CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título; ☐ Tesis de Postgrado;

Título del trabajo: Normativas de Seguridad y Configuración para la Gestión del Modelo Predictivo de Fallas Eléctricas en Líneas de Transmisión

Nombre del candidato(a): Jorge Alejandro Huentutripay Pozo

Carrera / Grado: Ingeniería en Informática

Campus: Viña del Mar ; **Departamento**: Electrónica e Informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Gonzalo Mendoza Cárdenas, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL

☒ El trabajo **NO contiene información que amerite confidencialidad** y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (embargo) por:

☐ 6 meses; ☐ 12 meses; ☐ 2 años; ☐ 3 años; ☐ 5 años; ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 08/08/2025 ; **Firma:** _____

Estudiante o Candidato(a):

Fecha: 08/08/2025 ; **Firma:** _____

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

Normativas de Seguridad y Configuración para la Gestión del Modelo Predictivo de Fallas Eléctricas en Líneas de Transmisión

Jorge Huentutripay Pozo

huentutripayjorge@gmail.com

Gonzalo Mendoza Cárdenas
Profesor Guía

Resumen: El documento presenta el desarrollo de un marco normativo y de configuración para gestionar un modelo predictivo de fallas eléctricas en líneas de transmisión, enfocado en cumplir con los estándares de seguridad requeridos en el sector eléctrico nacional. Se llevó a cabo una investigación de estándares internacionales y normativas nacionales relevantes, identificando y seleccionando los puntos aplicables al caso de uso. Con base en estos hallazgos, se elaboró una política de seguridad estructurada en secciones, diseñada para abordar los requerimientos regulatorios y operativos del sector. La política fue implementada en la arquitectura de la solución propuesta, validando su cumplimiento en un entorno de pruebas. Su objetivo principal fue garantizar que cumpliera con las normativas vigentes y fuera aplicable a soluciones tecnológicas en el sector eléctrico nacional. El resultado obtenido es una política de seguridad completa que sirve como modelo adaptable para futuras soluciones en la industria eléctrica, proporcionando robustez frente a desafíos de ciberseguridad.

1. Introducción

Después del periodo de la pandemia del 2020, empezó un surgimiento bastante notorio de ataques de ciberseguridad e identificación de vulnerabilidades. A lo largo de todo el mundo, múltiples récords históricos en incidentes de ciberseguridad e identificación de vulnerabilidades están perpetuando la idea de que estos números solo irán subiendo con la adopción de la transformación digital en las empresas y en todo el mundo.

La digitalización de los procesos de negocio, industriales y de defensa nacional supone nuevos riesgos para el entorno digital del país. Las empresas y entidades de interés nacional necesitan empezar a implementar planes de ciberseguridad de forma integral y estratégica, apoyándose en la comunicación efectiva y la cooperación con la industria y el estado para el fortalecimiento de la ciberseguridad en Chile, entendiendo que es necesario una cultura de prevención y capacitación en estos temas, ya que, de algún modo u otro, todas las personas que interactúan con el entorno digital deben tener competencia en este tópico.

Según el artículo *Cybersecurity Risks in a Pandemic*[1] publicado por Journal of Medical Internet Research, se estima en 6 billones de dólares las pérdidas generadas por ciber amenazas para el año 2021.

En Latinoamérica la situación no es muy distinta, ya que según cifras recolectadas por la Universidad Ean[2], el 98% manifestó un aumento en la frecuencia de ciber ataques durante la pandemia, destacando la implementación de dispositivos IoT, estrategias de nube y servicios de escritorios remotos como los principales ambientes afectados.

Este panorama no es muy distinto a lo que percibe Chile. El 19 de septiembre del año 2022, el grupo de hackers Guacamaya filtró aproximadamente 400.000 correos electrónicos de las Fuerzas Armadas de Chile[3]. Caso no muy distinto es el de la última semana de mayo del 2023, cuando el grupo de hackers Rhysida publicó en su sitio de filtraciones aproximadamente 360.000 documentos de la misma entidad[4], presumiendo que esta solo era el 30% de la información sustraída. Este aumento en la gravedad de los casos empezó a generar mucho debate en el Congreso Nacional, por lo que después de una larga espera, el 12 de diciembre del 2023, se aprobó el proyecto de Ley Marco de Ciberseguridad e Infraestructura Crítica. Esto presenta nuevos desafíos regulatorios y establece a nivel nacional la meta de avanzar a paso firme a un país con excelencia en el área de la ciberseguridad.

2. Marco Teórico

Este trabajo se basa en la teoría de la seguridad de la información y la gestión de datos en el contexto de un desarrollo de soluciones en la nube, teniendo como usuario final entidades chilenas que provean energía a nivel nacional y estén supervisadas bajo el Coordinador Eléctrico Nacional y/o las leyes chilenas relacionadas al sector eléctrico nacional.

Se realizó un análisis exhaustivo de estudios y métricas recientes sobre el estado de la ciberseguridad en el país. Este análisis incluyó la revisión de normativas chilenas, como el Estándar de Ciberseguridad del CEN, y estándares internacionales de gestión de la seguridad de la información, como la ISO/IEC 27001, todo esto con el fin de facilitar el cumplimiento normativo por parte de los usuarios finales.

2.1 Seguridad de la Información

La seguridad de la información se define como la protección de la información importante en contra del acceso, divulgación, alteración u cualquier otro uso no autorizado, entendiendo su existencia en un escenario de amenazas en constante cambio.

Comprende una variedad de herramientas, recursos y procesos, entre ellos:

- Seguridad de aplicaciones
- Seguridad en la nube
- Recuperación ante desastres
- Respuesta a incidentes
- Seguridad de infraestructura
- Administración de vulnerabilidades

---

[1] Journal of Medical Internet Research. Cybersecurity Risks in a Pandemic. *JMIR Publications*, Vol. 22, No. 9, 2020.

[2] El virus del cibercrimen aumento el 2020. Universidad de Ean. Publicado por Fredy Bautista García

[3] Hackeo masivo al Estado Mayor Conjunto expuso miles de documentos de áreas sensibles de la defensa. Nicolás Sepúlveda. Publicado por CIPER Chile

[4] Rhysida revela 360.000 documentos secretos y reservados del Ejército de Chile. Nicolás García. Publicado por infodefensa.com

2.2 Ciberseguridad

La ciberseguridad se centra en la protección de las redes, dispositivos, datos y sistemas de información digital en contra de ataques cibernéticos o accesos no autorizados que amenacen la continuidad del negocio, buscando abarcar tres conceptos fundamentales que forman la triada CIA.

Las tres siglas de la triada CIA significan confidencialidad, integridad y disponibilidad. Este es un modelo común que pone como pilar principal la protección de la información para la construcción de sistemas de seguridad informática. Garantizar estos tres principios es crucial para la operación de un negocio y un perfil de seguridad más sólido.

Confidencialidad: Es el principio que asegura que la información sea accesible solo por las personas que están autorizadas, protegiendo estos datos sensibles o privados de terceros mal intencionados.

Integridad: Es el principio que asegura que la información no sea alterada o modificada fuera de su uso autorizado, asegurando su confiabilidad a lo largo del tiempo.

Disponibilidad: Es el principio que asegura que la información este disponible y sea accesible en cualquier momento que sea requerida por las personas autorizadas.

2.3 Organización Internacional de Normalización

Por sus siglas en ingles ISO, la Organización Internacional de Normalización, fundada en 1947, tiene como objetivo la creación y publicación de estándares (o normas) internacionales bajo una entidad independiente y sin fines de lucro.

Los estándares, según la pagina oficial de la organización, se dividen en 12 categorías: Salud, Tecnologías de la Información, Gestión y Servicios, Seguridad, Transporte, Energía, Diversidad e Inclusión, Sostenibilidad Ambiental, Alimentos y agricultura, Materiales, Edificación y Construcción, Ingeniería. Dentro de las normas esenciales y destacadas por la propia organización, se encuentran las siguientes:

ISO 9001:2015: Establece los criterios para un sistema de gestión de calidad, con un enfoque en la mejora continua, control de procesos y liderazgo

ISO 37001:2025: Establece los criterios para un sistema de gestión antisoborno, apoyando en áreas como formación, auditorias y evaluación de riesgos

ISO 27001:2022: Establece los criterios para un sistema de gestión de seguridad de la información, buscando resguardar la confidencialidad, integridad y disponibilidad de la información

ISO 14001:2015: Establece los criterios para un sistema de gestión ambiental, enfocándose en reducir el impacto ambiental y asegurar el cumplimiento legal

ISO 45001:2018: Establece los criterios para un sistema de gestión de la seguridad y salud en el trabajo a través de la identificación de riesgos y la formación del personal.

ISO 42001:2023: Establece los criterios para una gestión segura y ética de la inteligencia artificial (IA) que mitigue riesgos éticos y fomente la confianza en la IA

2.4 Infraestructura Critica

La infraestructura critica bajo las leyes nacionales se definen como el conjunto de instalaciones, sistemas físicos o servicios esenciales y de utilidad públicas, así como aquellos cuya afectación cause un grave daño a la salud o al abastecimiento de la población, a la actividad económica esencial, al medioambiente o a la seguridad del país. También incluye la infraestructura indispensable para la generación, transmisión, transporte, producción, almacenamiento y distribución de los servicios e insumos básicos para la población.

2.5 Sistema Eléctrico Nacional

El sistema eléctrico nacional la red principal de generación, transmisión y distribución de energía eléctrica de Chile. Nació oficialmente en 2017 tras el compromiso de la fusión de los dos principales sistemas eléctricos históricos del país[5]: el Sistema Interconectado Central y el Sistema Interconectado del Norte Grande. El objetivo de esta fusión fue la creación de una red troncal que logró comprender el 97% del suministro total.

Dentro de las métricas más destacables a la fecha de abril del 2025 es que cuenta con 39.915 kilómetros en líneas de transmisión, dentro de los cuales participan 850 empresas coordinadas por la entidad central y principal de este sistema eléctrico, el Coordinador Eléctrico Nacional.

2.6 Coordinador Eléctrico Nacional

Según la definición entregada por la misma entidad, el Coordinador Eléctrico Nacional es un organismo independiente, sin fines de lucro encargado de la coordinación de la operación del Sistema Eléctrico Nacional.

Además, la entidad del Coordinador es de derecho público, es decir, persigue el bien común. Su rol principal se representa usualmente como un auditor de las empresas coordinadas, estableciendo y asegurando el cumplimiento de las políticas existentes y el proceso de mejora continua.

2.7 Informática en la nube

La informática en la nube es un modelo de servicios que ofrece recursos de computación a través de internet, como almacenamiento, bases de datos, servidores, redes y plataformas para el alojamiento y distribución de distintos tipos de soluciones tecnológicas que requieran de una infraestructura desplegada y disponible al instante en internet.

Esto permite el acceso a recursos e infraestructura de forma remota con un modelo de pago por uso, lo cual, gracias a las economías de escala, ahorra dinero al usuario final en el proceso de comprar, poseer y mantener servidores y centros de datos físicos, ayudando al negocio a enfocarse en desarrollar y entregar mayor valor al usuario final.

Para entender el aumento significativo del mercado de la informática en la nube, según datos recopilados por Synergy Research Group, el año 2024 el mercado alcanzo la cifra de 330.000 millones de dólares[6], un aumento del 45% a comparación del año 2022, que presentó la cifra de 228.000 millones de dólares.

---

[5] En Atacama se concretó la nueva interconexión eléctrica nacional. Ministerio de Energía, 6 de Diciembre del 2017.

[6] Cloud Market Jumped to $330 billion in 2024 – GenAI is Now Driving Half of the Growth. Publicado por Synergy Research Group

Dentro de los proveedores principales podremos encontrar Amazon Web Services, pionero en servicios en la nube, Azure, con una fuerte integración con los productos de Microsoft, y Google Cloud Plataform, con una trayectoria más reciente, pero con un enfoque innovador.

