Innovarpel 2023

Digitalización y Ciberseguridad en la Industria del Oil&Gas

Hotel Colón | Quito, Ecuador

21 y 22 de noviembre de 2023

ORGANIZA

arpel

REALIZA

SEMINARIUM

Avance en la Ciberseguridad OT de ENAP

Carolina Melo Molina

Patricia Alvarez Tapia

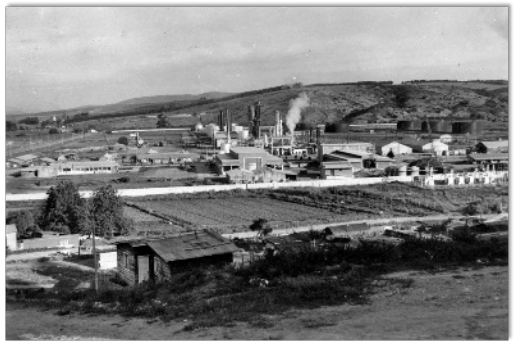
Jefas de División Aplicaciones

Refinería Aconcagua y Refinería Bío Bío

Algo de historia de ENAP

•En **Diciembre 29 de 1945**, el primer pozo petrolero fue descubierto en Chile, su ubicación fué en **Springhill en el area de Magallanes**.

•La E**mpresa Nacional del Petróleo (ENAP)** fue fundada el **19 de Junio de 1950**.



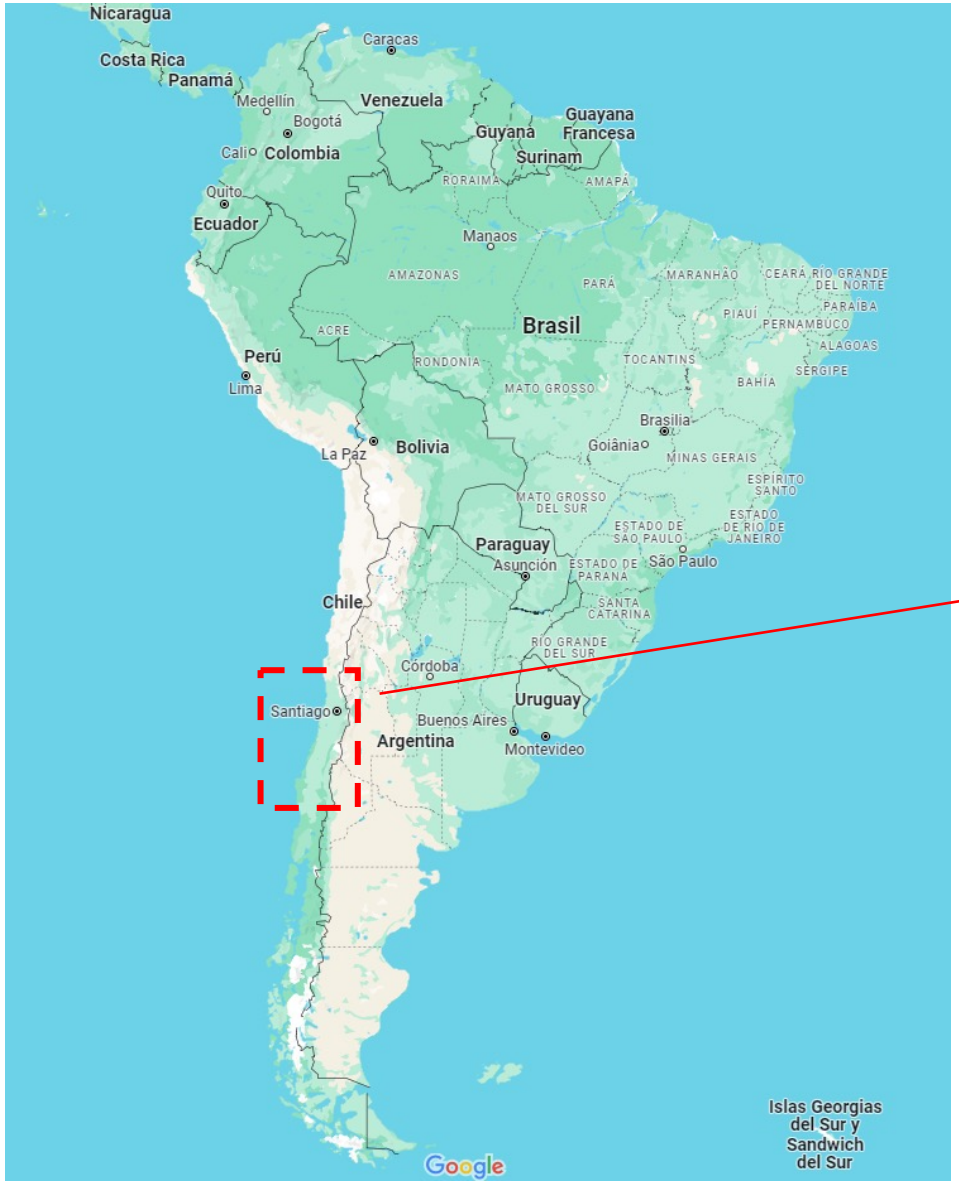
•ENAP **Refinerías Aconcagua** (ERA) fue inagurada en **1955**.

•ENAP **Refinerías Bío Bío** (ERBB) fue inagurada en **1966**.

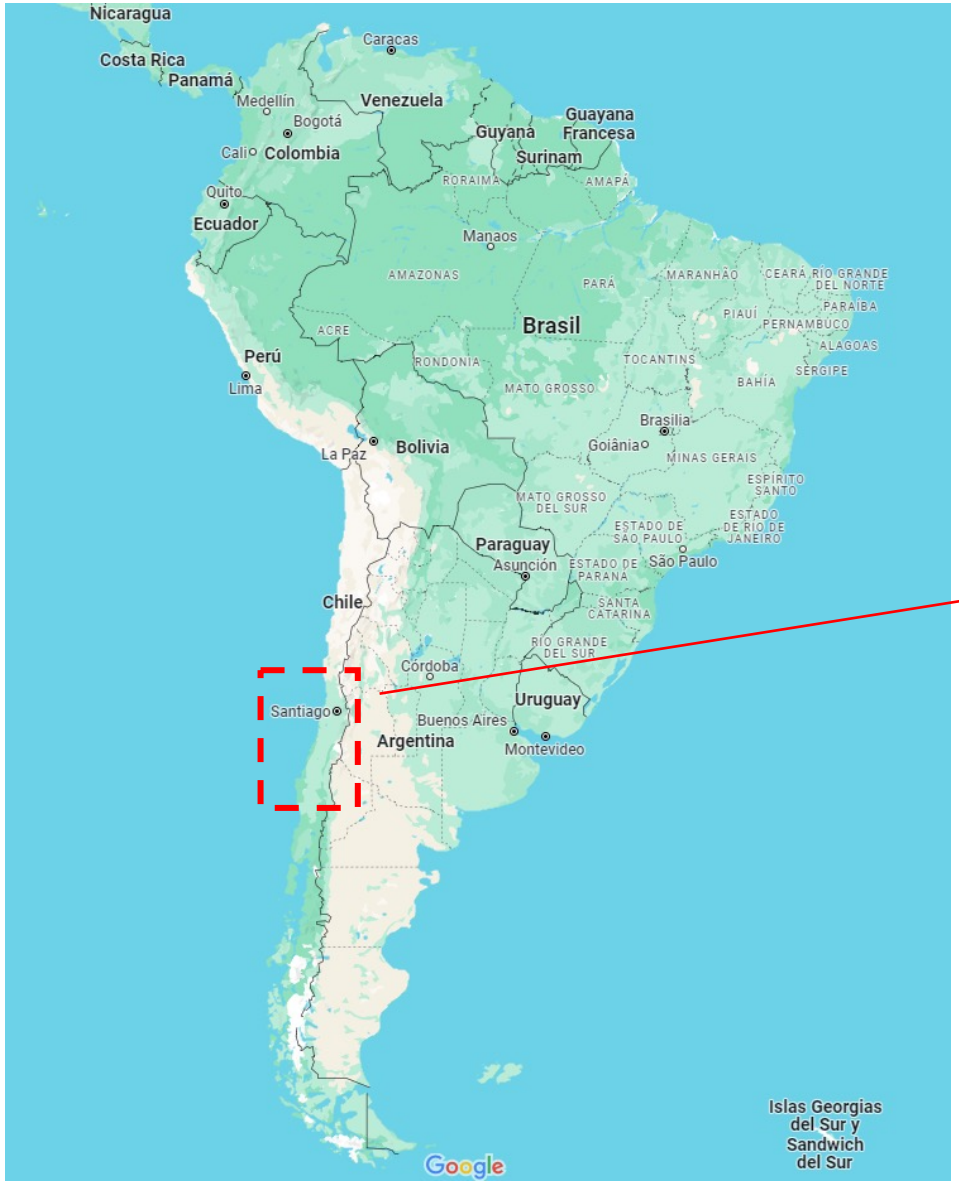
•En **1981** ENAP ingresó al negocio **Logístico**, con plantas de almacenamiento de combustibles líquidos y gaseosos en **Maipú, San Fernando y Linares**.

