



PROPUESTA METODOLOGÍA PARA EL DESARROLLO E INSTALACIÓN DE SISTEMAS DE CARGA EN CHILE

FRANCO PALMA TREJO

**Tesis para optar al Título de Ingeniero Civil en Informática y
Telecomunicaciones y al Grado de Magíster en Ciencias de la
Ingeniería con mención en Informática y Telecomunicaciones.**

Profesor guía: Luciano Ahumada Fierro

**FACULTAD DE INGENIERÍA Y CIENCIAS
ESCUELA DE INFORMÁTICA Y TELECOMUNICACIONES**

**Santiago, Chile
2024**

PROPUESTA METODOLOGÍA PARA EL DESARROLLO E INSTALACIÓN DE SISTEMAS DE CARGA EN CHILE

FRANCO PALMA TREJO

**Tesis para optar al Título de Ingeniero Civil en Informática y
Telecomunicaciones y al Grado de Magíster en Ciencias de la
Ingeniería con mención en Informática y Telecomunicaciones.**

**Profesor guía: Luciano Ahumada Fierro
Profesor comisión: Nicolás Boettcher Palma
Profesor examinador: Jonathan Frez Zachary**

**FACULTAD DE INGENIERÍA Y CIENCIAS
ESCUELA DE INFORMÁTICA Y TELECOMUNICACIONES**

**Santiago, Chile
2024**

✉ Franco Palma Trejo
✉ franco.palma@mail.udp.cl

Espero que el contenido de esta tesis pueda ser un valioso recurso y contribución para futuras investigaciones sobre la electromovilidad. Que los hallazgos y conclusiones aquí presentados puedan servir de base y guía para aquellos que continúen explorando este tema en el futuro.

Agradecimientos

Quiero expresar mi profunda gratitud a mis padres, Jaime y Patricia, por su inquebrantable apoyo y sacrificio, que hicieron posible que pudiera dedicarme a mis estudios y completar esta tesis. Su amor, aliento y confianza incondicional fueron la fuerza impulsora detrás de cada paso que di en este viaje académico.

Agradezco a mi familia por su constante respaldo y por creer en mí desde el principio. Sus palabras ánimo han sido un faro en los momentos difíciles.

A mis hermanas, Camila y Fernanda, les agradezco profundamente por su apoyo incondicional a lo largo de este proceso. Su amor, comprensión y ánimo han sido un pilar fundamental en mi camino hacia la culminación de esta tesis.

A mis amigos de la universidad, su compañerismo, apoyo mutuo y risas compartidas han enriquecido mi experiencia universitaria y han sido un recordatorio constante de la importancia de la amistad en este viaje.

Agradezco a cada profesor que he tenido durante estos años de estudio. Sus enseñanzas, orientación y estímulo han moldeado mi pensamiento crítico y han sido la base de mi crecimiento académico y personal.

Un agradecimiento especial a mi profesor tutor, Luciano Ahumada, cuya orientación experta y apoyo fueron fundamentales para superar los desafíos y completar esta tesis. A pesar de las circunstancias adversas, su compromiso y dedicación fueron una fuente constante de inspiración.

Por último, pero no menos importante, agradezco a la universidad por brindarme el entorno académico propicio y la flexibilidad necesaria para llevar a cabo este proyecto de investigación. Su compromiso con la excelencia académica ha sido un motor constante en mi camino hacia la consecución de mis metas.

A todos los que me ayudaron y apoyaron durante este proceso, mi más sincero agradecimiento. Este logro no habría sido posible sin su apoyo, aliento y presencia constante a lo largo de este viaje.

¡Gracias!