A continuación, se presenta una tabla comparativa, buscando resaltar las diferencias esenciales de cada una de las plataformas, *dejando fuera aspectos técnicos como personales que puedan afectar a la elección de cada una de las plataformas y entendiendo que las razones de la decisión no serán abordadas en este documento*.

	Amazon Web Services	**Microsoft Azure**	**Google Cloud Platform**
Madurez	Desde 2006, con el ecosistema más amplio y maduro del mercado	Desde 2010 competidor fuerte con AWS, enfocado en el área empresarial	Desde 2008, pero aun consolidándose, avanzando rápidamente en el ámbito de la IA
Seguridad y Cumplimiento	Seguridad por capas, con gran granularidad en políticas de acceso. Fuerte adopción en salud, finanzas y defensa	Integración con Active Directory, enfocado en seguridad empresarial del ecosistema de Microsoft. Amplio historial de cumplimiento en el sector gubernamental	Seguridad basada en prácticas modernas e innovadoras como zero trust. Menos presencia en regulaciones especificas como banca o defensa
Flexibilidad	Ofrece herramientas para construir desde cero compatibles con distintos ecosistemas	Enlazado fuertemente al ecosistema de Windows, Office y productos de Microsoft	Ofrece soluciones y herramientas modernas, pero con limitante en versiones legacy de productos
Uso Gratuito	Nivel gratuito permanente en muchos servicios claves, además de pruebas mensuales que varían por servicio	Nivel gratuito por 12 meses para servicios específicos para ese periodo	Nivel gratuito permanente en servicios seleccionados y crédito inicial de $300 por 90 días

**Fuente: docs.aws.amazon.com, learn.microsoft.com, cloud.google.com*

Tabla 1. Tabla comparativa entre proveedores de servicios en la nube.

3. Definición y Metodología de Trabajo

Para una integración efectiva de la solución con las normativas en las que nos basaremos, se debe incluir un proceso que logre levantar los distintos requisitos y controles de interés para el negocio y aplicables a nuestro caso, con el fin de apoyar en un posterior proceso de diseño una línea base para la configuración y arquitectura de esta solución que pueda asegurar los estándares mínimos de seguridad requeridos por las normativas seleccionadas

Una correcta gestión de estos dos procesos puede beneficiar la implementación de los controles de seguridad necesarios para el cumplimiento normativo de la solución robusta en términos de seguridad de la información.

3.1 Revisión de Normativas

Se llevará a cabo un análisis exhaustivo de una selección de estándares internacionales relevantes, tales como la ISO 27001, junto con normativas nacionales específicas del sector eléctrico chileno, como la Ley Marco de Ciberseguridad e Infraestructura Crítica y el Estándar de Ciberseguridad del Sistema Eléctrico Nacional. Este análisis tiene como objetivo identificar los requerimientos y lineamientos aplicables, asegurando que el marco de configuración propuesto esté alineado con las regulaciones vigentes que afectan directamente a los usuarios finales de la solución. Se incluirán recomendaciones de mejores prácticas y directrices para la posterior definición de las políticas de seguridad

3.2 Diseño del Marco de Configuración

Basado en los hallazgos obtenidos durante la revisión de normativas, se diseñará un marco de configuración integral que contemple las mejores prácticas de ciberseguridad, resiliencia operativa y requerimientos de seguridad necesarios para el cumplimiento regulatorio. Este marco incluirá políticas específicas para garantizar la confidencialidad, integridad y disponibilidad de los sistemas, así como otros procesos pertinentes para la implementación de un sistema de gestión de seguridad de la información. Además, se definirá de que manera se monitoreará el cumplimiento continuo, permitiendo la integración de auditorías regulares y adaptaciones frente a cambios regulatorios o tecnológicos.

3.3 Implementación

Se procederá con la implementación del marco de configuración diseñado en la arquitectura de la solución, simulando un entorno controlado de prueba que simule las condiciones reales de operación. Esta arquitectura deberá validar la efectividad de las configuraciones propuestas en términos de seguridad y funcionalidad, así como identificar posibles áreas de mejora antes de su despliegue en el sistema productivo. Durante esta fase, se implementarán las políticas descritas anteriormente directamente en la solución propuesta, construyendo una arquitectura que cumpla con todos los requisitos de seguridad establecidos.

4. Desarrollo de la Investigación

4.1 Selección de Normas

4.2 Norma: UNE-ISO/IEC 27001:2023

En Chile, la nueva Ley Marco de Ciberseguridad e Infraestructura Crítica define la ciberseguridad en base a la protección de la seguridad de la información, tomando como referencia las normas ISO, específicamente la ISO 27001, una de las más conocidas y adoptadas en la industria.

La norma ISO 27001 se ha preparado para establecer los requisitos para levantar un Sistema de Gestión de la Seguridad de la Información, o SGSI según sus siglas. Tomando en cuenta los documentos que se hablarán más adelante, veremos como esto se alinea perfectamente con el cumplimiento de las regulaciones del sector de transmisión eléctrica.

4.2.1 Contenidos del documento

Dentro de los contenidos que tiene esta norma, podremos obtener definiciones, requisitos, y practicas recomendadas a lo largo de las siguientes secciones claves.

Secciones Claves:

- Contexto de la organización *(Clausula 4)*
- Liderazgo *(Clausula 5)*
- Planificación *(Clausula 6)*
- Apoyo *(Clausula 7)*
- Operación *(Clausula 8)*
- Evaluación del desempeño *(Clausula 9)*
- Mejora *(Clausula 10)*

Junto a estas, encontraremos el Anexo A titulado *Controles de seguridad*, el cual nos presenta 93 controles de seguridad organizados en 4 dominios.

Categorías:

- Controles organizacionales
- Controles orientados a personas
- Controles físicos
- Controles tecnológicos

En el contexto actual, Chile se ubica en el 5to puesto de Sudamérica con 123 certificaciones ISO/IEC 27001, esto según los resultados de la ISO Survey 2023[7], encuesta encargada de recolectar el número de certificados válidos para los estándares ISO, siendo referencia el 1er puesto de Colombia con 395 certificaciones. Debido a la naturaleza de las nuevas regulaciones, es de esperar que organizaciones y empresas chilenas empiecen a buscar certificarse en estas normas, un fenómeno que ya se está viendo con más frecuencia en los sectores considerados infraestructura crítica como lo es la industria eléctrica.

4.2.2 Investigación del Documento

Para la investigación de este documento, se buscará extraer la mayor cantidad de controles, requisitos y practicas recomendadas, intentando seguir los lineamentos establecidos en las regulaciones y los demás estándares expuestos en esta tesina con el objetivo de lograr la mayor conformidad para una correcta implementación de un sistema para gestionar los riesgos relacionados con la seguridad de la información.

4.2.2.1 Sobre el Contexto de la organización

La norma ISO menciona la importancia de que la organización entienda y analice los factores internos y externos que afectan a la gestión de la seguridad de la información

En el apartado 4.1 se hace referencia exactamente a esto, estableciendo el deber que tiene la organización de determinar las cuestiones externas e internas pertinentes a su propósito y que afecten

[7] ISO Survey 2023 results – number of certificates and sites per country and the number of sectors overall.

la capacidad de lograr los resultados previstos de su Sistema de Gestión de la Seguridad de la Información (SGSI).

Dado que la solución propuesta para la empresa contempla un servicio tercerizado, es importante que este pueda ayudar a satisfacer los objetivos de los clientes que busquen lograr la conformidad con la norma.

Este detalle se reafirma un poco más adelante en el documento, mencionando en el apartado 4.3 que las interfaces y dependencias existentes entre la organización y terceros son factores esenciales a la hora de determinar el alcance del SGSI.

4.2.2.2 Sobre la planificación

La sección de Planificación se refiere al proceso de establecer las acciones necesarias para garantizar la seguridad de la información, buscando identificar y abordar los riesgos que puedan dificultar el cumplimiento de los objetivos del SGSI.

En la norma se destaca lo importante que es considerar los requisitos levantados sobre el contexto de la organización, siendo unos de los fines que más nos compete el prevenir o reducir efectos indeseados que afecte el cumplimiento de estos requisitos. Esto requiere una implementación solida que busque reducir la superficie de ataque, reduciendo la incertidumbre y los riesgos que puedan acentuar futuros incidentes.

En el apartado 6.1.2 de la norma, se puede evidenciar un gran valor en la búsqueda e identificación de los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información, por lo que se requerirá implementar en la solución medidas exhaustivas para lograr minimizar estos riesgos y asegurar que solo las partes interesadas puedan tener acceso a la información pertinente y en cualquier momento que se necesite, como por ejemplo, para efectos de auditorías internas o también para la documentación requerida por el SGSI.

En el siguiente inciso se menciona que la organización deberá determinar todos los controles que sean necesarios para implementar estas medidas en el tratamiento de riesgos de seguridad de la información, pudiendo diseñar controles según sea necesario, entendiendo que los controles enumerados en el anexo A no pueden ser suficientes en algunos casos.

4.2.2.3 Sobre la evaluación del desempeño

En la sección de Evaluación del desempeño se establece la necesidad de medir, monitorear, analizar y evaluar si el Sistema de Gestión de la Información está funcionando correctamente, avanzando de manera eficaz hacia los objetivos establecidos para este.

Dentro de lo que podemos destacar de aquí, es que la organización determinará qué, cuando y como es necesario monitorizar y medir para así lograr resultados válidos, siendo necesario que el método pueda producir resultados comparables y reproducibles. Es por esto por lo que en la solución se requerirá implementar herramientas para poder monitorear y disponibilizar esta información para las evaluaciones de desempeño o futuras auditorías del Sistema de Gestión de la Información.

4.3 Estándar de Ciberseguridad para el Sector Eléctrico Nacional (SEN)

El día 27 de julio de 2020, el **Coordinador Eléctrico Nacional** presentó el Estándar de Ciberseguridad para el Sector Eléctrico Nacional, el cual establece los requisitos y medidas de control mínimas

aplicables al sector eléctrico con el fin de proteger el servicio de energía eléctrica de potenciales ciber amenazas que pongan en riesgo su seguridad y continuidad.

Según la misma introducción del documento, se realizó un análisis exhaustivo sobre las diferentes normativas internacionales existentes sobre ciberseguridad en el sector eléctrico, **lo que resultó en la decisión de tomar como referencia el estándar NERC-CIP**. Su implementación se llevó a cabo con el apoyo especializado de CAISO, operador independiente del sistema de California que entrega aproximadamente el 80% del suministro eléctrico de este estado.

La norma NERC-CIP es el estándar de ciberseguridad que aplican las empresas de servicios públicos en Norteamérica, con el objetivo de establecer los requisitos específicos **para la gestión de la seguridad de la información en infraestructuras críticas**, haciendo foco en las redes de suministro eléctrico.

4.3.1 Contenidos del documento

La estructura de esta norma está basada en 13 estándares que definen los requerimientos para identificar ciber activos críticos, crear controles de seguridad y mejorar la seguridad tanto física como electrónica, **tomando la categorización de estos ciber activos como base para establecer estas definiciones**. Estos estándares son:

- *CIP-002:* Categorización de Ciber Sistemas SEN
- *CIP-003:* Controles de Gestión de la Seguridad
- *CIP-004:* Personal y Capacitación
- *CIP-005:* Perímetro de Seguridad Electrónica
- *CIP-006:* Seguridad Física de Ciber Sistemas SEN
- *CIP-007:* Gestión de la Seguridad de Sistemas
- *CIP-008:* Reporte de Incidentes y Planes de Respuesta
- *CIP-009:* Planes de Recuperación para Ciber Sistemas SEN
- *CIP-010:* Gestión de Cambio de Configuración y Evaluación de Vulnerabilidades
- *CIP-011:* Protección de Información
- *CIP-012:* Comunicaciones entre Centros de Control
- *CIP-013:* Gestión de Riesgos en la Cadena de Suministros
- *CIP-014:* Seguridad Física

4.3.2 Investigación del Documento

4.3.2.1 Sobre el Cumplimiento y Monitoreo

Este documento establece que las entidades responsables deberán monitorear el nivel de cumplimiento de las medidas de control e informar al Coordinado para cada uno de los requerimientos que aparecerán a lo largo del presente documento. Tambien se establece que debe existir comunicación entre los actores mencionados en el estándar, ya que estas entidades responsables tendrán que notificar, a través del Encargado CIP, los incidentes de ciberseguridad reportables al Coordinador, a la Superintendencia de Electricidad y Combustible, y otras autoridades que defina esta misma.