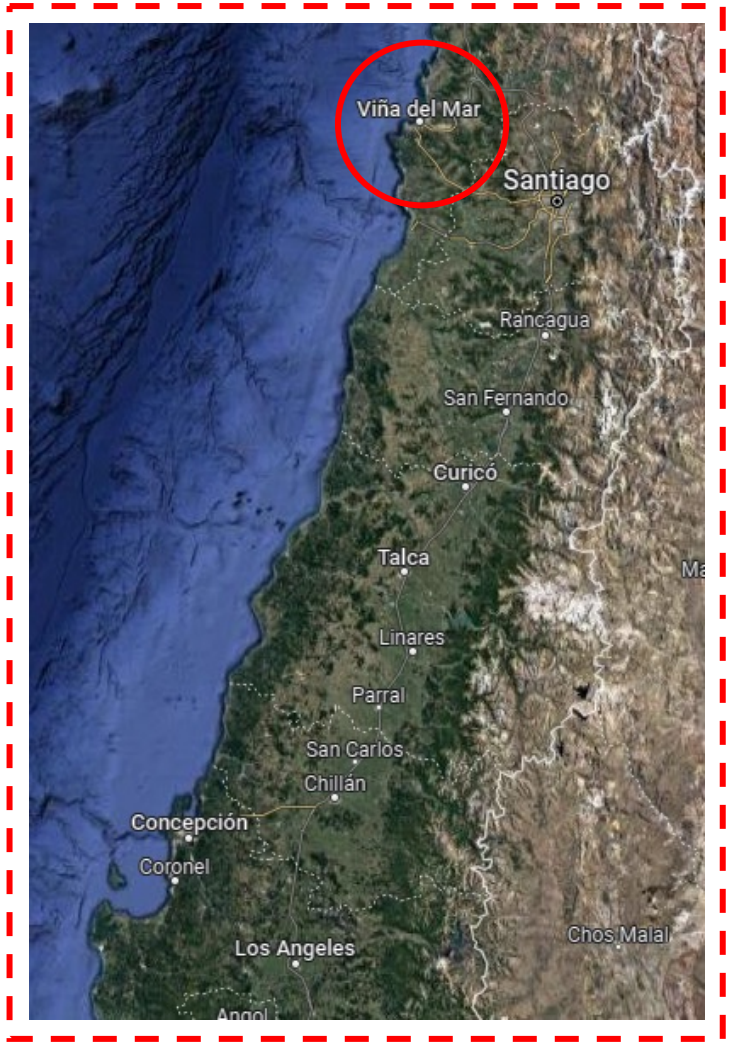
•El **01 de Enero de 2004**, las Refinerías se fusionaron en una sola unidad de negocios llamada **ENAP Refinerías S.A.**

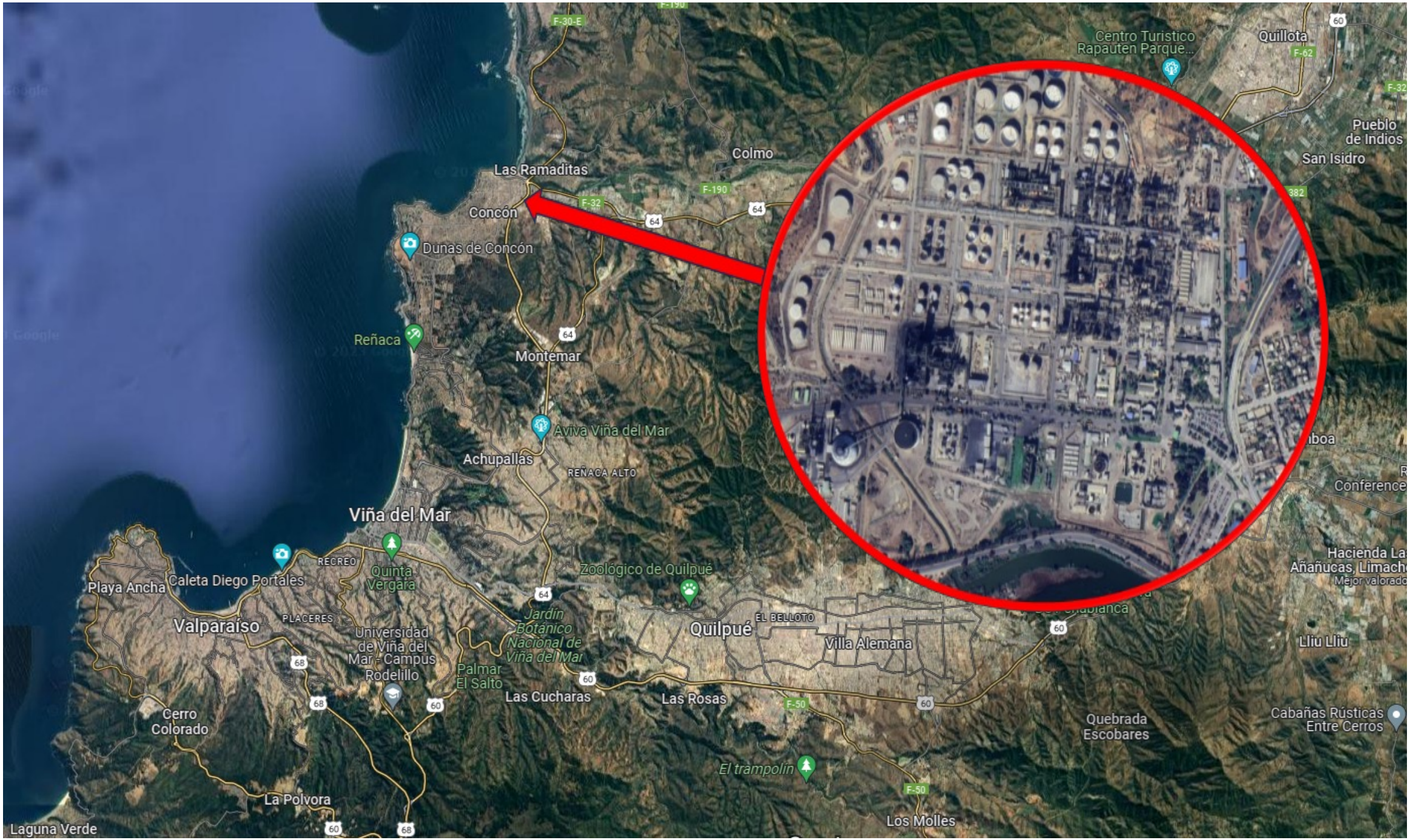
Distribución de Refinerías



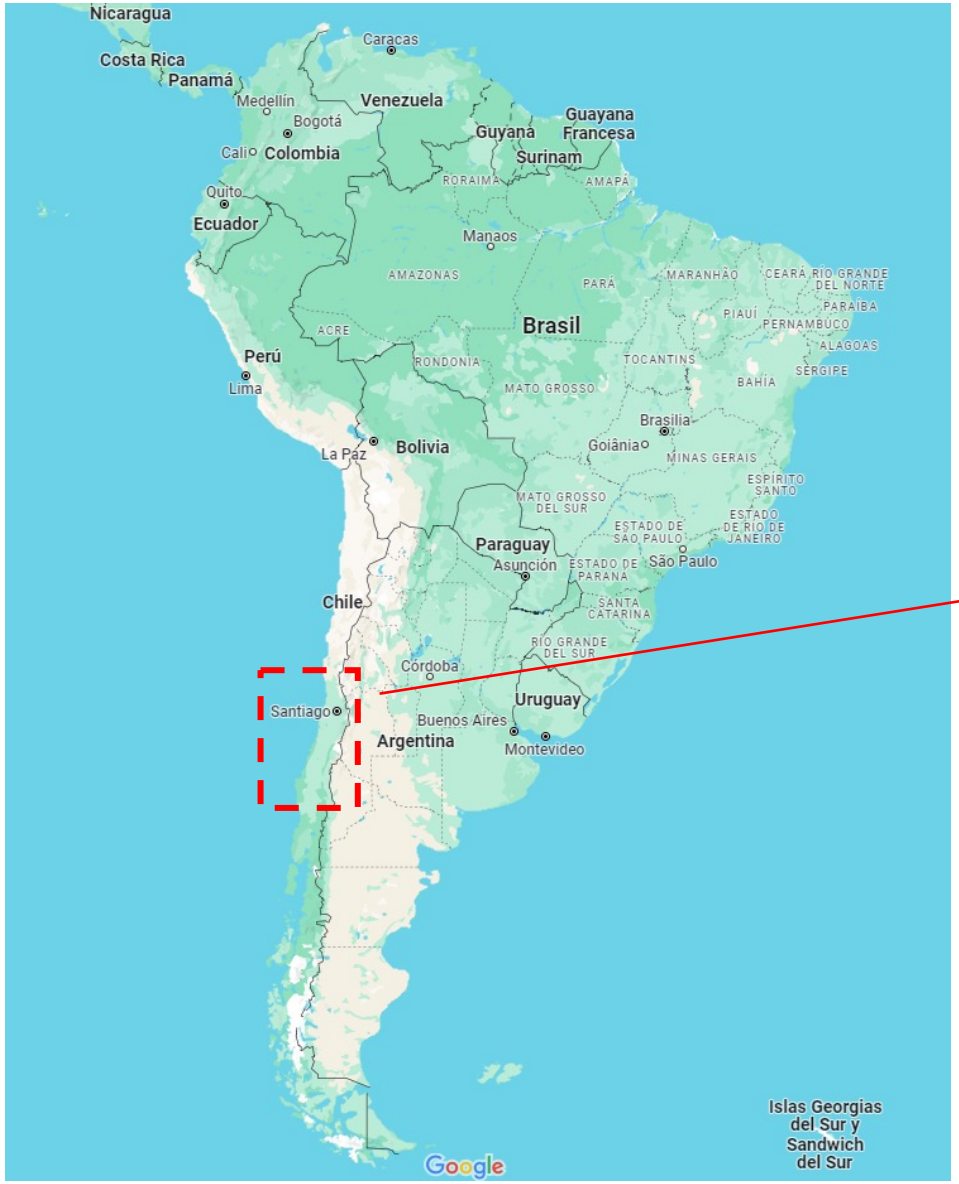
Distribución de Refinerías - Refinería Aconcagua