Resumen

La presente tesis titulada “Propuesta Metodológica para el Desarrollo e Instalación de Sistemas de Carga en Chile”, ofrece una visión integral sobre la electromovilidad y su implementación en Chile, focalizándose en los vehículos eléctricos, sus sistemas de carga, y los modelos de arquitectura de sistemas de electromovilidad que facilitan la interoperabilidad en el sistema. Se subraya la importancia de una metodología adecuada para el desarrollo e instalación de sistemas de carga, considerando especialmente la seguridad de la información y la protección contra el robo de identidad durante los procesos de recarga.

El trabajo inicia abordando el contexto y motivación detrás de la electromovilidad, resaltando la necesidad de avanzar hacia opciones de transporte más sostenibles como respuesta al cambio climático. La adopción de vehículos eléctricos surge entonces como una solución potencial para reducir las emisiones de gases de efecto invernadero, aprovechando la eficiencia energética y las energías renovables. Sin embargo, el documento identifica desafíos como el alto costo inicial de los vehículos eléctricos y la necesidad de desarrollar una infraestructura de carga adecuada que garantice la seguridad y la interoperabilidad.

La metodología propuesta se enfoca en la investigación para explorar los distintos modelos de arquitectura y vulnerabilidades asociadas a la electromovilidad. A través de un análisis detallado, se propone una capa de seguridad diseñada para ser aplicable en los diversos modelos de interoperabilidad, con el objetivo de proteger la información confidencial del usuario y prevenir el robo de identidad.

El trabajo examina distintos modelos de arquitectura de sistemas de electromovilidad, incluyendo el *E-Mobility Architecture Model* (EMAM), el *Smart City Infrastructure Architecture Model* (SCIAM), el *E-Mobility Information System Architecture* (EM-ISA), entre otros. Cada modelo se analiza en términos de sus características, capacidades y limitaciones, con especial atención a los aspectos de seguridad y comunicación.

En cuanto a la seguridad, el documento destaca la importancia de abordar vulnerabilidades específicas asociadas a los sistemas de carga de vehículos eléctricos. Se propone una capa de seguridad detallada que cubre perspectivas como la actualización y segmentación, la información, la infraestructura,

y la autenticación. Esta capa se contextualiza dentro de modelos de interoperabilidad, dando luces sobre su efectividad para mejorar la seguridad del sistema.

Las conclusiones del trabajo enfatizan la viabilidad de implementar vehículos eléctricos en Chile, resaltando la necesidad de una infraestructura de carga segura y interoperable. El documento llama a la acción para la adopción de medidas regulatorias y el desarrollo de tecnologías que faciliten la transición hacia la electromovilidad, considerando tanto los beneficios ambientales como los desafíos técnicos y de seguridad.

Así, se presenta una contribución significativa al campo de la electromovilidad en Chile, ofreciendo un marco metodológico para el desarrollo e instalación de sistemas de carga seguros e interoperables. A través de un enfoque multidisciplinario, aborda los aspectos técnicos, regulatorios y de seguridad necesarios para avanzar hacia un transporte más sostenible y eficiente energéticamente.

Abstract

This thesis, entitled “Methodological Proposal for the Development and Installation of Charging Systems in Chile,” offers a comprehensive view of electromobility and its implementation in our country, focusing on electric vehicles, their charging infrastructure, and the electromobility architectural models that facilitate interoperability. The importance of an appropriate methodology for developing and installing charging systems is emphasized, especially considering the security of information and protection against identity theft during the charging processes.

The work begins by addressing the context and motivation behind electromobility, highlighting the need to move towards more sustainable transportation options in response to climate change. Thus, adopting electric vehicles emerges as a potential solution to reduce greenhouse gas emissions, leveraging energy efficiency and renewable energies. However, the document identifies challenges such as the high initial cost of electric vehicles and the need to develop a suitable charging infrastructure that ensures safety and interoperability.

The proposed methodology focuses on research to explore the different architecture models and vulnerabilities associated with electromobility. A detailed analysis proposes a security layer designed to be applicable across various interoperability models to protect the user’s confidential information and prevent identity theft.