Bajo el mismo lineamiento es que se recomienda establecer un Sistema de Gestión de Seguridad de la Información que, entre otras cosas, incorpore modelos e indicadores que permitan medir el nivel de madurez del organismo en materias de ciberseguridad y su conformidad respecto al estándar.

Estas obligaciones responden al requerimiento de lograr una comunicación eficaz y transparente de la información crítica y/o de interés para cada parte interesada, que se podría considerar esencial y el común a lo largo de las regulaciones, normas y estándares en las que se busca sentar los lineamientos en temas de ciberseguridad en Chile.

Debido a estos dos párrafos se reiterará buscar implementar en la solución propuesta sistemas y procesos que permitan a las partes interesadas acceder a la información requerida tanto para la conformidad de las regulaciones como para el interés propio de la empresa.

4.3.2.2 Sobre la Reserva y Confidencialidad

Se establece a la obligación de la empresa responsable de implementar procedimientos para preservar el carácter de reservado de la Información Reservada, incluyendo firmar acuerdos de confidencialidad necesarios, por lo que como organismo no relacionado que proveerá una solución a esta empresa, se deberá incluir una referencia para estos casos.

4.3.2.3 Sobre los Criterios para Calificación de Impacto

Gracias a los criterios para la calificación de Ciber Sistemas SEN, uno de los pilares del estándar, ya que, se puede asegurar una respuesta y protección adecuada para los distintos incidentes de ciberseguridad dependiendo de los impactos adversos que podría provocar. Esta calificación se presentará en niveles como Impacto Alto, Medio y Bajo.

Los Centros de Control utilizados por las empresas coordinadas corresponden a quizás las salas más importantes para lograr asegurar disponibilidad a través del monitoreo de los activos que operan, por lo que está clasificado como uno de los dos tipos de instalaciones existentes de Impacto Alto.

Dentro de las clasificadas en la categoría de Impacto Medio están las instalaciones de transmisión pertenecientes al sistema de transmisión nacional junto con las instalaciones de transmisión conectadas directamente al sistema de transmisión nacional, que además pertenezcan a sistemas de transmisión dedicados o zonales con niveles de tensión igual o superior a 220kV. Otro tipo dentro de esta categoría son las instalaciones de transmisión identificadas como necesarias para no violar los limites de transmisión durante contingencias.

Para casos futuros en los que se incluya el uso de artefactos IoT que requieran conexión al equipo de estas instalaciones, será necesario tomar los resguardos necesarios para abarcar los requisitos que el estándar asigne a las instalaciones de este tipo, ya que, hasta el momento de escribir este documento la solución no contempla estas conexiones o tecnologías, pero si vale la pena mencionar esto.

Finalmente, dentro de la calificación de Impacto Bajo están las Instalaciones de transmisión del SEN que no lograron entrar en las descripciones anteriores.

Estos son los Ciber Sistemas SEN con los que la solución interactuará, ahora con los Centros de Control, y en un futuro con las instalaciones de transmisión.

4.3.2.4 Estándares NERC-CIP

La sección 7 del estándar principal contiene los subestándares NERC-CIP presentados a continuación, con definiciones aplicables al contexto de la solución.

<u>CIP-002 – Categorización de Ciber Sistemas</u>

Este estándar tal y como se mencionó anteriormente cumple con el propósito de identificar y categorizar los Ciber Sistemas SEN y sus Ciber Activos. Es de acuerdo a esta clasificación que la entidad responsable establecerá las protecciones y protocolos adecuados para la interacción con estos Ciber Activos, por lo que podría sugerir una necesidad de flexibilizar, o generalizar las políticas sobre la interacción con estos sistemas, buscando una definición que se pueda adaptar para la distinta categorización establecida en este estándar y los futuros cambios de categoría de los activos, que en circunstancias normales, se deberían revisar al menos una vez cada 15 meses

CIP-003 – Controles de Gestión de la Seguridad.

Este estándar tiene como propósito el especificar los controles de gestión de la seguridad que establezcan la responsabilidad para proteger Ciber Sistemas SEN contra eventos que puedan afectar el correcto funcionamiento del SEN.

El requisito 1 de este estándar nos sugiere que para ciber sistemas SEN de Impacto Alto y Medio deben existir políticas sobre Reportes de Incidentes y Planes de Respuesta, Protección de la Información, y Gestión de Cambio de Configuraciones y Evaluación de Vulnerabilidades, por lo que esto se incluirá en las políticas para la interacción de la solución con estas entidades responsables.

También para la interacción con activos que contengan Ciber Sistemas de Impacto Bajo, si es que existen, se deberá incluir en las políticas para la interacción con las entidades responsables temas como controles de acceso electrónico y respuesta a incidentes de ciberseguridad.

Es importante destacar que estos Ciber Sistemas de Impacto Bajo tienen planes de ciberseguridad establecidos para las temáticas vistas en la sección 7.2.4 del estándar. En este contexto, los tópicos de interés que este plan debe aplicar son los siguientes:

Conciencia de Ciberseguridad: En este estándar, se puede rescatar el hecho que, al menos una vez cada 15 meses calendario, la entidad deberá reforzar sus prácticas de ciberseguridad, por lo que seria de gran apoyo para estos eventos se ponga a disposición un documento con buenas practicas y los procedimientos para interactuar con la solución propuesta

Control de Acceso Electrónico: En este estándar se puede destacar el inciso que establece que la entidad responsable deberá permitir solo el acceso electrónico entrante y saliente necesario para las comunicaciones, siendo uno de los escenarios la interacción entre un Ciber Sistema de Impacto Bajo y un Ciber Activo fuera del activo que contenga a este Ciber Sistema. Como podría ser la comunicación entre las instalaciones y los centros de control, o el centro de control y estos servicios tercerizados.

Respuesta a Incidentes de Ciberseguridad: En este estándar se menciona la obligación de contar con al menos un plan de respuesta a incidentes de ciberseguridad, ya sea por activo o grupo de activos. Estos planes deberán incluir elementos básicos, tales como seria la clasificación y respuesta a estos incidentes, la identificación de roles y responsabilidades, el periodo de tiempo entre cada testeo del plan y una posible actualización de estos planes en respuesta a un testeo.

Mitigación de Riesgos de Código Malicioso en Ciber Activos Transitorios y Medios Removibles: Como el nombre del estándar lo indica, esta establece la obligación de implementar al menos un plan para mitigar el riesgo de introducción de código malicioso en Ciber Sistemas SEN de Impacto Bajo a través de Ciber Activos Transitorios y Medios Removibles.

Clasificación Ciber Activos Transitorios

Dentro de la categoría de Ciber Activos Transitorios podrían ir los distintos dispositivos que en futuras funcionalidades establecerían comunicación entre estas instalaciones y la solución propuesta.

En las especificaciones necesarias para el plan, se establece que para Ciber Activos Transitorios gestionados por terceros, se deberá hacer uso de al menos uno de los siguientes métodos antes de su conexión a un Ciber Sistema SEN de Impacto Bajo.

- Revisión del nivel de actualización del antivirus
- Revisión del proceso de actualización del antivirus utilizado por terceros
- Revisión de la aplicación de lista blanca utilizadas por terceros
- Revisión del uso de sistemas operativos vivos y software ejecutable solo desde medios de lectura
- Revisión del reforzamiento de sistemas utilizado por terceros
- Otros métodos para mitigar la introducción de código malicioso

<u>CIP-004 – Personal y Capacitación</u>

Este estándar busca minimizar los riesgos derivados de los actos de individuos que interactúen con Ciber Sistemas SEN, exigiendo conciencia de seguridad y capacitación del personal.

El ítem 3.4 de la tabla de requerimientos del estándar establece que la evaluación de riesgos del personal realizado para terceros o proveedores de servicio cumplen con procesos tales como los de confirmar identidad, verificar antecedentes de riesgos y la evaluación de estos para la autorización de accesos.

También es conveniente destacar que, según el ítem 4.1 de la misma tabla menciona cuales son los accesos que requerirán un proceso para la autorización. Es de nuestro interés conocer y aplicar los cambios necesarios para satisfacer los procesos de acceso electrónico y a las localizaciones de almacenamiento designados para la información de Ciber Sistemas SEN.

<u>CIP-005 – Perímetro de Seguridad Electrónica</u>

El propósito de este estándar es administrar el acceso electrónico a Ciber Sistemas SEN utilizando un Perímetro de Seguridad Electrónica para apoyar la protección de estos sistemas contra eventos que afecten el correcto funcionamiento del Sistema Eléctrico Nacional.

El ítem 1.3 nos presenta el primer requerimiento de nuestro interés especificado en el estándar. Este requerimiento habla sobre el control que se debe tener sobre el permiso de acceso entrante y saliente a estos Perímetros de Seguridad Electrónica.

Otro tema que se menciona es que las entidades responsables tendrán uno o más métodos para detectar comunicaciones maliciosas, tanto para comunicaciones entrantes y salientes, por lo que se deberá considerar estos para asegurar la correcta comunicación entre la solución y los Ciber Sistemas SEN.

Los ítems 2.1, 2.2 y 2.3 mencionan que, para el acceso remoto interactivo, se usará un Sistema Intermedio con el fin de evitar una comunicación directa con el Ciber Activo, además de hacer uso de encriptación y autenticación multi-factor para añadir más capas de seguridad a estas sesiones

CIP-007 – Gestión de la Seguridad de Sistemas

Como su nombre sugiere, el propósito del estándar es gestionar la seguridad de sistemas especificando los requerimientos técnicos, operaciones y procedimentales para la protección de Ciber Sistemas SEN contra eventos que afecten el correcto funcionamiento del Sistema Eléctrico Nacional

En los requerimientos se destaca el correcto uso de puertos y la administración de parches de seguridad por parte de la entidad responsable, esto último pudiendo ser un buen agregado a las políticas de nuestro caso. También se habla sobre la previsión de código malicioso, como por ejemplo los ítems 3.1 y 3.2 que mencionan la implementación de métodos para prevenir, detectar y mitigar código malicioso

El tópico que más nos concierne es el del monitoreo de eventos de seguridad, partiendo por el ítem 4.1 que establece la obligación de registrar eventos a nivel de Ciber Sistema SEN o Ciber Activo para la gestión de incidentes de ciberseguridad tales como intentos fallidos de inicio de sesión, o también código malicioso detectado.

Siguiendo la misma línea, el ítem 4.2 menciona que se deberá generar alertas para los eventos que la entidad responsable determine sea necesario.

Se vuelve a hacer énfasis en los registros o eventos, ya que según el ítem 4.3 se requerirá guardar estos por al menos 90 días calendario, a excepto bajo circunstancias excepcionales. Con estos eventos se usarán para crear, en intervalos de hasta 15 días calendario, resúmenes sobre inicios de sesión con el objetivo de identificar incidentes de ciberseguridad no detectados.

Por último, se deberá considerar los requerimientos de nuestro interés en el mismo estándar sobre Controles de Acceso a Sistemas, haciendo énfasis mayoritariamente en tópicos de autenticación, mencionando cambios de contraseña en intervalos de, por ejemplo, 15 meses, en sistemas que solo usen contraseña para este proceso.

CIP-008 – Reporte de Incidentes y Planes de Respuesta

El propósito de este estándar es mitigar los riesgos en la operación del sistema eléctrico nacional a raíz de un incidente de ciberseguridad, especificando los requerimientos necesarios para responder ante estos incidentes.