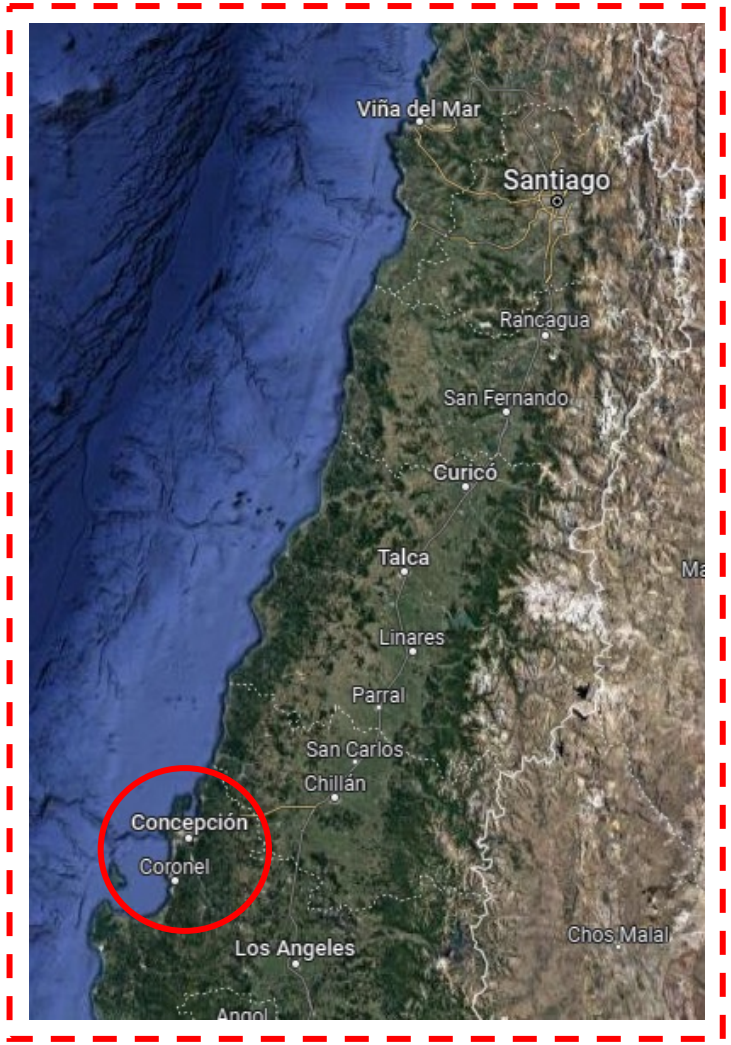





Centro Turistico Rapaúten Parque...
Quillota
Pueblo de Indios
San Isidro
Colmo
Las Ramaditas
Concón
Dunas de Concón
Reñaca
Montemar
Aviva Viña del Mar
Achupallas
REÑACA ALTO
Viña del Mar
Zoológico de Quilpué
Quinta Vergara
Caleta Diego Portales
Playa Ancha
Valparaíso
PLACERES
Universidad de Viña del Mar - Campus Rodelillo
Jardín Botánico Nacional de Viña del Mar
Palmar El Salto
Las Cucharas
Las Rosas
Quilpué
EL BELLOTO
Villa Alemana
Lliu Lliu
Cerro Colorado
La Polvora
Laguna Verde
El trampolín
Los Molles
Quebrada Escobares
Cabañas Rústicas Entre Cerros
Hacienda La Añañucas, Limache
Mejor valorado

Distribución de Refinerías - Refinería Bio Bío

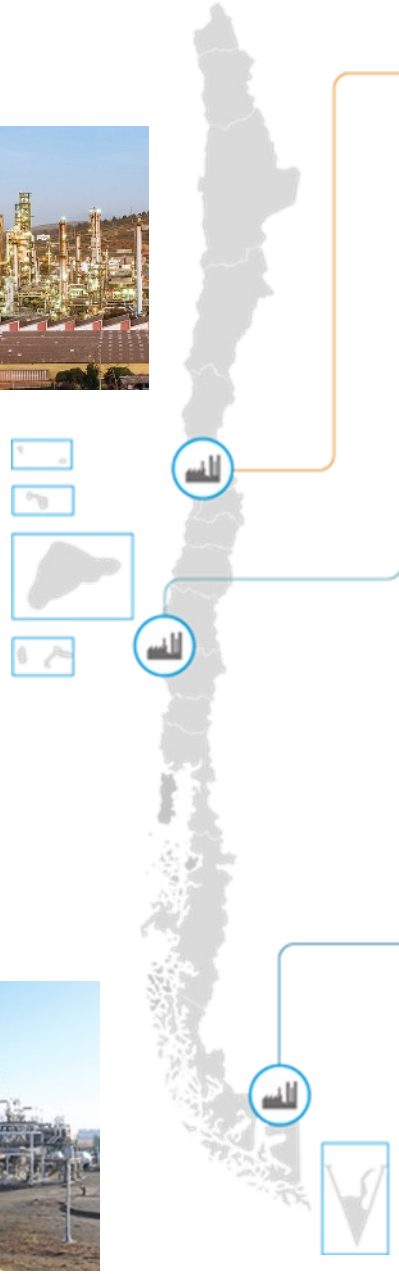





Cocholgüe
Tome
Bularco
Pissis
El Refugio
Rafael
Candelaria
Tumbes
Taiguen
El Laurel
Punta de Parra
ÑUBLE
BÍO BÍO
Ranquil
Litrinal
Lirquén
Talcahuano
Penco
Bellavista 4
Cancha de los Litres
El Quillay
Huachipato
Penablanca
Caleta Lenga
El Rosal
Peñuelas
Pantanillo
Concepción
San Jorge
Rincónada
Panicalco
San Pedro de la Paz
San Antonio de Cuda
El Guindo
Parque Nacional Nonguén
Talcamo
La Esperanza
Las Lagunas (001)
Pichaco
Copiulemu
Rodolmo
Cerro Alto
San José(001)
Manquimavida
El Aguila
Chiguayante
Pachagua
Lucay

Distribución de Refinerías

ENAP dispone de tres refinerías distribuidas a lo largo del país



REFINERÍA ACONCAGUA

Puesta en Servicio	12 de Noviembre de 1955
Ubicación	Comuna de Concón, Región de Valparaíso, Chile.
Productos	Gas licuado, gasolinas de variado octanaje, kerosenes doméstico y de aviación, diesel, solventes, fuel olis, pitch asfálticos y carbón de petróleo.
Capacidad de Refinación	104.000 barriles día de petróleo crudo.
Principales Instalaciones	• Complejo Industrial de Refinería Aconcagua • Terminal Marítimo de Quintero • Terminal Vinapu - Isla de Pascua

REFINERÍA BIO BÍO

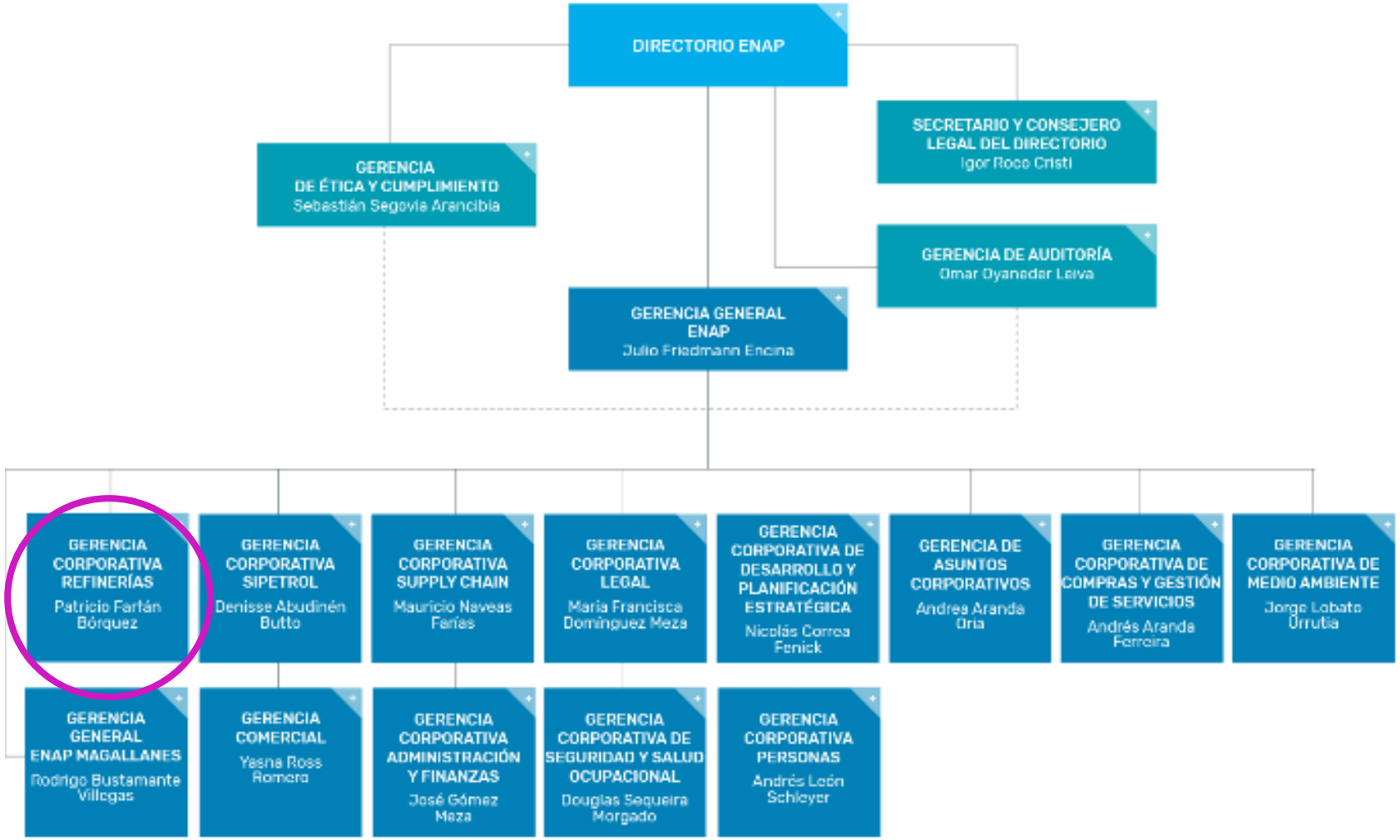
Puesta en Servicio	29 de Julio de 1966
Ubicación	Comuna de Hualpén, Región del Biobío, Chile.
Productos	Etileno, propileno, propano butano, gasolinas kerosene, doméstico, kerosene de aviación, petróleos diesel, petróleos combustibles, pinch asfáltico, Coke, sulfhidrato de sodio, Azufre.
Capacidad de Refinación	116.000 barriles día de petróleo crudo.
Principales Instalaciones	• Complejo Industrial de Refinería Bío Bío • Terminal Marítimo San Vicente

REFINERÍA GREGORIO

Ubicación	Comuna de San Gregorio, Región de Magallanes y Antártica Chilena.
Productos	Petróleo diesel, kerosén de aviación y nafta.
Mercado	Abastece de combustibles a la Región de Magallanes y al resto de las refinerías de ENAP.
Capacidad de Refinación	15.700 barriles día de petróleo crudo.
Principales Instalaciones	• Refinería y Terminal Multiboyas de Gregorio • Planta de combustibles y patio de carga en Cabo Negro.

