a un requerimiento de la SEC – emisión de encuesta.* • *Definir requisitos mínimos de resguardo de la seguridad cibernética aplicables al sector eléctrico.* • *Evento previsible (como la ciberseguridad) no constituye fuerza mayor* • *Instruir medidas inmediatas a los Coordinados.*
Ministerio del Interior No Formalizado	*Constituir CSIRT de la Industria Eléctrica.*

CSIRT Ministerio del Interior y Seguridad Pública – Gobierno de Chile → CSIRT Equipo de Respuesta ante Incidentes de Seguridad Informática → CSIRT Sectoriales

CSIRT Computer Security Incident Response Team

1. Contexto

[1] Contexto [2] Plan de Ciberseguridad

Cuestionario de Riesgo, Seguridad y continuidad de negocio

Del levantamiento realizado se determina que cada Coordinado realice:

- Autoevaluación de riesgos y gestión de los riesgos que hayan sido identificados.
- Implementación de medidas de seguridad de la información, registro de eventos y monitoreo permanente.
- Implementación de controles y formalización de procedimientos relacionados.
- Definición e implementación de planes de continuidad de negocio (BCP) y de recuperación ante desastre (DRP).

Detectar, prevenir, responder, concientizar y compartir

2. Plan de Ciberseguridad

[1] Contexto **[2] Plan de Ciberseguridad**

PROPOSITO: establecer una instancia de trabajo con la Autoridad y Coordinados, para efectos de cumplir los siguientes objetivos:

1. Definir e implementar en forma urgente requerimientos mínimos que permita acortar brechas en el corto plazo

2. Definir plan de trabajo para adoptar la norma NERC-CIP en el mediano plazo.

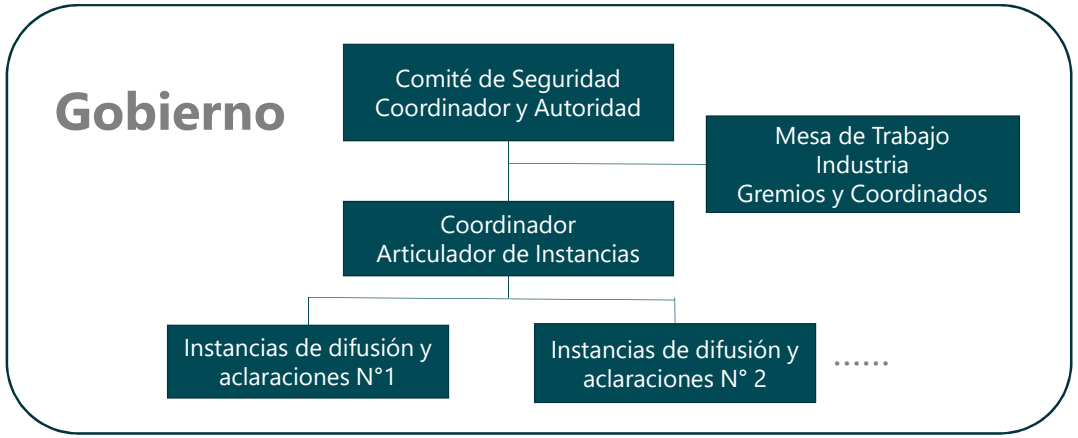
- Estrategia – Comité de Seguridad (Ministerio, CNE y SEC)
  - Propósito y Visión
  - Organización - Gobierno
  - Objetivos , Plan de alto nivel (CP y MP) (definir el qué)
  - Responsabilidades, medidas de control y sanciones

- Corto Plazo – Implementación requerimientos mínimos "urgentes"
  - Levantamiento de línea base – Estado actual
  - Planificar e implementar medidas – Compromisos
  - Mesa de trabajo para informar y aclarar medidas

- Propuesta de Mediano plazo – Implementar Estándar
  - Priorización de Capítulos de NERC-CIP/27002 y adecuaciones
  - Plan de implementación - Compromisos
  - Medidas de control - sanciones