En resumen, en la tabla de requerimientos se menciona la obligación de implementar uno o más procesos para la identificación, clasificación y respuesta a estos incidentes, incluyendo criterios para evaluar y definir intentos de compromiso a los Ciber Sistemas SEN, por lo que se requerirá la presencia de tecnologías y herramientas que puedan aportar a documentar la información requerida por las entidades responsables en estos casos.

Dentro de la información solicitada destaca el impacto funcional, el vector de ataque y el nivel de intrusión que se logró a raíz del incidente de ciberseguridad, con el fin de notificar con la mayor cantidad de detalles a las partes interesadas los incidentes de ciberseguridad, para así en un futuro actualizar los planes de respuesta a estos incidentes y promover la mejora continua de estos procesos.

CIP-010 – Gestión de Cambio de Configuración y Evaluación de Vulnerabilidades

El propósito de este estándar es prevenir y detectar cambios no autorizados a Ciber Sistemas SEN que puedan afectar al correcto funcionamiento del Sistema Eléctrico Nacional.

Dentro de los requisitos más destacables para nuestro caso son los requerimientos en los Planes para Ciber Activos Transitorios gestionados por terceros, equipo que podría estar relacionado con futuras funcionalidades de la solución propuesta.

Estos planes requerirán la implementación de procesos para mitigación de vulnerabilidades e introducción de código malicioso. Dentro de los métodos usados se destacan tales como la revisión de los procesos de parches de seguridad usados por terceros y sus métodos para la mitigación de vulnerabilidades. Otro tópico que se revisa en los terceros es el nivel de actualización de antivirus y sus procesos para estas actualizaciones, además de la aplicación de lista blanca, sistemas operativos, softwares ejecutables y otros métodos para mitigar la introducción de código malicioso.

CIP-011 – Protección de Información

El propósito de este estándar es prevenir el acceso no autorizado a información en Ciber Sistemas SEN, intentando evitar la fuga o corrupción de información que su mal uso represente una amenaza al Sistema Eléctrico Nacional

El único requerimiento aplicable a nuestro caso sugiere una necesidad de gestionar correctamente el almacenamiento, tránsito y uso de la información de Ciber Sistemas SEN, por lo que se requerirá el uso de protocolos seguros de transferencia de datos para las comunicaciones entre la solución y la entidad responsable

CIP-013 – Gestión de Riesgos en la Cadena de Suministros

Este estándar, quizás el que más afecta al proveedor de servicios y software, habla sobre mitigar los riesgos de ciberseguridad en la cadena de suministro, implementando controles de seguridad para la correcta gestión de estos riesgos.

En los requerimientos se establece la obligación de la entidad responsable de desarrollar al menos un plan documentado para la gestión de este tipo de riesgos.

En la compra de Ciber Sistemas SEN, se deben aplicar procesos para solicitar al fabricante cumplir los siguientes requisitos

- Notificar incidentes relacionados a productos o servicios suministrados
- Coordinar la respuesta a estos incidentes
- Notificar cuando el acceso remoto o local ya no se requiera para el fabricante
- Divulgar las vulnerabilidades conocidas relacionadas a productos o servicios suministrados
- Verificación de la integridad y autenticidad de todo software y parche suministrado para el uso en Ciber Sistemas SEN
- Coordinar controles para el acceso remoto con el fabricante.

4.5 Ley Marco de Ciberseguridad e Infraestructura Crítica

Después del periodo de la pandemia, empezaron a surgir en todo el mundo muchos estudios y noticias sobre ataques de ciberseguridad a distintas escalas, pero según reveló IBM en una entrevista con Infobae, en el año 2022 la situación en Latinoamérica, específicamente en Brasil, México y Perú, se

caracterizó por dos tipos en específico, el phishing y el ransomware, este último representando el 61% de los casos reportados.

Misma es la situación en Chile, ya que el Reporte Ciberseguridad 2024 de Entel Digital ubicó a Chile en la cuarta posición de los países más afectados con ransomware en la región para el periodo del año 2023, el cual tuvo un aumento del 200% respecto al año anterior en los ataques de este tipo.

Un panorama así logró apresurar las discusiones en el congreso, las cuales después de 1 año culminaron en la aprobación de la Ley Marco de Ciberseguridad e Infraestructura Critica por parte del Senado de Chile, esto a mitades de diciembre del 2023. La promulgación no tuvo lugar hasta el día 8 de abril del 2024, con su publicación en el diario oficial marcando este hito histórico en la región de Latinoamérica.

En el contexto actual, con la implementación de la Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información y la aprobación de la Política Nacional de Ciberseguridad 2023-2028, Chile se convierte en el país pionero en temas de Ciberseguridad, logrando posicionarse a la fecha de 21 de septiembre del 2024, en el 2do puesto del ranking National Cyber Security Index.

4.5.1 Contenidos del Documento

La Ley Marco de Ciberseguridad e Infraestructura Crítica cuenta con 10 títulos, los cuales contendrán 55 de los 61 artículos descritos en esta ley. Estos títulos son:

- Disposiciones generales (Articulo 1 al 3)
- Obligaciones de ciberseguridad (Articulo 4 al 9)
- Objeto, naturaleza y atribuciones (Articulo 10 al 24)
- Coordinación regulatoria y otras disposiciones (Articulo 25 al 28)
- Del Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional (Articulo 29 al 32)
- De la reserva de información en el sector público en materia de ciberseguridad (Articulo 33 al 36)
- De las infracciones y sanciones (Articulo 37 al 47)
- Del Comité Interministerial sobre Ciberseguridad (Articulo 48 al 52)
- Órganos autónomos constitucionales (Articulo 53)
- De las modificaciones a diversos cuerpos legales (Articulo 54 y 55)

Los 6 artículos restantes pertenecen a las Disposiciones Transitorias para la aplicación de la ley descrita.

4.5.2 Investigación del Documento

Para la investigación de este documento, se buscará identificar todos los artículos los cuales para su conformidad sea necesaria la participación de los proveedores de servicios tercerizados, con el objetivo de implementar las medidas necesarias para facilitar el cumplimiento de los requerimientos legales de las partes interesadas.

4.5.2.1 Contexto

Intentando entender el contexto, el articulo 1 de esta ley establece que el objeto de la ley es:

- Establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares
- Establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad
- Establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones determinadas en el articulo 4, y los mecanismos de control, supervisión y de responsabilidad ante infracciones

Estos tres puntos ya sugieren que esta ley no definirá a nivel muy técnico los procedimientos y mecanismos de control a usar en casos de incidentes de seguridad informática, si no más bien, establecer obligaciones, protocolos generales sobre el actuar de los particulares y organismos del estado frente a estos eventos, e infracciones por el no cumplimiento de estos últimos dos.

Además, se crearon dos entidades nuevas en el entorno cibernético del país, la Agencia Nacional de Ciberseguridad, bajo las siglas ANCI, y el Equipo de Respuesta ante Incidentes de Seguridad Informática de la Defensa Nacional, bajo las siglas CSIRT.

- La ANCI, de carácter técnico y especializado, cumplirá con los objetivos de asesorar al presidente en materias de ciberseguridad, colaborar en la protección de los intereses nacionales en el ciberespacio, coordinar el actuar de las instituciones y los organismos de la administración del estado en materia de ciberseguridad
- El CSIRT está encargado de coordinar, proteger y asegurar las redes y sistemas del Ministerio de Defensa Nacional, servicios esenciales y operadores vitales para la defensa nacional.

Estas dos entidades participarán activamente en la regulación y cumplimiento de la mayoría de los artículos escritos en esta ley, lo que las posiciona como los pilares fundamentales para la estructura de ciberseguridad del país.

4.5.2.2 Artículos de Interés

Articulo 4

Especifica que la ley se les aplicará a las instituciones que presten servicios calificados como esenciales según el inciso segundo y tercero del mismo artículo. El inciso segundo define los servicios esenciales como aquellos provistos por los organismos de la Administración del Estado y por el Coordinador Eléctrico Nacional. Más adelante en este articulo también se mencionan instituciones privadas que participen en la generación, transmisión o distribución eléctrica.

Esta definición es muy importante teniendo en cuenta que la solución actual solo contempla a las empresas que responden al Coordinador Eléctrico Nacional, pero se ha mencionado en un futuro la posibilidad de expandirse a mercados como lo podría ser el minero, conocido por ser propietario de una gran cantidad de kilómetros en líneas de transmisión construidas.

Articulo 5

Los operadores de importancia vital están definidos como prestadores de servicios esenciales tales que su provisión dependa de las redes y sistemas informáticos y que su afectación, interceptación, interrupción o destrucción tenga un impacto significativo en la seguridad y orden público, en la provisión continua y regular de servicios esenciales, y en el cumplimiento de las funciones del Estado. Las

instituciones privadas que entran en esta definición cumplen los requisitos anteriores, y además tienen un rol critico en el abastecimiento de la población, la distribución de bienes o la producción de aquellos indispensables o estratégicos para el país.

Tomando el ejemplo anterior, Chile al ser un país en el que su economía esta fuertemente relacionada al rendimiento del sector minero, estos también entrarían en la definición de operador de importancia vital.

Articulo 7

Los deberes generales se aplicarán a todas las instituciones abarcadas por la ley, ya sean operadores de vital importancia, o solo prestadores de servicios esenciales. Estos deberes abarcan desde las medidas para prevenir y gestionar riesgos asociados a la ciberseguridad, hasta el reporte y resolución de incidentes de ciberseguridad que amenacen la continuidad operacional del servicio o la confidencialidad e integridad de la información o sistemas informáticos.

Dentro de las responsabilidades que se podrían proponer como proveedor se deberá incluir mecanismos para registrar todos los incidentes de seguridad que afecten a los distintos componentes y módulos de la solución, pudiendo incluir indicadores de compromiso u otros artefactos que tengan relación con el incidente a reportar.

Articulo 8

Para el caso de los deberes específicos de los operadores de importancia vital, uno de los requisitos mostrados es implementar un sistema de gestión de seguridad de la información que determine los riesgos que puedan afectar los objetivos de seguridad del negocio, lo que sugiere un enfoque basado en estándares internacionales, como puede ser la norma ISO 27001, usualmente asociada a este tipo de sistemas de gestión.

Uno de los deberes específicos es el de someterse a revisiones periódicas con una frecuencia mínima de dos años, además de realizar continuamente revisiones, ejercicios, simulacros y análisis de las redes, sistemas informáticos, entre otros elementos que comprometan la ciberseguridad, debiendo comunicar la información de estas acciones al CSIRT, lo que refuerza la necesidad de disponibilizar la mayor cantidad de artefactos resultantes de las operaciones del cliente para apoyar el cumplimiento de estas obligaciones.

Otro deber que deben cumplir este tipo de operadores es el de informar a los potenciales afectados sobre la ocurrencia de incidentes que pudieran comprometer su información o redes y sistemas informáticos, haciendo énfasis en los que estén involucrados datos sensibles, así que será necesario establecer un canal de información en el que se emitan alertas al momento de ocurrir un incidente de ciberseguridad, buscando minimizar el tiempo de respuesta del operador que necesita cumplir estas regulaciones.

De no cumplir alguno de estos deberes, según el artículo 39 los operadores de importancia vital podrán ser sancionados, calificando estas faltas como leves, graves y gravísimas.

Articulo 9

Se especifica como deber de las instituciones obligadas por la ley, el reportar al CSIRT Nacional los incidentes de ciberseguridad que puedan tener efectos significativos, teniendo que cumplir ciertos protocolos según el tiempo transcurrido desde el conocimiento del incidente de ciberseguridad.

A las tres horas, una alerta temprana sobre la ocurrencia del incidente. A las 72 horas, una actualización de la primera información, incluyendo una evaluación preliminar del incidente, gravedad, impacto e indicadores de compromiso, siendo este plazo reducido a 24 horas para los operadores de importancia vital. Por último, a los 15 días de haber enviado la alerta, se deberá entregar un informe final que incluya una descripción detallada del incidente, el tipo de amenaza o causa principal, las medidas de mitigación aplicadas y en curso, y si es necesario, las repercusiones transfronterizas del incidente.