Empresa Nacional del Petóleo (ENAP)

ENAP



Ruta Ciberseguridad Tecnología de la Operación ENAP

2008 → 2014 → 2015 - 2016 → 2017 → 2018 → 2020 → 2021 → 2022 → 2023

Ruta Ciberseguridad Tecnología de la Operación ENAP

Levantamiento de redes:
Diagnóstico
Plan de acción

2008 → **2014** → **2015 - 2016** → **2017** → **2018** → **2020** → **2021** → **2022** → **2023**

Ruta Ciberseguridad Tecnología de la Operación ENAP

Levantamiento de redes:
Diagnóstico
Plan de acción

2008 → 2014 → 2015 - 2016 → 2017 → 2018 → 2020 → 2021 → 2022 → 2023

Ruta Ciberseguridad Tecnología de la Operación ENAP

Levantamiento de redes:
Diagnóstico
Plan de acción

2008 → **2014**

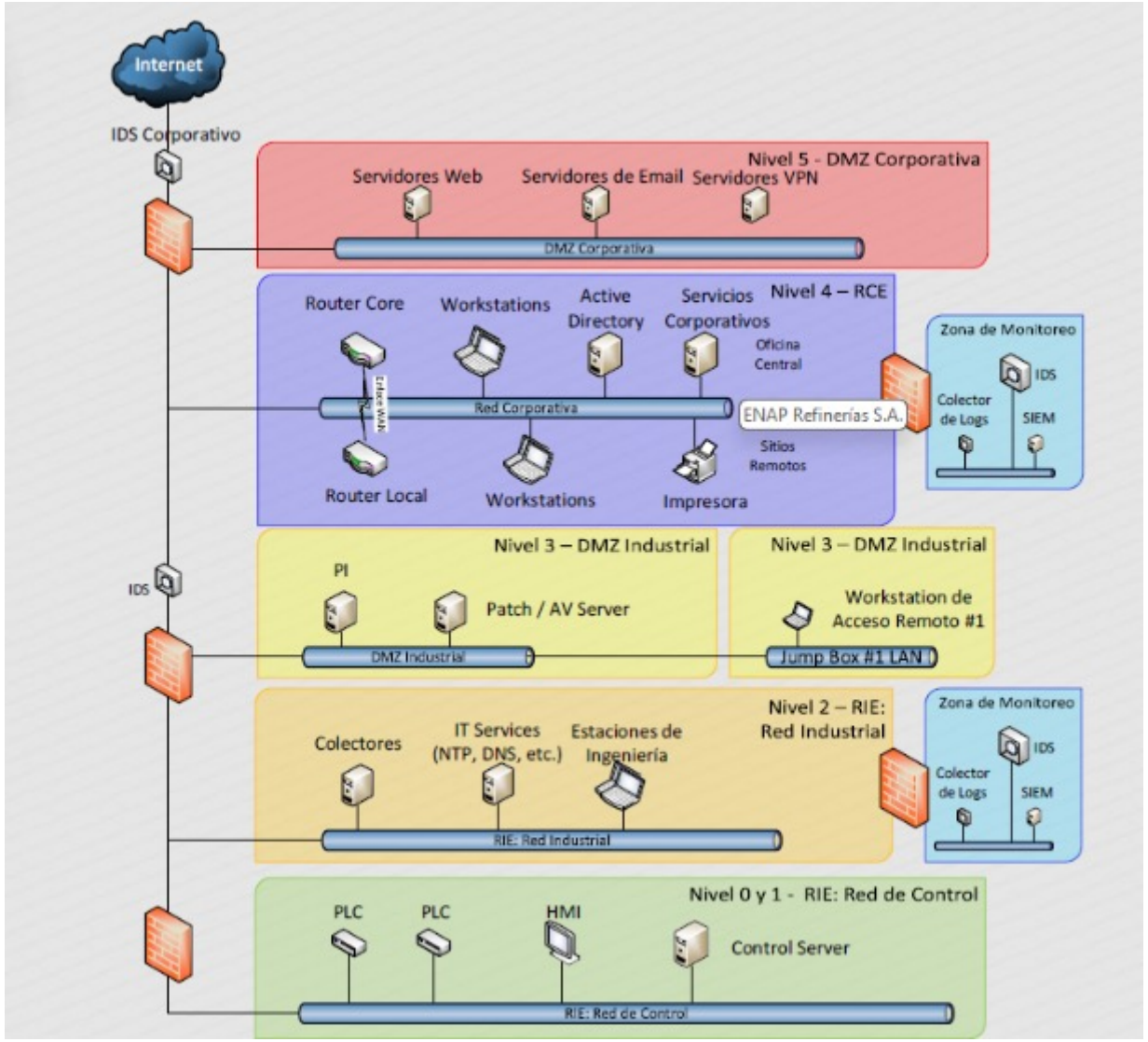
Trabajo colaborativo entre
IT/OT para realizar
una Segregación de Redes

2015 - 2016

2017 → **2018** → **2020** → **2021** → **2022** → **2023**

Ruta Ciberseguridad Tecnología de la Operación ENAP

Modelo de Referencia



Ruta Ciberseguridad Tecnología de la Operación ENAP

Levantamiento de redes:
Diagnóstico
Plan de acción

2008 → **2014**

Trabajo colaborativo entre
IT/OT para realizar
una Segregación de Redes

2015 - 2016

La Dirección Corporativa de Integridad de Sistema TI de la época, lideró el proyecto para la adopción del marco de NIST y la ISA99/IEC 62443.

2017 → **2018** → **2020** → **2021** → **2022** → **2023**

Ruta Ciberseguridad Tecnología de la Operación ENAP

Levantamiento de redes:
Diagnóstico
Plan de acción

2008

2014

Trabajo colaborativo entre
IT/OT para realizar
una Segregación de Redes

2015 - 2016

La Dirección Corporativa de Integridad de Sistema TI de la época, lideró el proyecto para la adopción del marco de NIST y la ISA99/IEC 62443.

Ransomware
Wannacry
Redes Industriales
Redes de control

2017 **2018** **2020** **2021** **2022** **2023**

Ruta Ciberseguridad Tecnología de la Operación ENAP

Levantamiento de redes:
Diagnóstico
Plan de acción

2008

2014

Trabajo colaborativo entre
IT/OT para realizar
una Segregación de Redes

2015 - 2016

La Dirección Corporativa de Integridad de Sistema TI de la época, lideró el proyecto para la adopción del marco de NIST y la ISA99/IEC 62443.

Directora Seguridad de la Información

Comité de Ciberseguridad IT-OT

2017 **2018** **2020** **2021** **2022** **2023**

Ruta Ciberseguridad Tecnología de la Operación ENAP

Levantamiento de redes:
Diagnóstico
Plan de acción

2008

2014

Trabajo colaborativo entre
IT/OT para realizar
una Segregación de Redes

2015 - 2016

La Dirección Corporativa de Integridad de Sistema TI de la época, lideró el proyecto para la adopción del marco de NIST y la ISA99/IEC 62443.

2017

Directora Seguridad de la Información

Comité de Ciberseguridad IT-OT

2018

Incorporación del Riesgo de Ciberseguridad

Estándares de Ciberseguridad para el sector eléctrico

2020

2021

2022

2023

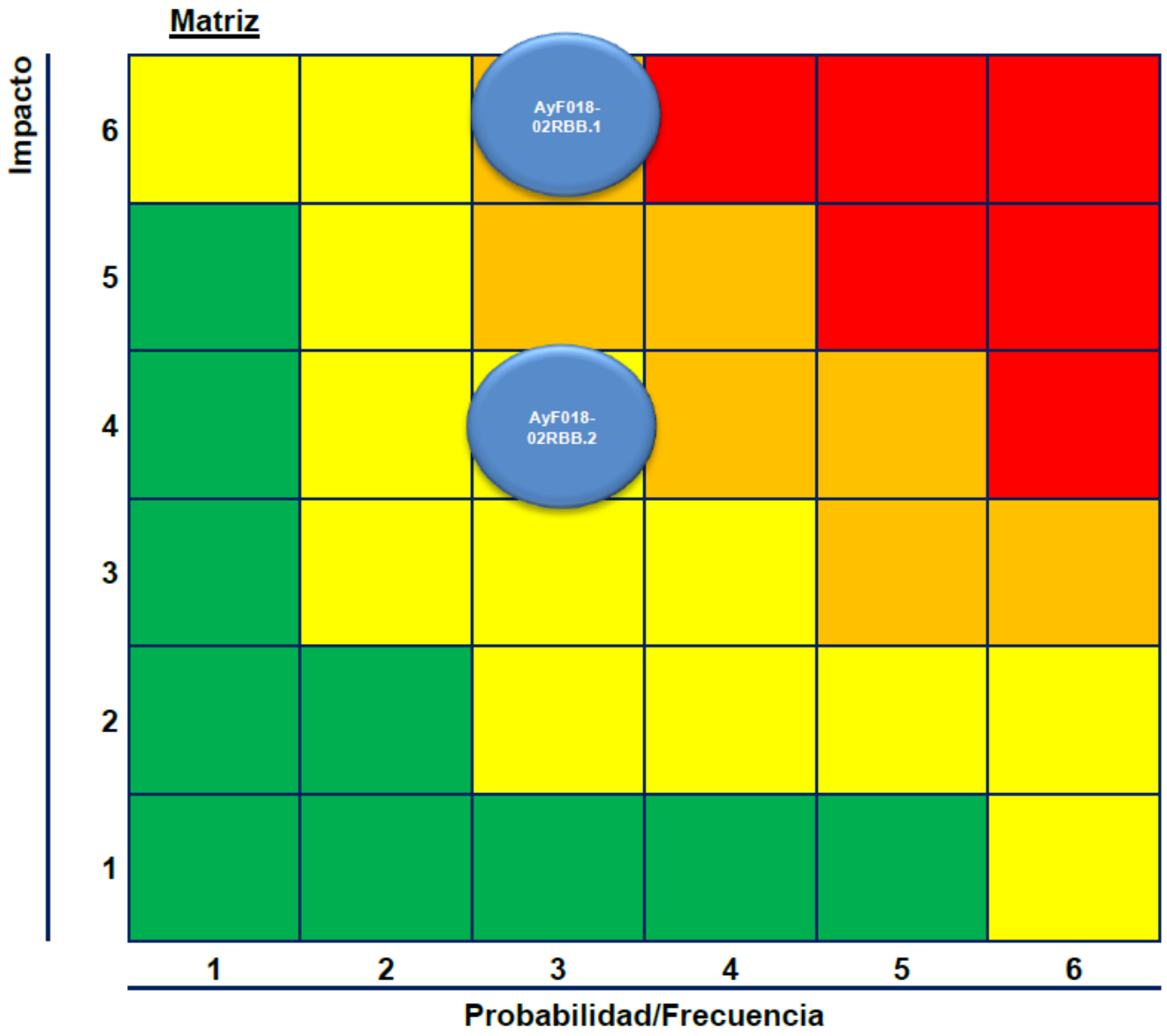
Incorporación del Riesgo de Ciberseguridad