The work examines different electromobility system architecture models, including the *E-Mobility Architecture Model* (EMAM), the *E-Mobility Information System Architecture* (EM-ISA), and the *Smart City Infrastructure Architecture Model* (SCIAM), among others. Each model is analyzed regarding its features, capabilities, and limitations, with special attention to security and communication aspects.

Regarding security, the document highlights the importance of addressing specific vulnerabilities associated with electric vehicle charging systems. A detailed security layer is proposed, covering perspectives such as update and segmentation, information, infrastructure, and authentication. This layer is contextualized within interoperability models, shedding light on its effectiveness in enhancing system security.

The conclusions of the work emphasize the feasibility of implementing

electric vehicles in Chile, highlighting the need for a secure and interoperable charging infrastructure. The document calls for action in adopting regulatory measures and developing technologies that facilitate the transition to electromobility, considering both environmental benefits and technical and security challenges.

Thus, a significant contribution is presented to the field of electromobility in Chile, offering a methodological framework for developing and installing secure and interoperable charging systems. A multidisciplinary approach addresses the technical, regulatory, and security aspects necessary to move towards more sustainable and energy-efficient transportation. .

Contenido

Resumen	i
Abstract	iii
Lista de tablas	vii
Lista de figuras	ix
Capítulo 1. Introducción	1
1.1. Motivación	2
1.2. Objetivos	3
1.2.1. Objetivo General	3
1.2.2. Objetivos Específicos	3
Capítulo 2. Metodología	5
2.1. Herramientas de investigación	6
2.1.1. Instrumento de recolección de datos cuantitativos . . .	6
Capítulo 3. Electromovilidad	7
3.1. Sistema de Recarga	8
3.2. Impulso hacia la Electromovilidad	10
3.2.1. Contexto nacional	11
3.3. Conclusiones	14
Capítulo 4. Interoperabilidad	15
4.1. Modelos de arquitectura de sistemas de electromovilidad . . .	16
4.1.1. E-Mobility Architecture Model (EMAM)	19
4.1.2. E-Mobility -Information System Architecture (EM-ISA)	20
4.1.3. Smart City Infrastructure Architecture Model (SCIAM)	21
4.1.4. Interoperability Reference Architecture for E-Mobility	22
4.1.5. E-Mobility Systems Architecture (EMSA)	23
4.1.6. A Blockchain Based Electric Vehicle Smart Charging System with Flexibility	25

4.1.7. Applying Enterprise Architecture for Digital Transformation of Electro Mobility towards Sustainable Transportation	28
4.2. Referencias hacia el modelo EMSA	30
4.2.1. Crítica: Vulnerabilidades de comunicación en un sistema	30
4.2.2. Referencia a la arquitectura para sistemas de reserva interoperables	32
4.3. Conclusiones	33
Capítulo 5. Seguridad	37
5.1. Ciberseguridad en el sistema de carga de vehículos eléctricos .	38
Capítulo 6. Capa de seguridad	45
6.1. Descripción de la capa	45
6.1.1. Perspectiva de actualización y segmentación	47
6.1.2. Perspectiva de información	49
6.1.3. Perspectiva de infraestructura	51
6.1.4. Perspectiva de autenticación	52
6.2. Intersecciones que cubrirá la capa en el modelo EMSA	55
6.2.1. Perspectiva de actualización y segmentación	57
6.2.2. Perspectiva de información	57
6.2.3. Perspectiva de infraestructura	59
6.2.4. Perspectiva de autenticación	61
6.3. Testeo de la capa de seguridad	63
6.3.1. Perspectiva de actualización y segmentación	63
6.3.2. Perspectiva de información	64
6.3.3. Perspectiva de infraestructura	64
6.3.4. Perspectiva de autenticación	64
6.4. Resultados obtenidos	65
6.5. Resultados obtenidos al aplicar las distintas perspectivas . . .	65
6.6. Conclusiones	91
Capítulo 7. Conclusiones	93
Referencias bibliográficas	95