Será este articulo el que se establezca como referencia para los tiempos de respuesta mínimos que se propondrá como responsabilidad del proveedor de la solución.

Articulo 26

Establece que "las autoridades sectoriales podrán emitir normativas [...] e instrucciones necesarias para fortalecer la ciberseguridad en las instituciones de su sector." lo que las instituciones supervisadas por la autoridad deberán cumplir de manera obligatoria, lo que significa que, para poder lograr la conformidad con esta ley, se deberá lograr también la conformidad con las normativas sectoriales.

Articulo 27

Establece que un incidente de ciberseguridad es de efecto significativo si es capaz de interrumpir la continuidad de un servicio esencial, afectar sistemas informáticos con datos sensibles, la integridad física o la salud de las personas, además de tomar mayor atención a criterios como el numero de personas afectadas, la duración del incidente, o la extensión geográfica del incidente

La recurrente mención de datos sensibles a lo largo del documento de la ley hace crecer la necesidad casi obligatoria en la era digital de políticas robustas en cuanto a protección de datos, buscando asegurar elementos como la confidencialidad, integridad y disponibilidad de estos.

En este mismo contexto, esta ley también califica como reservada o secreta la información de los sistemas de gestión de seguridad de la información y los registros previstos en el artículo 8°, intentando evitar su divulgación, comunicación o conocimiento con el fin de resguardar la seguridad y los intereses de la Nación.

4.6. Matriz de Riesgos

La gestión de riesgos es un proceso esencial a la hora de construir las bases de una solución segura que permita entender las necesidades del negocio con respecto a los requisitos de seguridad de la información. [8]

Las actividades para la gestión de riesgos de seguridad de la información, según la norma ISO 27005, abarca la evaluación, tratamiento, aceptación, comunicación y monitoreo.

En este caso, realizaremos una evaluación de riesgos para así crear una matriz de riesgos, basándonos en lineamientos descritos por la norma.

4.6.1 Descripción de la Solución

La solución, en formato simplificado, que se presenta es un modelo predictivo de fallas en las líneas de transmisión eléctrica. Esta solución se espera desplegarla en Amazon Web Services a través del servicio

[8] ISO/IEC 27005:2018 Information Technology – Security Techniques – Information security risk management, p.2.

API Gateway, que se encargará de consumir el modelo predictivo alojado en Amazon Sagemaker usando como intermediario funciones Lambda que manejen la lógica de negocio.

El entrenamiento de este modelo se incluirá en el servicio de Sagemaker, consumiendo datos desde unidades de almacenamiento S3.

Se espera que, con fines de mejorar la solución y ofrecer nuevas funcionalidades, las empresas entreguen datos operacionales que pueden ser catalogados como sensibles.

4.6.2 Inventario de Activos

Dentro de la evaluación del riesgo se debe determinar el valor de los distintos activos que se poseen, por lo que un inventario de activos ayudará a deliberar la criticidad de estos en lo que a confidencialidad, integridad y disponibilidad se refiere.

Este inventario de activo considerará activos principales y sus dependencias, adjuntando una breve descripción y una valoración según su confidencialidad, integridad y disponibilidad.

Activo	Descripción	Valoración		
		C	I	D
Modelo de Machine Learning	Modelo entrenado y desplegado en Sagemaker	Alta	Media	Alta
Datos de Entrenamiento	Datos de entrenamiento de fuentes publicas	Baja	Media	Baja
Funciones Lambda	Código que ejecuta lógica de negocio	Media	Alta	Alta
API Gateway	Punto de entrada para consumir el modelo	Media	Alta	Alta
Datos Sensibles de Clientes	Datos entregados por el cliente para uso y mejora de solución	Alta	Alta	Baja
Roles y Políticas IAM	Permisos para control de acceso a recursos y servicios	Alta	Alta	Alta
Infraestructura de Nube	Redes y entornos que alojan la solución	Media	Alta	Alta
Registros y Métricas	Información sobre eventos, métricas y trazabilidad	Alta	Alta	Media
Credenciales Privilegiadas	Credenciales o llaves de acceso a recursos y servicios	Alta	Alta	Alta
Sistemas de Monitoreo	Herramientas de monitoreo de la solución	Media	Media	Alta

Tabla 1. Inventario de Activos de la Solución

4.6.3 Identificación de amenazas y vulnerabilidades

Una vez se tiene un inventario de activos, es necesario realizar una identificación de amenazas y vulnerabilidades asociadas a estos mismos activos. En una instancia inicial, es esencial hacer un levantamiento de las amenazas más comunes, entendiendo que existe un cambio continuo en las amenazas más relevantes, según vaya evolucionando la solución, el negocio y el entorno.

En esta siguiente tabla, se mostrarán las amenazas y vulnerabilidades más relevantes para cada activo:

Activo	Amenaza	Vulnerabilidad
Modelo de Machine Learning	Filtración de código fuente del modelo	Cifrado débil o control inadecuado de acceso
Datos de Entrenamiento	Manipulación de datos en fuentes publicas	Falta de control sobre fuente
Funciones Lambda	Abuso de funciones o errores lógicos	Permisos IAM excesivos o ausencia de datos
API Gateway	Ataques DDoS o acceso no autorizado	Configuración débil de soluciones de seguridad
Datos Sensibles de Clientes	Exfiltración o modificación de datos de clientes	Exposición no esperada o gestión de accesos débil
Roles y Políticas IAM	Escalación de privilegios	Políticas excesivamente permisivas o generales
Infraestructura de Nube	Indisponibilidad o sabotaje	Falta de redundancia en infraestructura
Registros y Métricas	Exfiltración de información sensible	Exposición no esperada o gestión de accesos débil
Credenciales Privilegiadas	Robo o uso indebido	Almacenamiento inseguro o falta de rotación
Sistemas de Monitoreo	Indisponibilidad o sabotaje	Gestión de accesos débil o configuración errónea

Tabla 2. Amenazas y vulnerabilidades principales por activo

4.6.4 Análisis de Riesgo

El riesgo suele definirse a lo largo de distintas normas y marcos de referencia como la combinación de la posibilidad de que ocurra un evento perjudicial y el impacto negativo que este tendría.

Para poder realizar la evaluación de los riesgos, se definió las siguientes escalas para la probabilidad y el impacto:

Probabilidad:

1. Rara vez
2. Poco probable
3. Posible
4. Probable
5. Muy probable

Impacto:

1. Insignificante
2. Menor
3. Moderado
4. Mayor
5. Critico

El resultado de la evaluación de los riesgos según las amenazas levantadas se muestra en la siguiente tabla, asignando un puntaje calculado como la multiplicación de los valores de probabilidad e impacto:

Amenaza	Probabilidad	Impacto	Puntaje
Filtración de código fuente del modelo	1	4	4
Manipulación en datos de fuentes publicas	2	3	6
Abuso de funciones o errores lógicos	3	4	12
Ataques DDoS o acceso no autorizado	4	5	20
Exfiltración o modificación de datos de clientes	2	5	10
Escalación de privilegios	4	4	16
Indisponibilidad o sabotaje	2	5	10
Exfiltración de información sensible	3	4	12
Robo o uso indebido	4	4	16
Indisponibilidad o sabotaje	3	4	12

Tabla 3. Evaluación de riesgo por amenaza

4.6.5 Visualización del resultado

La visualización del resultado en una matriz de riesgo se mostrará en la siguiente tabla, asignando categorías según umbrales especificados en la leyenda de esta:

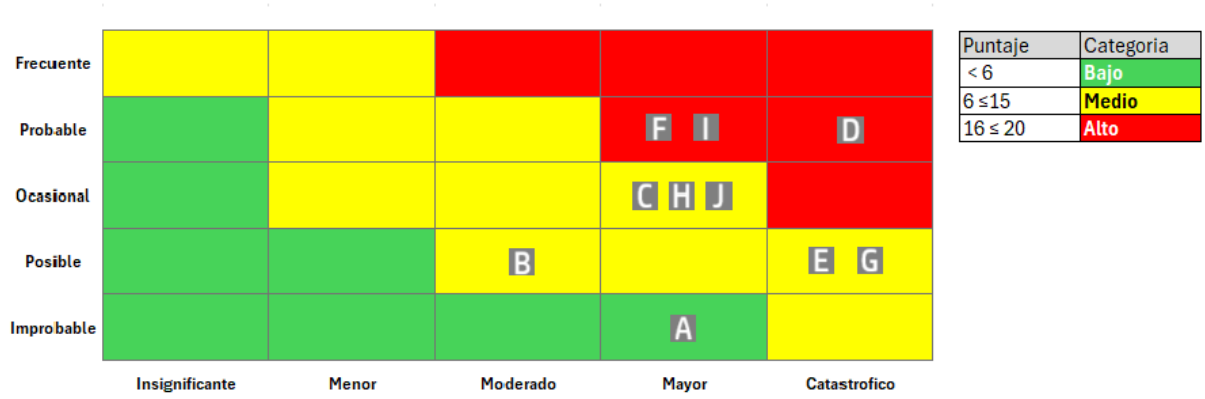

Figura 1. Matriz de riesgo resultante

Riesgos:

a. Filtración de código fuente del modelo
b. Manipulación en datos de fuentes publicas
c. Abuso de funciones o errores lógicos
d. Ataques DDoS o acceso no autorizado
e. Exfiltración o modificación de datos de clientes
f. Escalación de privilegios
g. Indisponibilidad o sabotaje
h. Exfiltración de información sensible
i. Robo o uso indebido
j. Indisponibilidad o sabotaje

k.

4.7 Políticas de Seguridad

Una política de seguridad robusta puede aportar beneficios clave como garantizar la confianza entre partes, reducir el riesgo de incidente, y asegurar la continuidad operativa, es por esto por lo que estas deben estar siempre alineadas con los requisitos del negocio.

Para efectos de este caso, nuestras políticas se dividirán en 6 categorías esenciales que serán abarcadas cada una según el contexto de la solución y sus riesgos, y además las buenas prácticas descritas en las normas abarcadas en este documento.

4.7.1 Seguridad de la Información

- El proveedor del servicio deberá implementar los métodos y protocolos necesarios para asegurar la confidencialidad, integridad y disponibilidad de la información, ya sea que esta esté en uso, en tránsito o en almacenamiento.
- El usuario debe asegurar la confidencialidad de sus credenciales de acceso, informando según sea necesario si se observa comportamiento sospechoso relacionado con estas.
- El usuario debe informar al proveedor del servicio con anticipo el cambio en la clasificación de la información reservada o sensible
- El proveedor del servicio deberá seguir el principio de mínimo conocimiento para otorgar acceso a información sensible o de carácter reservado, siempre respetando los acuerdos de confidencialidad.
- El usuario deberá presentar los acuerdos de confidencialidad necesarios antes de poder clasificar como reservada la información de su propiedad.

4.7.2 Cumplimiento Normativo y Transparencia

- El usuario deberá informar al proveedor del servicio sobre los requisitos de seguridad necesarios para lograr la conformidad con las normas y regulaciones que apliquen en su contexto.
- El proveedor del servicio deberá aplicar los requisitos de seguridad establecidos por las normas y regulaciones que el usuario debe cumplir para lograr su conformidad con estos documentos.
- El usuario deberá indicar en el acuerdo de prestación de servicios los artefactos y el nivel de detalle que requiere en el registro de los eventos e incidentes de ciberseguridad.
- El proveedor del servicio deberá disponibilizar un registro de los eventos de ciberseguridad clasificados como de interés, según el acuerdo de prestación de servicios.
- El proveedor del servicio deberá disponibilizar el historial de incidentes de ciberseguridad relacionados con el servicio prestado, incluyendo los artefactos requeridos por el usuario para cumplir las normas y regulaciones.
- El proveedor del servicio deberá notificar los incidentes de ciberseguridad con el nivel de detalle requerido por los usuarios afectados.
- El usuario deberá indicar en el acuerdo de prestación de servicios los intervalos de tiempo mínimos para notificar los incidentes de ciberseguridad.
- El proveedor del servicio deberá cumplir con los intervalos de tiempo mínimos para notificar incidentes de ciberseguridad y sus detalles, según lo exijan las normas y regulaciones.