Modelo de Gestión de Riesgos de ENAP

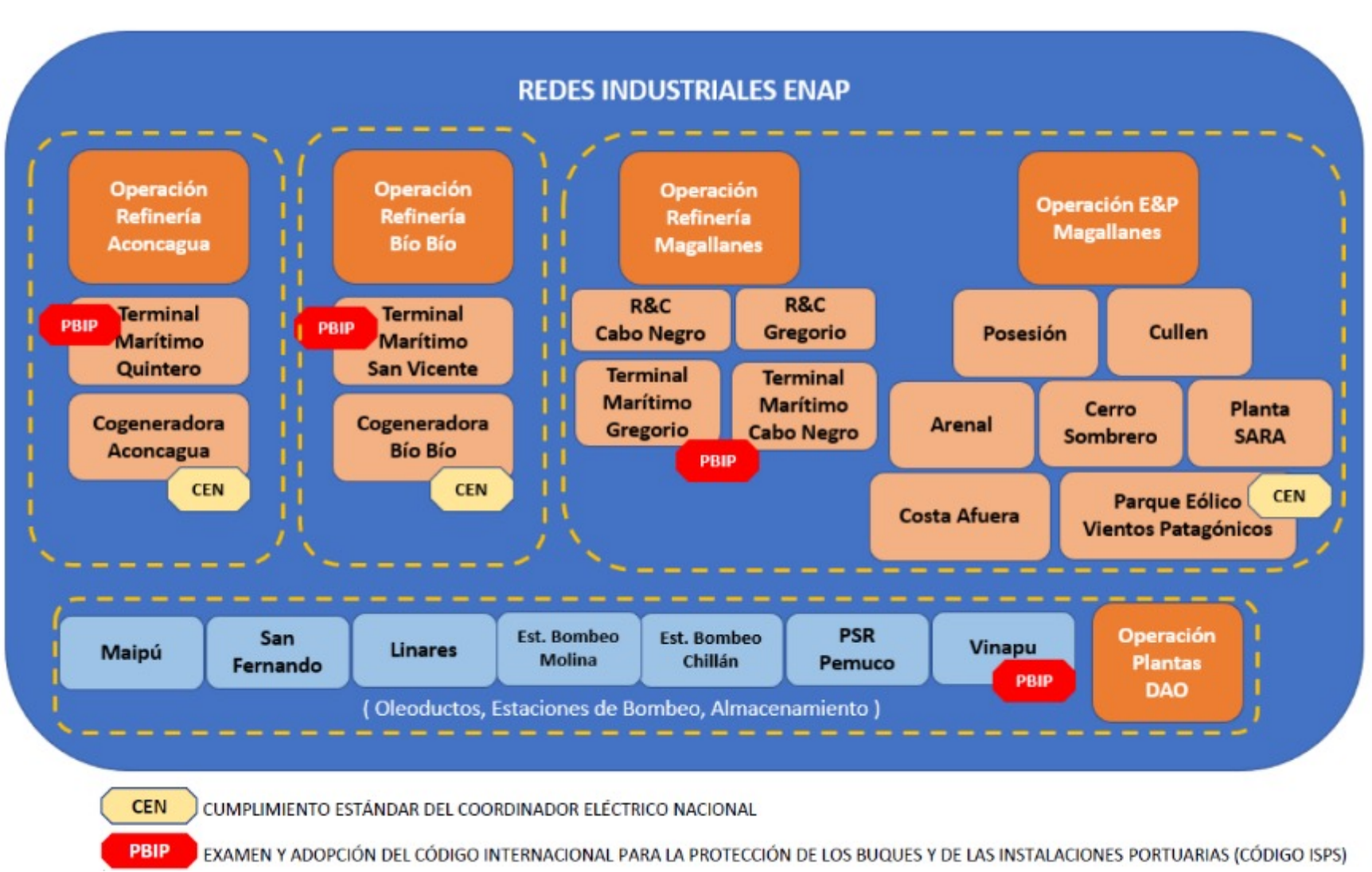
Matriz de Impacto

	Salud y Seguridad	Medio Ambiente	Financiero	Reputación	Licencia para Operar	Continuidad Operacional
6	Múltiples fatalidades y/o múltiples lesionados graves con incapacidad permanente significativa.	Impacto Ambiental Permanente o Prolongado sobre el área afectada: Daño Permanente al ecosistema o extinción de especies. Daño extensivo a un área ambientalmente sensible con una recuperación mayor a 5 años.	Desde: • 400 MM evento único	• Intervención de la compañía por parte de la autoridad. • Rebaja en la calificación de riesgos de ENAP, y requerimientos de tenedores de deuda e inversionistas • Atención crítica de medios nacionales y cobertura negativa en prensa internacional.	• Clausura/suspensión permanente para operar el Activo/ Concesión • Infracción catastrófica de la Ley /penas privativas de libertad para ejecutivos o representantes de la empresa/ disolución o cancelación de la persona jurídica	• Quiebre de stock que genera desabastecimiento de CL y/o GN Zonas Geográficas, Clientes Distribuidoras, Gasoductos, Clientes Mayoristas, Minoristas, Industriales, GNL Movil. • Daño crítico a los activos, operación se interrumpe por más de 3 meses. (Evento tipificado CL2 o GN2 por Of. Ord. N° 354 de 2019 del Min. Energía)
5		Impacto Ambiental Severo: Daño extensivo con afectación de un área sensible con recuperación mayor a 1 año y menor a 5 años, o a un área no sensible con recuperación a largo plazo (mayor a 5 años).	Desde: • 200 MM evento único	• Involucramiento de autoridades nacionales (p. ej., Subsecretario del Interior) • Caída sustantiva en rankings/mediciones de reputación (externas e internas). Preocupación de stakeholders internacionales • Atención crítica de medios de comunicación en el mediano y largo plazo (>1 año)	• Clausura/suspensión temporal para operar el Activo/Concesión • Infracción grave de la Ley, con responsabilidad penal de persona jurídica y natural/ Inicio de procesamiento a ejecutivos y representantes de la empresa. Pérdida total de beneficio fiscales. • Vulneración de Derechos Fundamentales de los Trabajadores.	• Interrupción de suministro a clientes de CL por más de 5 días y/o a clientes de GN por un volumen superior al 100% programado para el día. • Daño mayor en los activos, operación se interrumpe entre semana y 3 meses. (Evento tipificado CL2 o GN2 por Of. Ord. N 354 de 2019 del Min. Energía)
4	• 1 fatalidad • 1 lesionado grave con incapacidad permanente significativa.	Impacto Ambiental Grave: Afectación de un área sensible con recuperación mayor a 3 meses y menor a un año, o afectación de un área no sensible con recuperación mayor a 6 meses y menor a un año	Desde: • 50 MM evento único	• Debilitamiento manifiesto del ambiente de control interno de los procesos de negocio (Inobservancia del marco normativo interno). • Acciones organizadas de stakeholders (p.ej. campañas de denuncia, cuestionamientos de sindicatos) • Atención crítica de medios regionales y nacionales.	• Inicio de proceso de sanción (Penal, Civil, Administrativo). • Investigación por parte de reguladores o fiscalías por posible trasgresión a Ley 20.393. Pérdida parcial de beneficio fiscales.	• Interrupción de suministro a clientes de CL en un período menor a 5 días y/o a clientes de GN por un volumen entre 40% y 100% programado para el día. • Daño moderado en los activos, operación se interrumpe entre 1 a 5 días. (Evento tipificado CL1 o GN1 por Of. Ord. N° 354 de 2019 del Min. Energía)
3	1 ACTP con lesiones graves de acuerdo a criterios de clasificación asumidos por ENAP (Suseso/Minsal). Exposición con efectos irreversibles a la salud.	Impacto Ambiental Mayor: Afectación real a la población adyacente, o de un área sensible con recuperación mayor a 2 semanas y menor a 3 meses, o de un área no sensible con recuperación en un periodo mayor a 1 mes y menor a 6 meses.	Desde: • 5 MM evento único	• Atención puntual por miembros del Gobierno Regional • Atención crítica de medios de comunicación regionales (p. ej., Radio, periódicos locales).	• Presentación de reclamos/denuncias por parte de stakeholders locales (ej: municipalidades, seremi, miembros del Gobierno Regional). • Transgresión o incumplimiento grave del ambiente de control interno de los procesos de negocio	• Reclamos y quejas de clientes por incumplimiento de especificaciones, volúmenes y/o fechas en la entrega de productos. • Daño menor en los activos, operación se interrumpe por unas horas dentro del turno de trabajo. (Evento tipificado CL0 o GN(por Of. Ord. N° 354 de 2019 del Min. Energía)
2	1 ACTP con lesión leve o moderado, Exposición con efectos reversibles a la salud.	Impacto ambiental Moderado: Afectación de un área sensible con recuperación inmediata menor a 2 semanas o de un área no sensible con recuperación inmediata (Menor a 4 semanas).	Desde: • 1 MM evento único	• Requerimiento de información de algún stakeholder (p.ej. vecino de la comunidad local) o medio local • Exposición potencial a redes sociales, pero sin visibilidad en prensa	• Resolución del problema totalmente interno, sin participación de autoridades • Sanciones administrativas menores	• Productos fuera de especificación que se requiere reprocesar, sin impacto en los clientes. • Daño leve en los activos, operación no se ve interrumpida.
1	1 ASTP con atención de primeros auxilios Síntomas o molestias a la salud de bajo nivel	Impacto ambiental Leve: Emisiones o descargas puntuales no detectables	Hasta: • 1 MM evento único	• Reclamos de terceros, sin evidencia formal en los registros de ENAP	• Desprolijidad administrativa en actividades de control interno	• Sin impacto en los activos, operaciones y especificaciones de los productos.