Lista de tablas

Lista de figuras

Capítulo 1

Introducción

Electromovilidad se refiere al uso de sistemas de propulsión que operan con energía eléctrica en diversos modos de transporte. Específicamente, implica vehículos que emplean electricidad o fuentes de energía alternativas para funcionar a través de uno o más motores eléctricos. Históricamente, como se destaca en [1], la concepción y desarrollo de vehículos eléctricos (VE) data del siglo XIX, época de los primeros vehículos propulsados por combustión interna, electricidad, y vapor. A pesar de que inicialmente los vehículos eléctricos compartían el escenario con sus homólogos de combustión interna, el mercado automovilístico eventualmente se inclinó hacia estos últimos debido a dos factores principales: la producción en masa del Ford Model T, que redujo significativamente sus costos, y el éxito en el establecimiento de una amplia infraestructura de repostaje por parte de la industria petrolera, favoreciendo la conveniencia de los vehículos con motor de combustión interna (ICE, por sus siglas en inglés).

En la actualidad, impulsados por la urgente necesidad de responder al cambio climático, se promueve la adopción de vehículos eléctricos para disminuir las emisiones de gases de efecto invernadero (GEI) asociadas al transporte, una medida respaldada por el Acuerdo de París [2]. Cabe destacar que el transporte contribuye significativamente a las emisiones globales de GEI, representando aproximadamente entre el 28 % y el 30 %.

La electromovilidad no solo abarca los vehículos eléctricos sino también todo el ecosistema asociado, incluyendo los avances tecnológicos en baterías e

infraestructuras de carga, enmarcados en la lucha contra el cambio climático, la eficiencia energética, y el fomento de las energías renovables, entre otros aspectos.

Los vehículos eléctricos, incluyendo modelos híbridos enchufables y de batería completa, ofrecen una alternativa atractiva para cumplir con objetivos ambientales, sociales y de salud, destacándose por su eficiencia energética, siendo de dos a cuatro veces más eficientes que los motores de combustión interna tradicionales.

No obstante, la transición de vehículos de combustión interna a eléctricos enfrenta barreras, como el elevado costo inicial, principalmente atribuido al precio de las baterías de ion-litio. Se anticipa que este obstáculo se atenuará en el futuro cercano, con una reducción esperada en los costos de las baterías y, por ende, de los vehículos eléctricos hacia el período 2022-2025.

Para facilitar la transición hacia un transporte público eléctrico, es esencial contar con una infraestructura de carga adecuada. Esta infraestructura debe resolver desafíos técnicos, regulatorios y de modelos de negocio, aspectos que serán explorados en esta investigación con el objetivo de contribuir a la regulación de la seguridad en la electromovilidad.

1.1. Motivación

En la última década, un considerable número de chilenos ha optado por la compra de automóviles, elevando la tasa de motorización a 3,62 personas por vehículo. Actualmente, Chile cuenta con más de 5,22 millones de vehículos [3]. A medida que el parque automotor, dominado por vehículos con motores de combustión interna, continúa su expansión, se prevé un incremento correspondiente en la emisión de gases de efecto invernadero (GEI).

El principal motor detrás de este estudio es contribuir al esfuerzo nacional de Chile por fomentar un sistema de transporte más respetuoso con el medio ambiente. Esto se lograría mediante la promoción de vehículos que funcionan con motores eléctricos y tecnología plug-in (híbridos enchufables). Además, se busca proteger la información privada de los individuos y reforzar la seguridad del sistema de recarga para vehículos eléctricos (VE) en Chile, mediante la identificación de vulnerabilidades y la propuesta de soluciones para su corrección.