- El proveedor del servicio deberá disponibilizar la información requerida por el usuario para el monitoreo y evaluación de los activos informáticos relacionados con el servicio prestado.

4.7.3 Gestión de Activos y Servicios

- El proveedor del servicio deberá implementar métodos necesarios para reducir, según sea posible, la cantidad de activos expuestos a Internet.
- El proveedor del servicio deberá implementar medidas específicas de seguridad según la clasificación de los activos establecidos en el acuerdo de prestación de servicios.
- El proveedor del servicio deberá implementar métodos para identificar y mitigar código malicioso en los activos informáticos relacionados al servicio prestado.
- El proveedor del servicio deberá implementar uno o más planes de respuesta ante incidentes de ciberseguridad, con el objetivo de contener y minimizar el impacto de los incidentes en la seguridad de los activos informáticos.
- El proveedor del servicio deberá implementar protocolos que minimicen los riesgos asociados a la autorización de accesos a activos informáticos.
- El proveedor del servicio deberá implementar políticas de gestión de contraseñas que incluyan, como mínimo, los métodos de autenticación, los requisitos para la creación de credenciales y el tiempo de caducidad de estas.

4.7.4 Comunicación y Buenas Prácticas

- El proveedor del servicio deberá implementar los procesos y canales necesarios para lograr una comunicación eficaz y transparente de la información crítica o de interés para las partes interesadas.
- El proveedor del servicio deberá crear, disponibilizar y mantener un documento que muestre el correcto uso del servicio prestado, junto con las buenas prácticas asociadas a este.
- El usuario deberá seguir los procedimientos y las buenas practicas indicadas en el documento proporcionado por el proveedor.
- El proveedor del servicio deberá velar por el cumplimiento de los acuerdos de confidencialidad necesarios para mantener el carácter reservado de la información.

4.7.5 Gestión de Cambios

- El proveedor de servicios deberá establecer un plan de gestión de cambios para asegurar que cualquier cambio en la infraestructura o en el servicio sea planificado, probado, evaluado e implementado de manera controlada
- El proveedor deberá establecer los procesos necesarios para una correcta gestión de los parches de seguridad y las vulnerabilidades conocidas de software.
- El proveedor de servicios deberá documentar los cambios propuestos de forma detallada, incluyendo como mínimo la descripción del cambio, el impacto potencial, el plan de reversión y los resultados de las pruebas.
- El proveedor de servicios deberá comunicar de manera transparente a los usuarios sobre los cambios planificados y sus detalles con un plazo razonable de anticipación.
- El usuario deberá revisar y evaluar con anticipación los cambios planificados que puedan afectar su interacción con el servicio.
- El proveedor de servicios deberá monitorear los cambios realizados para evaluar el impacto real y garantizar su correcto funcionamiento después de la implementación

- El proveedor de servicios debe mantener un registro histórico de todos los cambios realizados y sus detalles con el fin de facilitar auditorias y la resolución de eventos o incidentes.

4.7.6 Recuperación

- El proveedor de servicios debe implementar un plan de recuperación del servicio ante desastres para garantizar la mínima interrupción del servicio y la recuperación de los datos, en un tiempo no menor a 1, 4 o 24 horas dependiendo si la criticidad del activo es alta, media o baja, respectivamente.
- El proveedor del servicio deberá gestionar un repositorio centralizado que registre de manera organizada y accesible las distintas versiones del servicio prestado o de los activos relacionados a este.
- El proveedor de servicios deberá realizar, mantener y almacenar copias de seguridad de los datos para mitigar incidentes de pérdida o corrupción de la información.
- El proveedor deberá asegurar que los procedimientos de recuperación sean documentados de manera correcta para lograr una acción correctiva rápida y eficaz.

4.8 Implementación en la Solución

La solución, en formato simplificado, que se presenta es un modelo predictivo de fallas en las líneas de transmisión eléctrica. Esta solución construida usando servicios de Amazon Web Services procesa y disponibiliza un modelo predictivo a través de Amazon Sagemaker entrenado con datos almacenados en una instancia S3. Posterior al entrenamiento, se despliega el modelo resultante en un punto de conexión de Sagemaker. Para su consumo, el usuario deberá consultar a un punto de conexión API Gateway, el cual llama a una función lambda que consulta al punto de conexión de Sagemaker desplegado anteriormente y devuelve la predicción al usuario a través del mismo punto de conexión API Gateway.

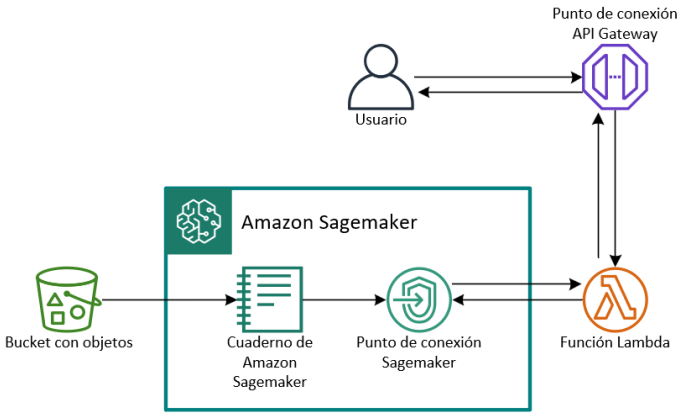

Figura 2. Diagrama de arquitectura de la solución

4.8.1 Implementación Política: Seguridad de la Información

En esta sección se solicita implementar los métodos y protocolos necesarios para asegurar la confidencialidad, integridad y disponibilidad de la información, en cualquiera de sus estados: en uso, en tránsito o en almacenamiento.

Según la guía de usuario de Amazon S3[9], todos los buckets S3 tienen configurado de manera predeterminada el cifrado del lado de servidor con claves administradas por AWS (SSE-S3). Este se refiere a que Amazon S3 cifra los objetos antes de guardarlos en los centros de datos.

Todo el transito de datos entrante y saliente de la función lambda también está encriptado de manera predeterminada por el protocolo TLS, ya que este por diseño solo acepta comunicación a través de HTTPS.

El uso de HTTPS/TLS es el estándar para garantizar que los datos no sean accesibles por terceros durante la transmisión, manteniendo las comunicaciones seguras y protegidas.

Es por esto que también, para la consulta del usuario a la API Gateway, será necesario ocupar HTTPS, pero esta vez haciendo uso de certificados SSL/TLS para nombres de dominio personalizado, permitiendo a los sistemas verificar la identidad de otro sistema para así establecer una conexión de red cifrada, logrando que solo el cliente y el servidor web puedan ver los datos que se envían, además de poder disfrutar de mejor escalabilidad y mantenimiento gracias a las herramientas de redireccionamiento que brinda un nombre de dominio.

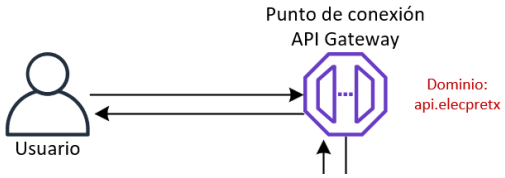

Figura 3. Etiqueta agregada al punto de conexión API Gateway

También se menciona que se deberá otorgar acceso a la información sensible o de carácter reservado utilizando el principio de mínimo conocimiento. Para esto, se requerirá generar un bucket S3 por cada cliente al que se le preste servicio, esto con el fin de almacenar de manera aislada la información sensible o de carácter reservado, facilitando la gestión de permisos y ayudando a mitigar el impacto en casos de que el activo de vea comprometido.

A continuación, se muestra el diagrama de la arquitectura, ya con la primera sección de la política implementada.

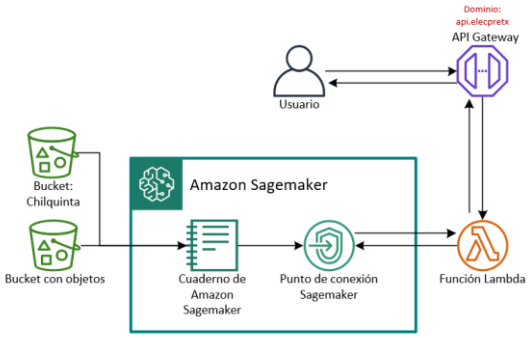

Figura 4. Diagrama de arquitectura hasta la sección 1

[9] Amazon Simple Storage Service – Guía del Usuario. Recuperado de https://docs.aws.amazon.com/es_es/AmazonS3/latest/userguide/s3-userguide.pdf

4.8.2 Implementación Políticas: Cumplimiento Normativo y Transparencia

Esta sección considera temas sobre el cumplimiento normativo y la transparencia necesaria con la información requerida para satisfacer esta necesidad de conformidad con las normas y regulaciones.

Será necesario hacer uso de servicios para mantener un registro de eventos de ciberseguridad que sean de especial interés para el usuario, y logre apoyar en la evaluación de métricas. La norma NERC CIP considera métricas como el N° de intentos de acceso no autorizado a recursos críticos, o N° de cambios en configuraciones de sistemas críticos, mientras que la ISO 27001 menciona métricas como N° de eventos con privilegios elevados o Tasa de éxito/fallo en autenticación MFA.

Amazon Cloudwatch es un servicio dedicado al monitoreo del rendimiento, estado actual de las aplicaciones y recursos con la capacidad de mantener un registro único y consistente de eventos ordenados de manera temporal.

A partir de toda la información que este servicio recolecta, se podrá levantar la documentación necesaria para apoyar al cliente a lograr la conformidad con las normas y regulaciones que exigen fuertes medidas de monitoreo y registro de eventos e incidentes de ciberseguridad.

De acuerdo con lo descrito, el diagrama resultante se muestra a continuación.

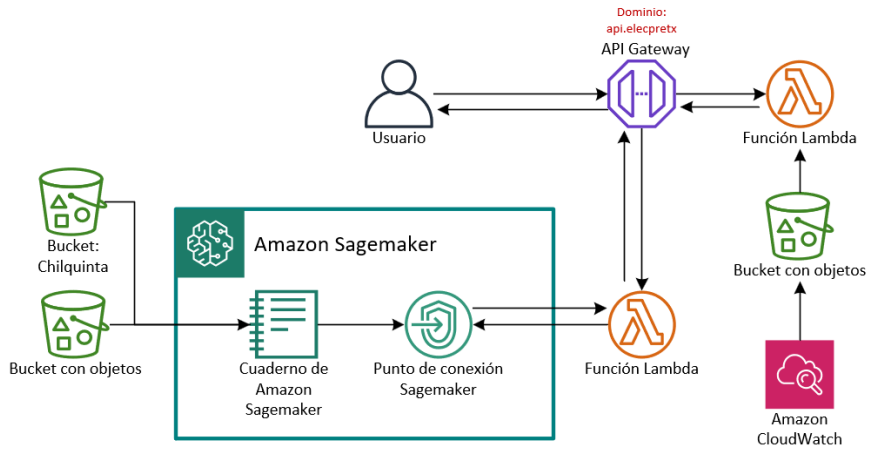

Figura 5. Diagrama de arquitectura hasta sección 2

4.8.3 Implementación Política: Gestión de Activos y Servicios

Esta sección trata tópicos sobre la gestión en temas de ciberseguridad de los activos informáticos y servicios prestados.

Primero, establece que se deberá trabajar en minimizar la cantidad de activos expuestos a internet. Hasta el momento, la mayoría de los recursos que se ven en el diagrama son accesibles a través de internet, por lo que se requerirá de crear una Virtual Private Cloud (VPC) para así aislar los activos en una nube privada virtual con acceso restringido, y solo permitir el trafico hacia internet a los activos que lo necesiten.