Incorporación del Riesgo de Ciberseguridad



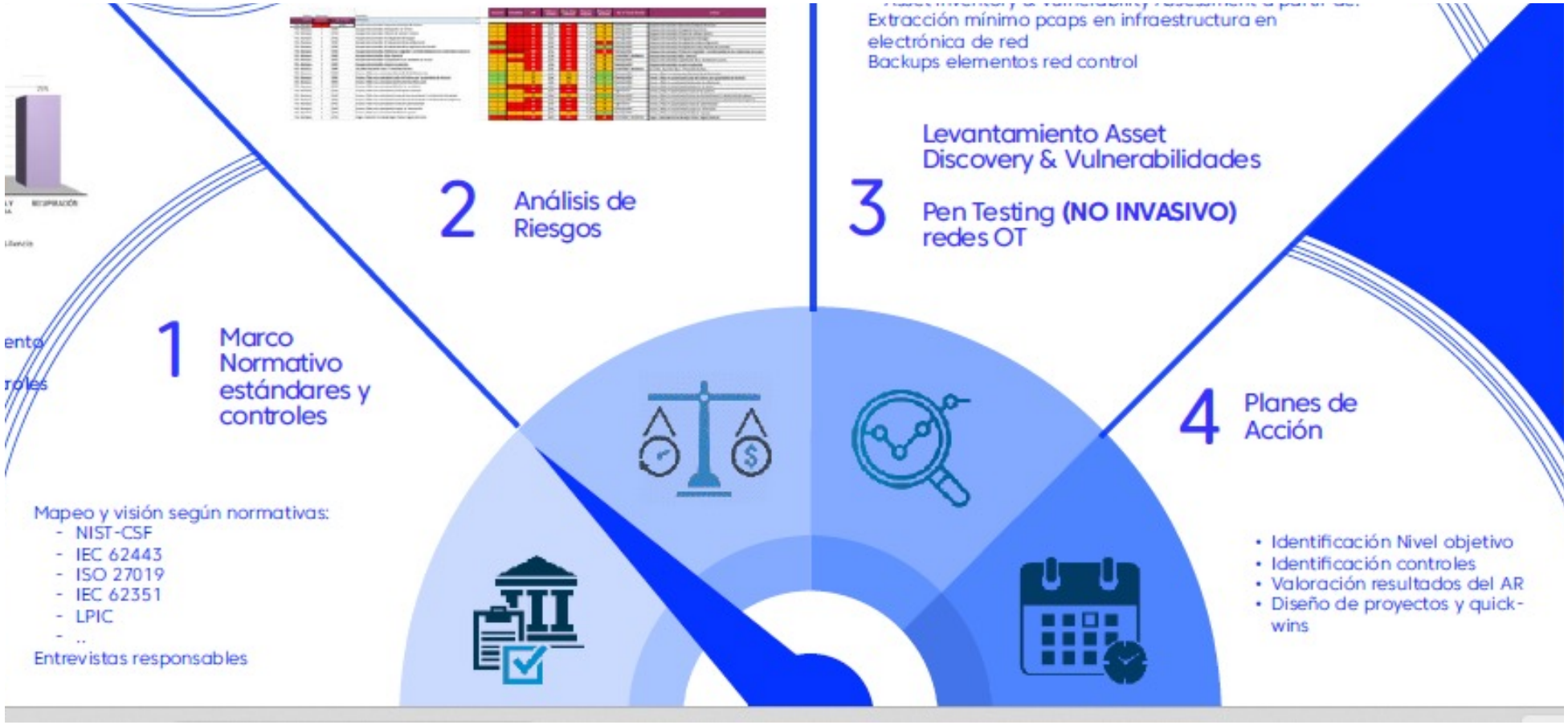
Alcance de Ciberseguridad OT de ENAP



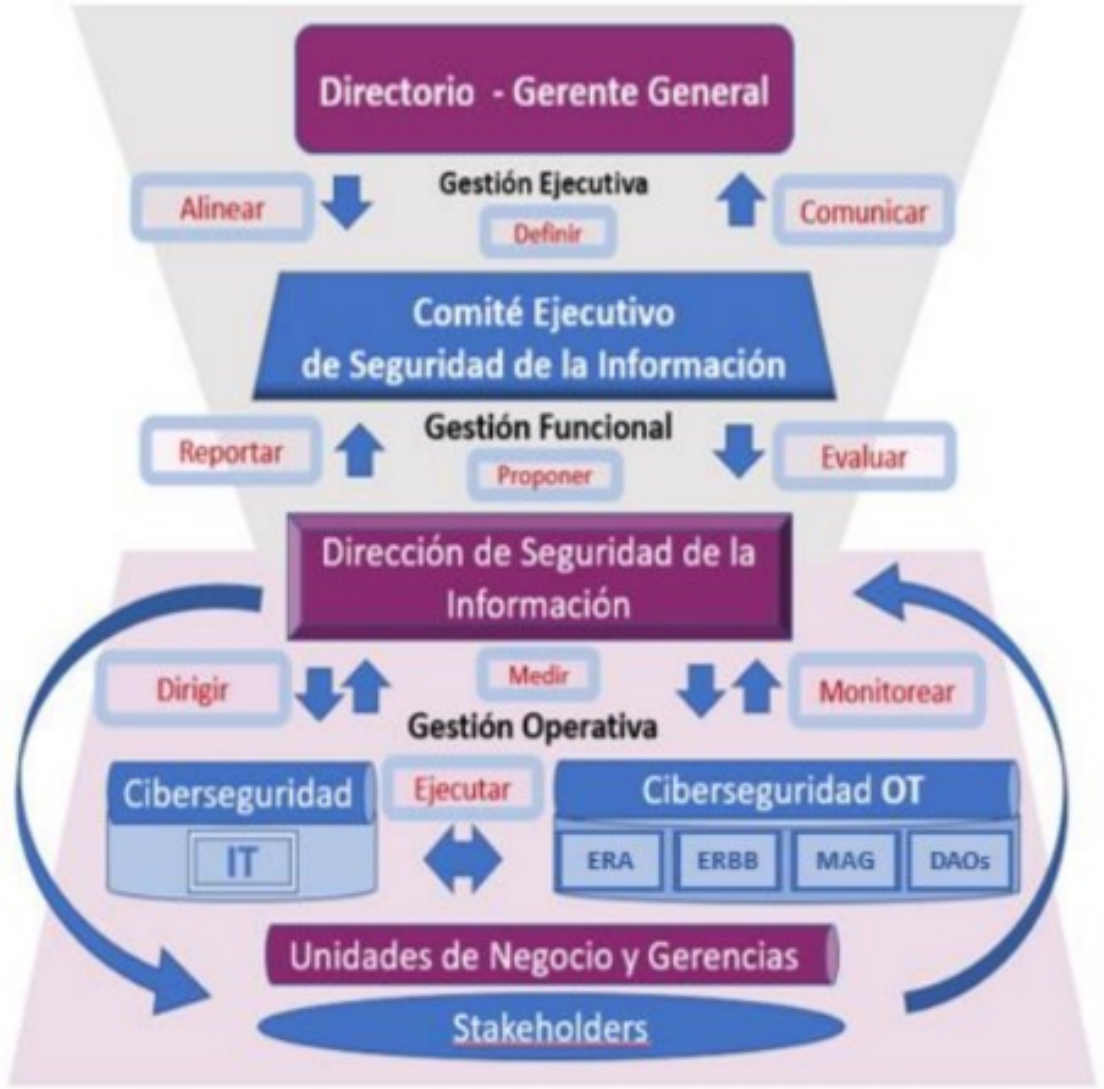
Evaluación Redes Industriales

Basado en Estándares Internacionales

- Framework Ciberseguridad NIST
- ISO 27001
- IEC 62443



Comité Ejecutivo de Seguridad de la Información

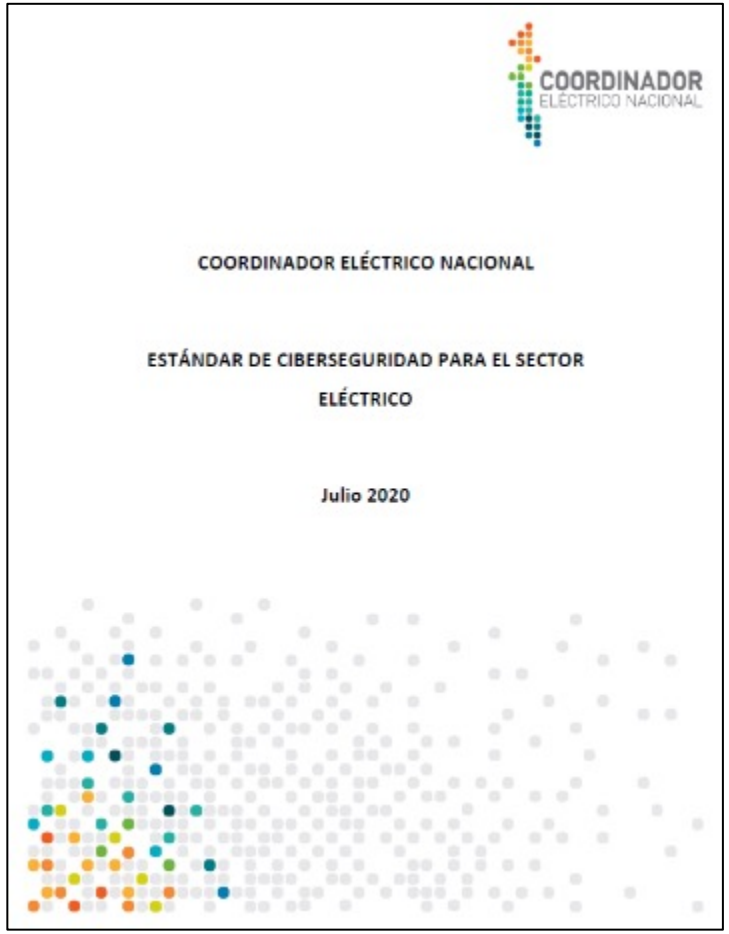


ANEXO: INTEGRANTES COMITÉ DE CIBERSEGURIDAD IT – OT

INTEGRANTES BÍO BÍO		
Ámbito	Estructura Organizativa	
OT	División Aplicaciones ERBB	Departamento de Ingeniería Bío Bío
	División Aplicaciones ERBB	Departamento de Ingeniería Bío Bío
	Div. Electric. Instrumento BB	Departamento de Mantención Bio Bio
	Div. Electric. Instrumento BB	Departamento de Mantención Bio Bio
IT	Departamento Inn. y Des. Tecn. ERSA	Gerencia de Innovación y Desarrollo Tecnológico

INTEGRANTES ACONCAGUA		
Ámbito	Estructura Organizativa	
OT	División Aplicaciones ERA	Departamento de Ingeniería ERA
	División Electric. Instr. y Electro. ERA	Departamento de Mantención ERA
	División Aplicaciones ERA	Departamento de Ingeniería ERA
	División Electric. Instr. y Electro. ERA	Departamento de Mantención ERA
	Departamento Inn. y Des. Tecn. ERSA	Gerencia de Innovación y Desarrollo Tecnológico

Estándar de Ciberseguridad para el Sector Eléctrico



Estándar de Ciberseguridad para el Sector Eléctrico

Ejemplos de evidencia solicitada

Requerimientos para instalaciones de Impacto Bajo

Esta sección incluye todos los requerimientos a cumplir por las instalaciones de impacto Bajo según lo solicitado por el Estándar

15. CIP-002: Categorización de Ciber Sistemas SEN
    Proceso de identificación de Ciber Sistemas SEN - R1

    ☐ Proporcione evidencia documentada con el proceso y/o procedimiento de Identificación, modificación, retiro o incorporación de Ciber Activos y Ciber Sistemas.