1.2. Objetivos

1.2.1. Objetivo General

Elaborar un estado del arte sobre la electromovilidad y modelos de interoperabilidad en el sistema de recarga de vehículos eléctricos aplicables en Chile, con la finalidad de resguardar la seguridad del modelo a utilizar en el sistema. Este objetivo se enmarca en el contexto de fomentar un sistema de transporte más sostenible y seguro en Chile, mediante la promoción del uso de vehículos eléctricos y el desarrollo e instalación de una infraestructura de carga segura y eficiente.

1.2.2. Objetivos Específicos

- Identificar tendencias y características de la electromovilidad, comprendiendo el estado actual y las perspectivas futuras de esta tecnología en el ámbito del transporte.
- Clasificar los modelos de interoperabilidad aplicables en la electromovilidad existentes, analizando las distintas arquitecturas de sistemas de recarga para vehículos eléctricos y su compatibilidad con el contexto chileno.
- Describir las vulnerabilidades de los modelos de interoperabilidad aplicables en la electromovilidad, identificando los riesgos y amenazas para la seguridad de la información y la integridad del sistema de recarga.
- Establecer una capa de seguridad utilizable en los distintos modelos de interoperabilidad aplicables en la electromovilidad, diseñando una solución que proteja contra el acceso no autorizado, el robo de identidad, y otros ciberataques.
- Evaluar la capa de seguridad establecida en distintos modelos de interoperabilidad aplicables en la electromovilidad, probando su efectividad en la protección de la información y la infraestructura de recarga frente a potenciales vulnerabilidades.

Capítulo 2

Metodología

Para llevar a cabo esta investigación, se ha seleccionado un enfoque cuantitativo mediante el Diseño Transaccional Exploratorio. La razón de esta elección radica en que dicho modelo facilita el análisis de una o varias variables dentro de un contexto o situación específica, proporcionando un panorama inicial en un momento determinado. Este enfoque es particularmente adecuado para abordar problemas de investigación emergentes o poco estudiados que cuentan con referencias a investigaciones previas [4].

Se examinarán diversas propuestas que contribuirán a esclarecer y entender el fenómeno asociado a las deficiencias en la seguridad de los modelos de interoperabilidad enfocados en la electromovilidad.

Para la recopilación de datos cuantitativos, se realizará una investigación documental (*desk research*), la cual estará enfocada en los modelos de interoperabilidad específicos de la electromovilidad.

El marco metodológico DISTRAC facilitará la interpretación y análisis de los hallazgos obtenidos durante la recopilación de datos. Esto permitirá, en etapas posteriores, desarrollar una herramienta práctica capaz de identificar modelos vulnerables y proponer medidas correctivas.

2.1. Herramientas de investigación

2.1.1. Instrumento de recolección de datos cuantitativos

Desk Research: Este método será empleado en la investigación debido a su enfoque en analizar material ya publicado, como informes, documentos, bibliotecas públicas, artículos, entre otros.

La fase inicial de la investigación se centra en compilar un panorama actualizado sobre la electromovilidad, modelos de interoperabilidad (con especial énfasis en aquellos aplicados a la electromovilidad) y las diversas vulnerabilidades identificadas por varios autores.

La recopilación de esta información se realizará a través del análisis de tesis, libros, artículos y documentos de asesoría técnica parlamentaria, entre otros. Las fuentes para esta tarea han sido sugeridas por el tutor encargado de la investigación, complementándose con la consulta de bases de datos especializadas como ResearchGate y Google Académico.

Capítulo 3

Electromovilidad

La electromovilidad se define como el empleo de energía eléctrica para alimentar uno o varios motores eléctricos destinados a propulsar vehículos usados como medios de transporte. En este sentido, abarca tanto los vehículos eléctricos puros (battery electric vehicle o BEV) como los vehículos híbridos enchufables (Plug-in Hybrid Electric Vehicle o PHEV) y aquellos basados en celdas de combustible. Sin embargo, este último grupo no se aborda en este documento, ya que no requieren conexión a la red eléctrica para su recarga. Los vehículos considerados incluyen desde bicicletas y motocicletas hasta automóviles, furgonetas ligeras, autobuses y camiones que necesiten recargar sus baterías mediante conexión a una red eléctrica.