La implementación de esta Virtual Private Cloud inicialmente afectará a servicios como el punto de conexión de Sagemaker, que están expuestos a internet sin contar con una gestión de políticas de acceso por parte de AWS. La seguridad de activos como pueden ser los buckets de S3 es gestionada por

AWS por lo que existen fuera de la VPC, sin embargo, pueden ser ligados a una nube privada a través del servicio VPC Endpoints.

Se crearán dos subredes, la subred publica que contendrá los servicios que comunican con los usuarios e internet, y la subred privada que protegerá a los servicios relacionados con el negocio que no requieran de una conexión permanente a internet.

También se menciona la necesidad de establecer métodos para identificar y mitigar código malicioso presente en los activos informáticos. Para la identificación de este código ya podemos ocupar Amazon Cloudwatch para revisar los registros de eventos, pero para mitigar será necesario establecer reglas de filtrado WAF junto con el uso de un protocolo como CORS, que logren validar la solicitud entrante a la API, descartando así las solicitudes que no cumplan los requisitos de:

- Estar firmada correctamente con credenciales que tengan los permisos necesarios
- Enviar el cuerpo de la petición con la interfaz solicitada para las peticiones de inferencia
- Enviar las cabeceras correctas según configuración del protocolo CORS

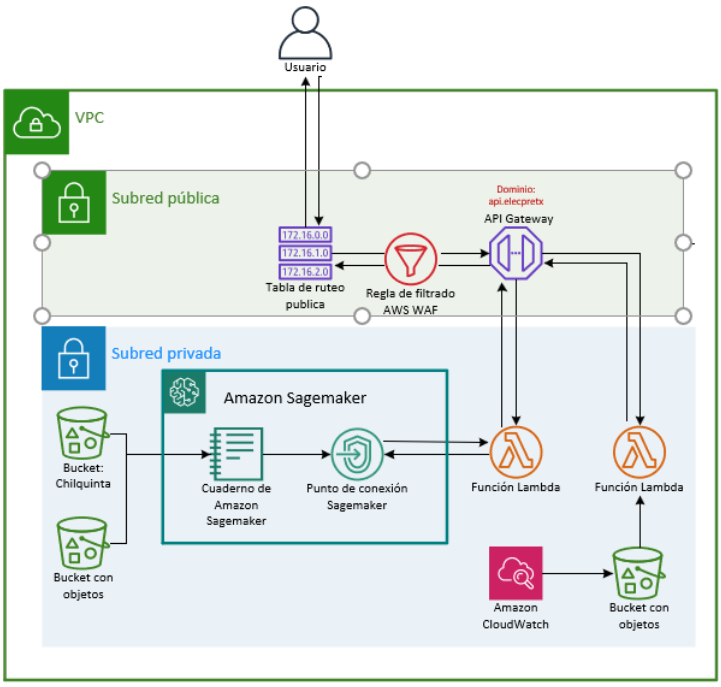

Figura 6. Arquitectura con las reglas de filtrado y la definición de la VPC

Por último, se establece que se deben implementar fuertes planes para la gestión de contraseñas y los riesgos de ciberseguridad asociados a la autorización de acceso a activos informáticos.

Es por esto por lo que se deberá hacer uso de AWS IAM, servicio utilizado para gestionar identidades, permisos y grupos de seguridad que sirvan para solo permitir el acceso a los usuarios autorizados a servicios y recursos de AWS. Hacer uso de este servicio nos da las herramientas para gestionar los permisos utilizando la granularidad que deseemos.

La configuración de los roles y grupos de seguridad, junto a sus permisos y reglas se puede encontrar en las tablas a continuación

Grupo de Seguridad	Regla de Entrada	Servicio o Puerto	Regla de Salida	Servicio o Puerto
Inference Lambda SG	Permitir	API Gateway (443/80)	Permitir	Sagemaker
Document Lambda SG	Permitir	API Gateway (443/80)	Permitir	Bucket: Eventos e Incidentes (443)
Notebook Sagemaker Instance			Permitir	Bucket: Entrenamiento (443)

Tabla 4. Reglas de Entrada y Salida para los Grupos de Seguridad creados

Roles	Permisos necesarios	Activo a asignar
InferenceServiceAccess	Invocar Endpoint de Sagemaker	Función Lambda: Inferencia
SagemakerServiceAccess	Leer y Modificar Bucket: Entrenamiento,	Endpoint: Sagemaker
DocumentServiceAccess	Leer Bucket: Eventos e Incidentes	Función Lambda: Registro

Tabla 5. Roles asignados para los activos de la solución en la nube

Para hacer uso de la API Gateway, será necesario usar el protocolo de firma Signature Version 4 para agregar la información de autenticación de IAM a la solicitud HTTPS y validar la identidad y permisos del usuario.

La solicitud HTTPS debe ser enviada con el método POST para poder adjuntar la información necesaria en el cuerpo de la solicitud y no en la URL.

- El parámetro Host, que deberá contener el hostname asignado a la API.
- El parámetro Content-Type, que deberá indicar que el cuerpo de la solicitud contiene data en formato JSON
- El parámetro X-Amz-Date, que deberá indicar la fecha y hora que se generó la solicitud en la firma de la solicitud usando SigV4
- El parámetro Authorization, que deberá contener las credenciales del usuario con permisos para llamar a la API, firmada usando SigV4.

Al terminar con esta sección, nuestro diagrama se vería de la siguiente manera:

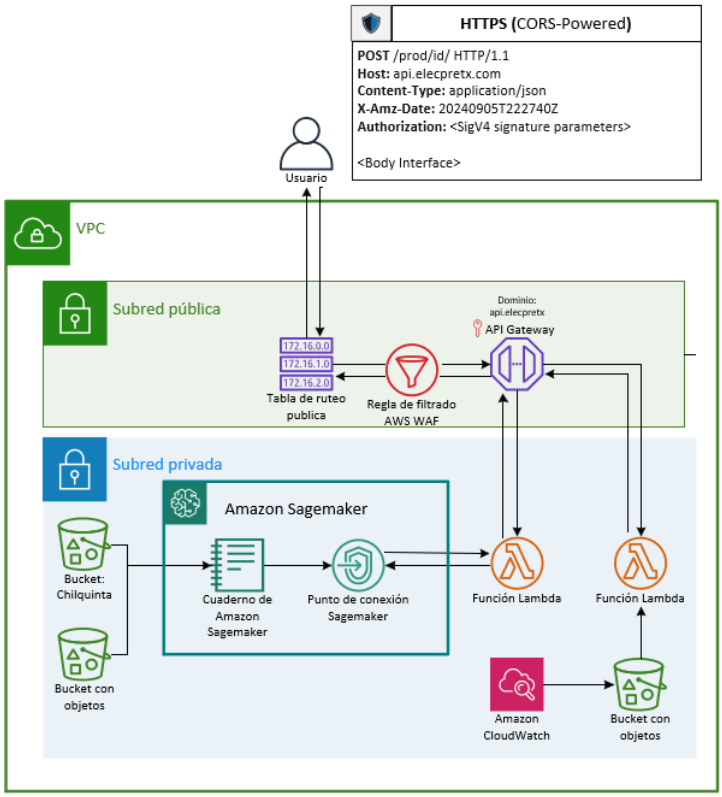

Figura 7. Diagrama de arquitectura hasta la sección 3

4.8.4 Implementación Política: Comunicación y Buenas Practicas

Esta sección establece lineamientos y requerimientos básicos enfocados en lograr una comunicación eficaz entre el proveedor y el usuario sobre tópicos de ciberseguridad. Además, solicita un documento con buenas prácticas y el procedimiento para ocupar correctamente la solución.

Este documento será disponibilizado en el bucket asignado para la información sensible de cada empresa, destacado en la siguiente imagen, entendiendo que puede haber soluciones personalizadas o planes de servicio más reducidos.

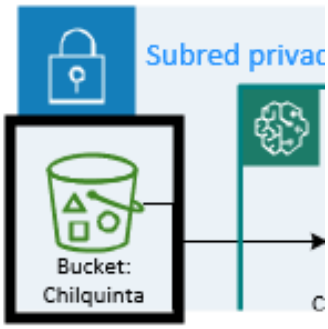

Figura 7**.** Bucket asignado para la información requerida por cada empresa

4.8.5 Implementación Política: Gestión de Cambios

La sección 5 trata sobre la gestión de los cambios y la necesidad de identificar vulnerabilidades causadas por el pobre mantenimiento de herramientas y la falta de un proceso de gestión de los cambios.

Se puede destacar la obligación que se tendrá como proveedor de servicios de documentar todos los cambios tanto propuestos como planificados, además de establecer medidas para lograr mitigar las vulnerabilidades conocidas de nuestra solución

Sobre esto último, se ocupará un servicio que se llama AWS Inspector, el cual analiza todas las instancias de contenedores o maquinas virtuales en busca de vulnerabilidades, lo que nos ayudará a reducir considerablemente las nuevas vulnerabilidades conocidas de algunos activos informáticos

En cuanto sean realizados los cambios planificados, se deberán agregar a un registro histórico sobre los cambios aplicados al servicio o su infraestructura. Para esto se ocupará un bucket universal con objetos que guarda todos los documentos requeridos para lograr conformidad con las normas y regulaciones estudiadas en este trabajo.

Al terminar de implementar esta sección, el diagrama se deberá ver de la siguiente manera

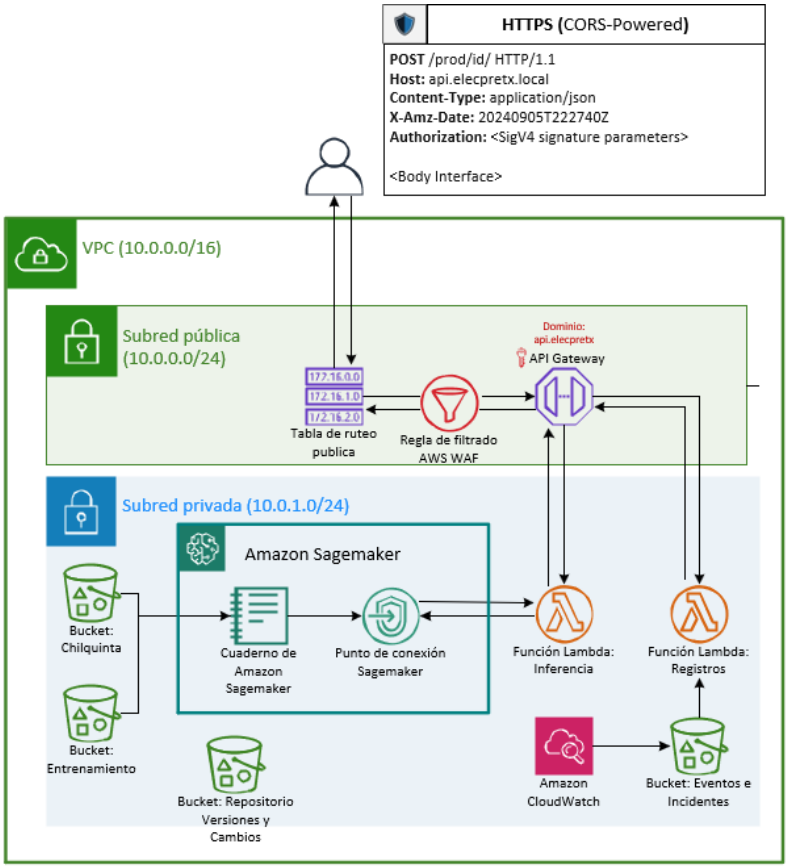

Figura 8. Diagrama de arquitectura hasta la sección 5

4.8.6 Implementación Política: Recuperación

En la ultima sección de nuestras políticas de seguridad se destaca la necesidad de mantener un repositorio centralizado que muestre de manera explicita y ordenada las distintas versiones de la solución y la información, por lo que se usará el mismo bucket usado para el registro histórico de los cambios.