16. CIP-002: Categorización de Ciber Sistemas SEN
    Revisión y aprobación de R1 - R2 ítem 2.1

    ☐ Proporcione evidencia del inventario de Ciber Activos y Ciber Sistemas, con sus ubicaciones definidas, y actualizar esta lista en caso de presentar cambios, al menos una vez cada 15 meses calendario

17. CIP-002: Categorización de Ciber Sistemas SEN
    Revisión y aprobación de R1 - R2 ítem 2.2

    ☐ Proporcione evidencia de la revisión y aprobación del Encargado CIP del listado elaborado anteriormente, al menos una vez cada 15 meses calendario

18. CIP-003: Controles de Gestión de la Seguridad
    Desarrollo de Política y Planes de Ciberseguridad - R1.b

    ☐ Para Ciber Sistemas SEN de Impacto Bajo: a) Conciencia de ciberseguridad, b) Controles de seguridad física, c) Control de acceso electrónico, d) Respuesta a incidentes de ciberseguridad, e) Mitigación de riesgos de código malicioso en Ciber Activos Transitorios y Medios Removibles, f) Declaración y respuesta a Circunstancias Excepcionales CIP.

19. CIP-003: Controles de Gestión de la Seguridad
    Planes de ciberseguridad. (Plazo para desarrollo de políticas) - R2 secc 1

    ☐ Proporcione evidencia con un calendario de ejecución de charlas de conciencia en Ciberseguridad de los temas antes mencionados.

20. CIP-003: Controles de Gestión de la Seguridad
    Planes de ciberseguridad. (Plazo para desarrollo de políticas) - R2 secc 2

    ☐ Proporcione evidencia de que se implementaron controles de seguridad física para controlar el acceso físico a la ubicación de los Ciber Sistemas SEN, (Control de acceso electrónico, biometría, otros)

Ruta Ciberseguridad Tecnología de la Operación ENAP

Levantamiento de redes:
Diagnóstico
Plan de acción

2008

2014

Trabajo colaborativo entre
IT/OT para realizar
una Segregación de Redes

2015 - 2016

La Dirección Corporativa de Integridad de Sistema TI de la época, lideró el proyecto para la adopción del marco de NIST y la ISA99/IEC 62443.

2017

Directora Seguridad de la Información

Comité de Ciberseguridad IT-OT

2018

Incorporación del Riesgo de Ciberseguridad

Estándares de Ciberseguridad para el sector eléctrico

2020

Definiciones organizacionales, procedimientos y KPIs

2021

2022

2023

Procedimientos y KPIs Equipos Críticos

Desarrollo de Procedimientos

- Actualización de diagramas de red
- Actualización de antivirus y antimalware
- Control de acceso lógico
- Recuperación ante desastres
- Gestión y respuesta ante incidentes de ciberseguridad

Indicadores (KPI's) Equipos Críticos	Objetivo
N° Equipos con DAT actualizado / N° Equipos Existentes	90%
N° Equipos con parches certificados / N° Equipos Existentes	90%
N° Equipos con soporte / N° Equipos Existentes	90%
N° Equipos con protección Puertos USB/ N° Equipos Existentes	100%

Ruta Ciberseguridad Tecnología de la Operación ENAP

Levantamiento de redes:
Diagnóstico
Plan de acción

2008 → **2014**

Trabajo colaborativo entre
IT/OT para realizar
una Segregación de Redes

2015 - 2016

La Dirección Corporativa de Integridad de Sistema TI de la época, lideró el proyecto para la adopción del marco de NIST y la ISA99/IEC 62443.