2. Plan de Ciberseguridad

[1] Contexto **[2] Plan de Ciberseguridad**



Etapa 1: Definición e implementación de estándar

- Requerimientos mínimos urgentes
- Implementación de Estándar

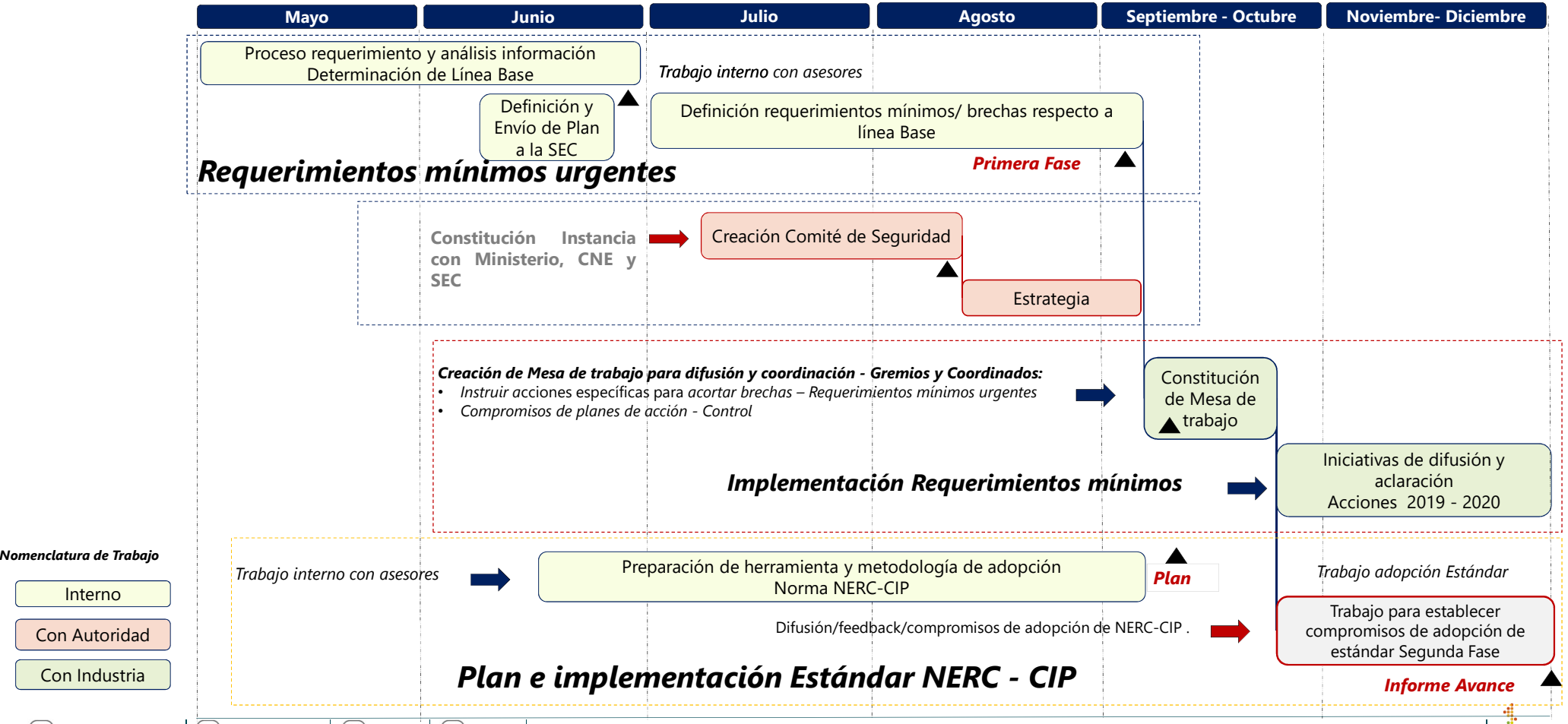
Etapa 2: En régimen – reporte y actualizaciones estándar

Alcance

- *Coordinación de esfuerzos*
- *Requerimiento de información*
- *Revisión de información*
- *Determinación de Brechas*
- *Estándar, planes y compromisos*
- *Seguimiento de implementación*
- *Informes periódicos de cumplimiento*
- *Ejecución de medidas por incumplimiento*

2. Plan de Ciberseguridad

[1] Contexto **[2] Plan de Ciberseguridad**



2. Requerimientos urgentes

[1] Contexto [2] Plan de Ciberseguridad **[3] Requerimientos urgentes**

Requerimientos mínimos de ciberseguridad

R1: Designar un Responsable de Seguridad/Ciberseguridad
R2: Diagrama de red
R3: Inventario de Sistemas
R4: Implementación y Revisión de las reglas de comunicaciones
R5: Contar con una solución de Antivirus/Antimalware
R6: Instalación de parches de seguridad
R7: Aplicar configuración segura/hardening en la Infraestructura Tecnológica
R8: Control de Acceso a sistemas
R9: Cambio de contraseñas / Política de contraseña segura
R10: Acceso Físico
R11: Política de Respaldos
R12: Educación y concientización en seguridad
R13: Plan de seguridad y respuesta a incidentes de seguridad

- Definición de procedimientos
- Reporte de cumplimiento de requerimientos (Estandarizado)
- Periodicidad de reportabilidad a definir
- Informado por Coordinados a SEC con copia al Coordinador

Nota: Requerimientos mínimos de ciberseguridad se encuentra alineados con el estándar NERC-CIP que se prevé implementar

2. Requerimientos urgentes

[1] Contexto [2] Plan de Ciberseguridad **[3] Requerimientos urgentes**

Mensajes finales:

- El riesgo y las amenazas a las que están expuestas las organizaciones, así como la efectividad de un ataque cibernético, no dependen del tamaño o función de la empresa. Un ataque específico puede afectar a todo el sistema eléctrico.

- Los costos de reparar los efectos de un ataque de ciberseguridad superar en forma importante la inversión para prevenirlos.

- Es urgente instaurar una cultura de seguridad para que las medidas de mitigación de riesgos sean valoradas aun cuando generen esfuerzo o incomodidades.

- Las medidas de seguridad deben ser impulsadas por la alta dirección de las organizaciones y cumplidas por todos sin excepciones.

- El tratamiento de la seguridad es una tarea permanente que requiere una constante evolución.


COORDINADOR
ELÉCTRICO NACIONAL
GRACIAS
Septiembre 2019