Además, se habló de mantener copias de seguridad sobre los datos dentro de los activos informáticos con el fin de mitigar la perdida de información y corrupción de esta y facilitar la recuperación en casos de desastre, que, según la política a implementar, es de 1 hora para activos con criticidad alta, 4 para criticidad media, y 24 para criticidad baja.

Como mención honorable, el diagrama propone la implementación de AWS Artifact, servicio que ayuda a administrar la conformidad con las normas y estándares disponibles, pudiendo pedir tanto informes de conformidad como también acuerdos a nivel de usuario.

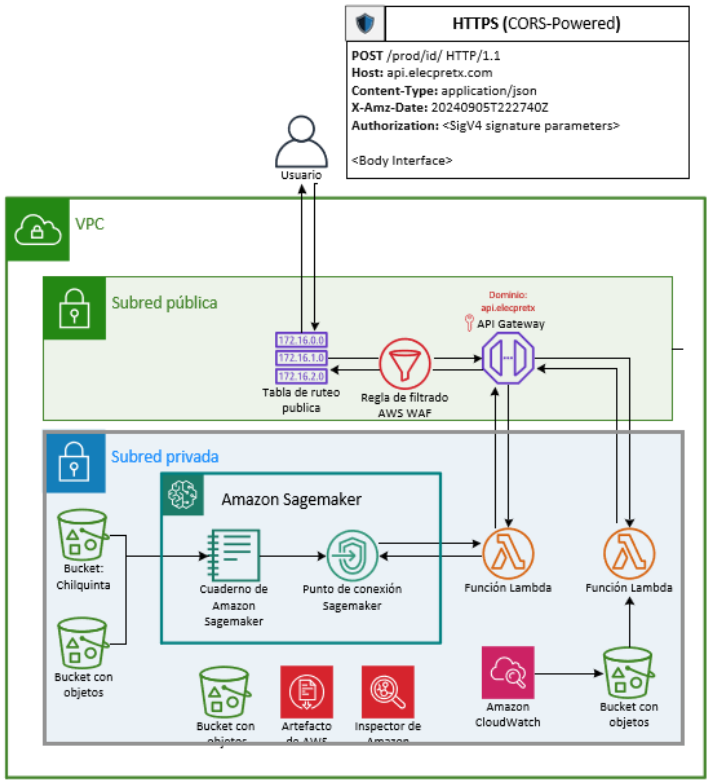

Figura 9. Diagrama de arquitectura resultante de la implementación de políticas

4.8.7 Implementación: Virtual Private Network

Para la finalidad de nuestro modelo de negocio, será necesario que toda nuestra red sea protegida detrás de una Virtual Private Network, o VPN por sus siglas. Esto permitirá restringir a nivel perimetral todo acceso no autorizado a los recursos de la solución, limitando solo el paso del trafico proveniente de clientes enrolados en alguno de los planes ofrecidos. Para esto, es necesario establecer el inventario de nuestra red con el fin de apoyar futuros desarrollos y configuraciones necesarias para la comunicación segura entre nuestras subredes, ya sean públicas o privadas.

Activo	Red	Hostname o Nombre	Contenido
API Gateway	10.0.0.0/24	api.elecpretx.local	API principal
Función Lambda: Inferencia	10.0.1.0/24	getPrediction	Función para obtener inferencia de modelo
Función Lambda: Registro	10.0.1.0/24	getDocument	Función para obtener el documento solicitado
Endpoint: Sagemaker	10.0.1.0/24	elecpretx-sm-1	Endpoint para solicitar inferencias
Notebook: Sagemaker	10.0.1.0/24	model-prod-elecpretx	Notebook para entrenar y desplegar el modelo de inferencia

Tabla 6. Configuración de red para los activos de la solución en la nube.

A pesar de que ya revisamos e implementamos toda la política de seguridad en la arquitectura, aún hay algunos detalles que se pueden mejorar. Por ejemplo, la API Gateway aún tiene acceso directo a internet.

Para solucionar esto, dentro de los patrones de diseño que existen para la implementación de VPN en AWS se encuentra el patrón Site-to-Site VPN. Este es un patrón seguro que permite establecer conexiones desde redes on-premise a las redes de AWS a través del uso de túneles VPN, esto con el fin de asegurar el transito de los datos usando IPSec y permitiendo que los dispositivos conectados a la VPN puedan interactuar de manera segura.

Según lo descrito, la integración de los dos cambios debería dejar nuestro diagrama de la siguiente manera.

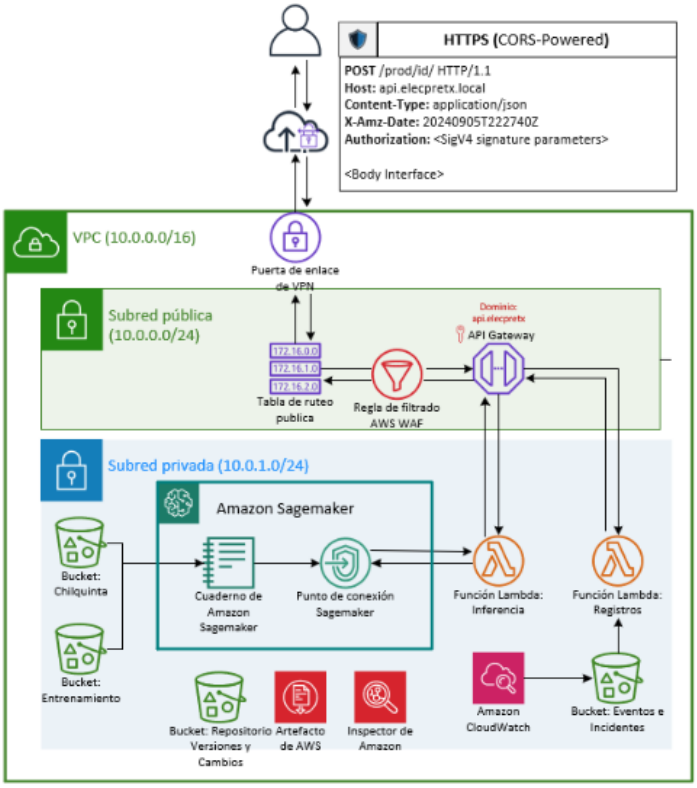

Figura 10. Diagrama final propuesto para la solución desplegada en Amazon Web Services

5. Conclusión

A lo largo de este trabajo, se adquirió un entendimiento más profundo del enfoque nacional en temas de ciberseguridad, particularmente en el contexto de empresas que gestionan infraestructura crítica como las líneas de transmisión eléctrica. Este enfoque subraya la importancia del monitoreo constante, que no solo garantiza el cumplimiento de normativas y estándares, sino que también facilita la mejora continua en la gestión de activos y servicios. El aprendizaje también destacó la relevancia de la comunicación y colaboración efectiva entre las entidades reguladoras y las empresas responsables, como un pilar esencial para construir una ciberseguridad sólida y efectiva en este sector.

Sin embargo, uno de los desafíos más significativos que enfrenta la ciberseguridad es la adopción y la capacitación del personal en estos temas. La formación adecuada es crucial para que las personas comprendan los riesgos, apliquen correctamente las políticas y utilicen de manera eficiente las herramientas tecnológicas disponibles. Además, se necesita un entorno digital que facilite la colaboración entre entidades reguladoras, empresas y otras partes interesadas, promoviendo un ecosistema de seguridad cohesivo y robusto.

En retrospectiva, el trabajo podría haberse beneficiado de un enfoque más técnico en el análisis de normativas específicas sobre ciberseguridad. La falta de conocimiento en ciertos términos y procedimientos específicos del sector eléctrico limitó el nivel de profundidad alcanzado. Asimismo, la arquitectura propuesta podría haberse ampliado para cubrir escenarios más exhaustivos y variados o

amenazas más profundas y complejas, permitiendo una mejora sustancial de las bases de seguridad de la información para la solución.

Para futuras versiones de estas políticas, seria esencial hacer aplicación de marcos de gobernanza como puede ser Control Objectives for Information Technologies (COBIT) para un mejor entendimiento entre los objetivos del negocio con los de la seguridad de la información. también, entendiendo el contexto nacional sobre las nuevas leyes en la materia, se hace mención especial a la Ley 21.719 de Protección de Datos Personales, que entrará en vigor en diciembre de 2026 en busca de un mejor monitoreo y sanción respecto al uso indebido de los datos personales.

En resumen, este trabajo representa un paso inicial hacia la creación de un marco sólido para gestionar modelos predictivos en infraestructura crítica, destacando áreas clave de aprendizaje y áreas de mejora. Los resultados obtenidos sientan las bases para futuros esfuerzos en la integración de ciberseguridad y tecnologías avanzadas en sectores esenciales para la sociedad.

6. Bibliografía

[1] Kaspersky. ¿Qué es la ciberseguridad? Recuperado de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[2] IBM. Seguridad de la Información Recuperado de https://www.ibm.com/mx-es/topics/information-security

[3] Biblioteca del Congreso Nacional de Chile. Ley 215432. Recuperado de https://www.bcn.cl/leychile/navegar?idNorma=1188583

[4] Ikusi. Aumento de ciberataques con la pandemia: ¿cuál es la situación actual? Recuperado de https://www.ikusi.com/mx/blog/aumento-de-ciberataques-con-la-pandemia-cual-es-la-situacion-actual

[5] ISO. Norma UNE-ISO/IEC 27001:2023. Recuperado de https://www.iso.org

[6] En Cancha. Chile está en los primeros puestos: Estos son los 5 países de América Latina con mejor ciberseguridad. Recuperado de https://www.encancha.cl/enlahora/mundo/2024/09/21/chile-esta-en-los-primeros-puestos-estos-son-los-5-paises-de-america-latina-con-mejor-ciberseguridad/

[7] Telefónica. Chile, país vanguardista en materia de ciberseguridad en Latinoamérica. Recuperado de https://www.telefonica.com/es/sala-comunicacion/blog/chile-pais-vanguardista-materia-ciberseguridad-latinoamerica/

[8] Journal of Medical Internet Research. Cybersecurity Risks in a Pandemic. *JMIR Publications*, Vol. 22, No. 9, 2020. Recuperado de https://www.jmir.org/2020/9/e23692

[9] ISO. ISO Survey 2023. Recuperado de https://www.iso.org/the-iso-survey.html

[10] Coordinador Eléctrico Nacional. Coordinador presentó el Estándar de Ciberseguridad para el Sector Eléctrico de Chile. Recuperado de https://www.coordinador.cl/novedades/coordinador-presento-estandar-de-ciberseguridad-para-el-sector-electrico-de-chile/

[11] Diario Oficial. Ley Marco de Ciberseguridad. Recuperado de https://www.diariooficial.interior.gob.cl/publicaciones/2024/04/08/43820/01/2475674.pdf

[12] Amazon Web Services (AWS). Opciones de conectividad de red a Amazon VPC. Recuperado de https://docs.aws.amazon.com/es_es/whitepapers/latest/aws-vpc-connectivity-options/network-to-amazon-vpc-connectivity-options.html

[13] Infobae. (2022, 12 de diciembre). Brasil, México y Perú son los países latinos con más ciberataques en 2022. Recuperado de https://www.infobae.com/america/tecno/2022/12/12/brasil-mexico-y-peru-son-los-paises-latinos-con-mas-ciberataques-en-2022/

[14] Global Suite Solutions. (2024, octubre). Key Statistics - Oct 2024. Recuperado de https://www.globalsuitesolutions.com/es/nerc-cip-cumplimiento-normativa/

[15] Entel Digital. Reporte Ciberseguridad 2024. Recuperado de https://enteldigital.cl/hubfs/Entel_Digital_Reporte_Ciberseguridad_2024_4ta_edicion.pdf

[16] Cámara de Comercio de Santiago. Nueva Ley de Protección de Datos exige preparación empresarial inmediata. Recuperado de https://www.ccs.cl/2025/06/04/nueva-ley-de-proteccion-de-datos-exige-preparacion-empresarial-inmediata/