2017

Directora Seguridad de la Información

Comité de Ciberseguridad IT-OT

2018

Incorporación del Riesgo de Ciberseguridad

Estándares de Ciberseguridad para el sector eléctrico

2020

Definiciones organizacionales, procedimientos y KPIs

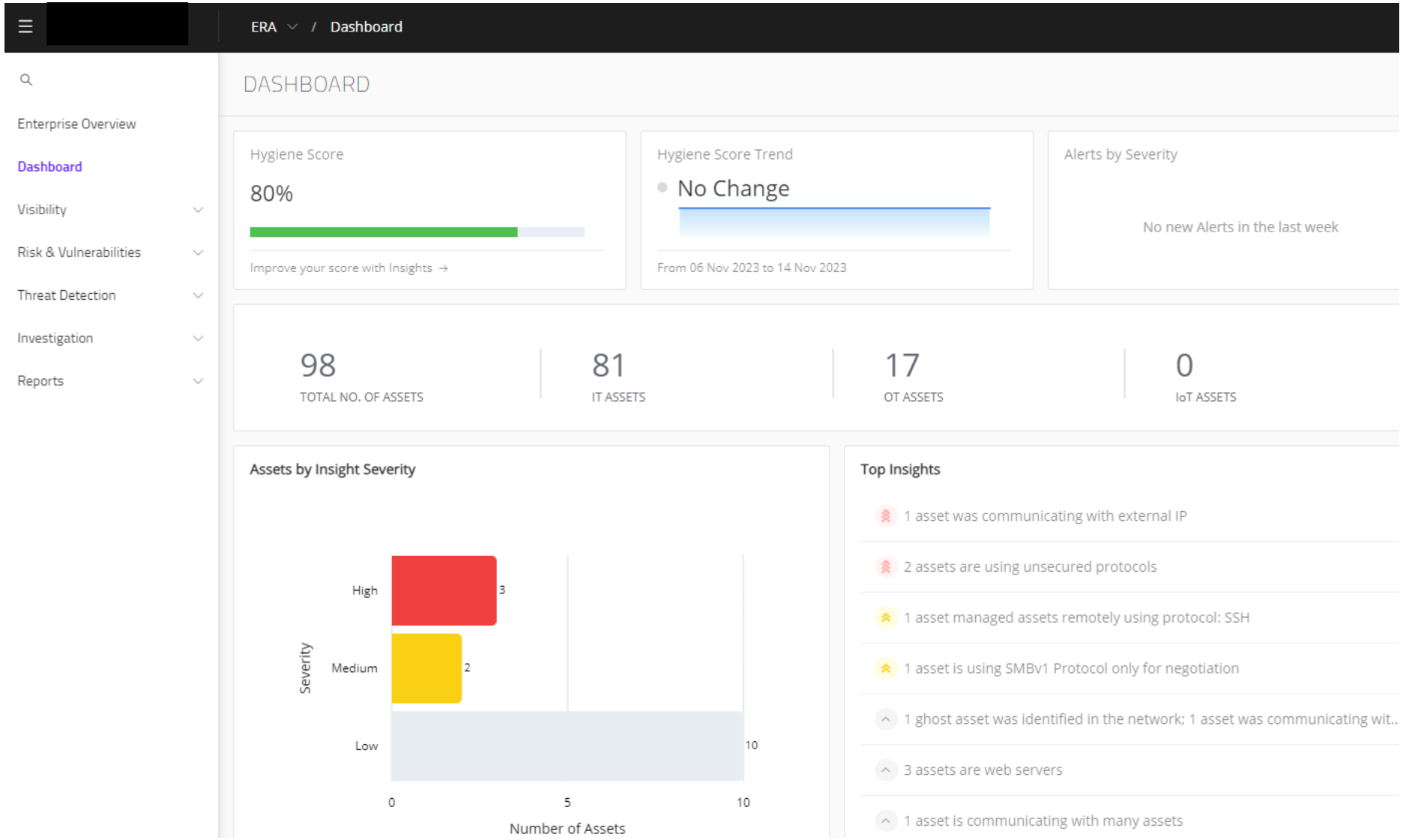
2021

Proyecto IDS

2022

2023

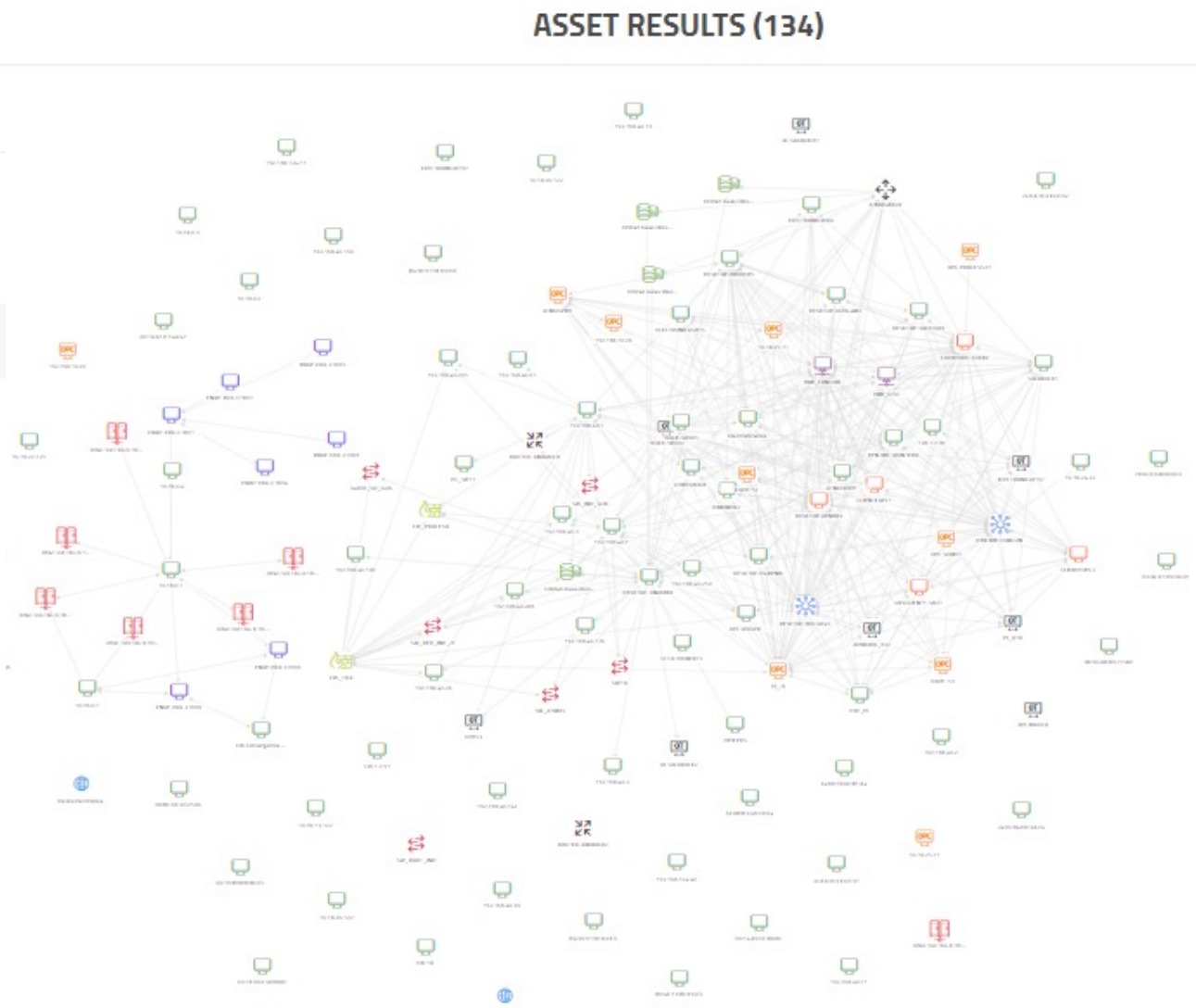
Proyecto Sistema Detección Intrusión ERA



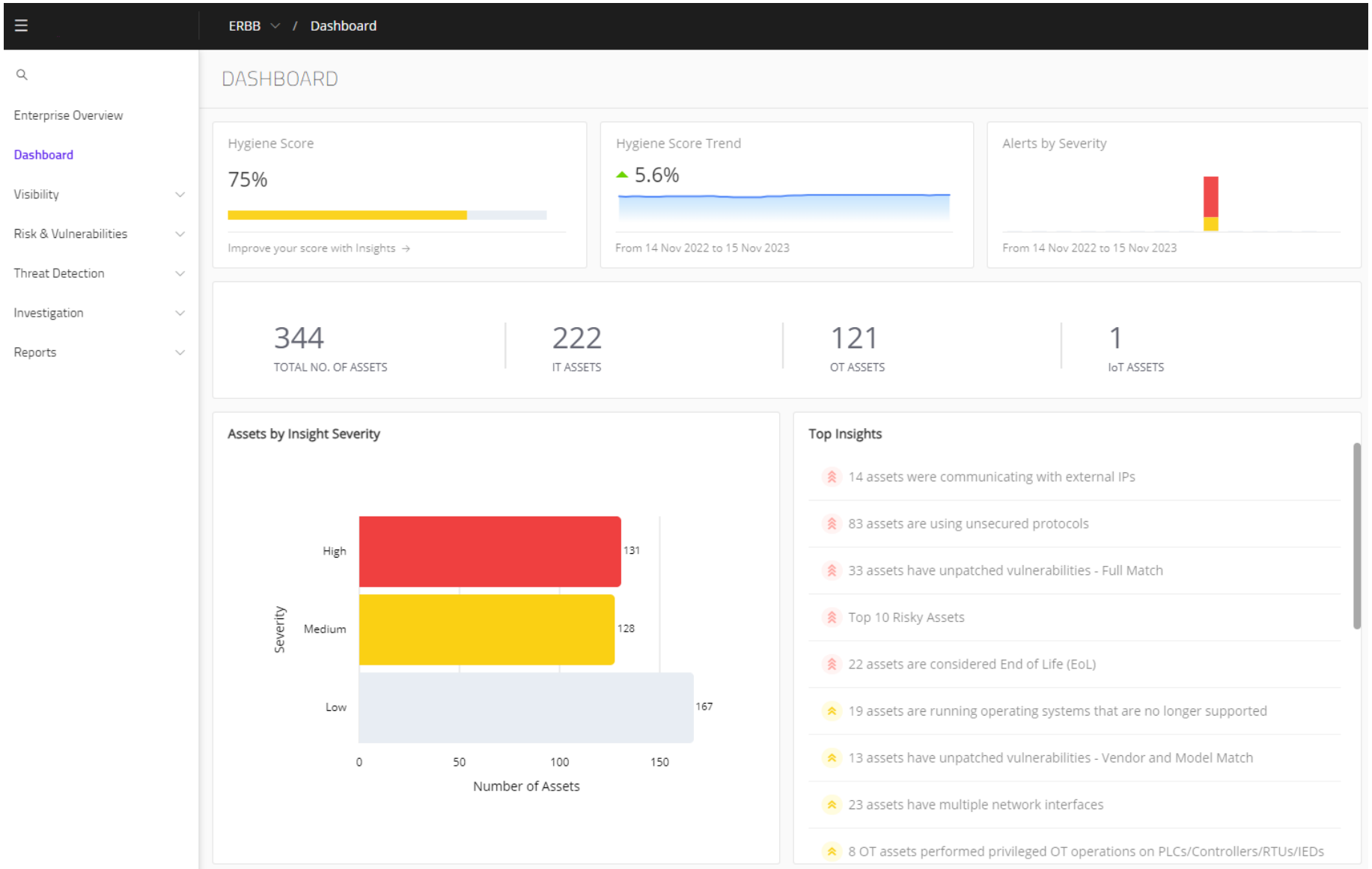
Proyecto Sistema Detección Intrusión ERA

RESULTS (134)

TYPE	VENDOR	CRITICALITY	RISK LEVEL
Endpoint	Cisco	Low	Medium
User Workstation	Dell	Medium	Medium
User Workstation	Dell	Medium	Medium
Endpoint	Phoenix Contact Electronics	Low	Medium
OPC Server	Dell	Medium	Medium
User Workstation	Dell	Medium	Medium
Endpoint	Dell	Low	Medium
OPC Server	Cisco	High	Medium



Proyecto Sistema Detección Intrusión ERBB



Proyecto Sistema Detección Intrusión ERBB

RESULTS (365)

TYPE	VENDOR	CRITICALITY	RISK LEVEL
Endpoint	Advantech Technology	Low	Medium
Endpoint	Dell	Low	Medium
Networking	Hirschmann	Medium	Medium
Networking	Hirschmann	Medium	Medium
Endpoint	Rockwell Automation	Low	Medium
Endpoint	Intel	Low	Medium
Endpoint	Rockwell Automation	Low	Medium
Gateway	Campbell Scientific	High	Medium

Ruta Ciberseguridad Tecnología de la Operación ENAP

Levantamiento de redes:
Diagnóstico
Plan de acción

2008

2014

Trabajo colaborativo entre
IT/OT para realizar
una Segregación de Redes

2015 - 2016

La Dirección Corporativa de Integridad de Sistema TI de la época, lideró el proyecto para la adopción del marco de NIST y la ISA99/IEC 62443.

2017

Directora Seguridad de la Información

Comité de Ciberseguridad IT-OT

2018

Incorporación del Riesgo de Ciberseguridad

Estándares de Ciberseguridad para el sector eléctrico

2020

Definiciones organizacionales, procedimientos y KPIs

2021

Proyecto IDS

2022

Servicio SOC

Equipo CSIRT en cada Refinería

Implantación Normas

2023

Desarrollo Normas

Plan de implantación a revisar con las UNs

#	Nombre de la Normativa	Fecha	Entrada en Vigor
1	Norma Políticas y procedimientos de Seguridad OT	01-abr-23	Corto Plazo
2	Norma Alcance del SGCI y Organización de la Seguridad OT	02-may-23	Corto Plazo
3	Norma Capacitación del personal y conciencia de la Seguridad OT	02-may-23	Corto Plazo
4	Norma Gestión y respuesta ante incidentes de ciberseguridad OT	02-may-23	Corto Plazo
5	Norma Seguridad Física y ambiental OT	01-ago-23	Mediano Plazo
6	Norma Segmentación de red OT	01-ago-23	Mediano Plazo
7	Norma Implementación de Gestión del Riesgo OT	01-ago-23	Mediano Plazo
8	Norma Desarrollo y Mantenimiento del Sistema OT	01-ago-23	Mediano Plazo
9	Norma Plan de Continuidad de Negocio OT	02-nov-23	Largo plazo
10	Norma de Conformidad OT	02-nov-23	Largo plazo
11	Norma Revisión, Mejora y Mantención del SGCI	02-nov-23	Largo plazo
12	Norma Identificación, clasificación y evaluación de riesgos OT	02-dic-23	Largo plazo
13	Norma Control de Acceso OT	02-dic-23	Largo plazo
14	Norma Gestión de información y documentos OT	02-dic-23	Largo plazo

Actividades 2024

- Continuar Capacitaciones en IEC62443
- Proceso de concientización global
- Proyecto de Antivirus automático en L2
- Acceso remoto redes industriales a través de zona segura (DMZ) mediante una plataforma segura y gestionada
- Continuar depurando alertas de SOC
- Continuar proyecto de habilitación de segmentos de la red de control a sensores del IDS

carolinamelo@enap.cl

palvarez@enap.cl

Innovarpel 2023

Digitalización y Ciberseguridad
en la Industria del Oil&Gas

Hotel Colón | Quito, Ecuador

21 y 22 de noviembre de 2023

ORGANIZA

arpel

REALIZA

SEMINARIUM