Los vehículos eléctricos ofrecen numerosas ventajas ambientales, destacando la reducción en la emisión de CO₂ y otros gases de efecto invernadero, siempre y cuando la energía utilizada provenga de fuentes renovables.

Otras ventajas significativas del uso de vehículos eléctricos (VE) incluyen una mayor eficiencia energética. Esto se debe a que los motores eléctricos, al ser más ligeros y no perder fuerza significativa en altas revoluciones, permiten una gestión más eficiente del consumo energético, especialmente porque pueden recuperar energía durante las desaceleraciones.

Según datos de la IEA [5], actualmente hay más de 10 millones de vehículos eléctricos en el mundo, incluyendo tanto BEV como PHEV. La mayoría de estos vehículos se encuentran en China, Estados Unidos y Noruega, este último país destaca por un significativo incremento en las ventas de VE,

impulsado por políticas gubernamentales proactivas en favor de la electromovilidad.

Las tablas 3.1 y 3.2 ilustran que el aumento en el número de VE está directamente relacionado con el crecimiento en la infraestructura de carga disponible. Esto refleja no solo una mayor demanda de estos vehículos a lo largo del tiempo sino también una reducción en la preocupación de los usuarios por la posibilidad de quedarse sin carga eléctrica.

	2014	2015	2016	2017	2018	2019	2020
China	85,3	292,7	628,7	1207,7	2288,8	3349,1	4508,7
Estados Unidos	290,2	404,1	563,7	762,1	1123,4	1450,0	1778,1
Noruega	35,4	69,2	114,1	176,3	249,0	328,6	484,7
Reino Unido	24,1	48,5	86,4	133,7	184,0	259,0	435,1
Francia	31,5	54,5	84,0	118,8	165,5	226,8	416,2
Alemania	24,9	48,1	72,7	109,6	177,1	238,8	330,8
Japón	111,5	134,6	153,1	202,9	236,3	263,8	293,1
Países Bajos	43,8	87,5	112,2	119,3	142,7	203,4	291,1
Canadá	10,7	17,7	29,3	45,9	90,1	141,1	209,1
Suecia	7,3	15,9	29,3	49,7	78,6	97,0	178,7
Corea	2,7	6,0	11,0	25,7	60,6	96,7	136,6
Finlandia	0,9	1,6	3,3	7,2	15,5	29,4	55,3
Portugal	1,3	2,5	4,3	8,7	17,0	29,7	49,7
Australia	1,9	3,7	5,1	7,3	10,9	20,1	26,7
Nueva Zelanda	0,4	0,9	2,4	5,9	11,4	17,7	23,0
India	3,4	4,4	4,8	7,0	9,1	11,1	12,7
México	0,2	0,3	1,0	2,2	4,0	4,7	7,2
Brasil	0,1	0,1	0,3	0,7	1,1	3,0	4,9
Sudáfrica	0,0	0,3	0,7	0,9	1,0	1,2	1,4
Chile	0,0	0,1	0,1	0,2	0,4	0,6	0,8
Total	703,1	1244,9	1992,4	3137,8	5093,7	7122,8	10197,0

Tabla 3.1. Stock (en miles) de vehículos eléctricos y vehículos híbridos del 2014 al 2020.

Fuente: IEA, 2021

3.1. Sistema de Recarga

Los sistemas de recarga para vehículos eléctricos se componen de varios elementos capaces de intercambiar tanto energía eléctrica como información.

Los vehículos eléctricos se cargan en puntos de recarga o electrolineras. Estas instalaciones están diseñadas específicamente para la carga de vehículos eléctricos y son análogas a las gasolineras tradicionales, pero suministran electricidad en vez de combustibles fósiles. Un punto de carga estándar cuenta con un cargador eléctrico, un cable para conectar el vehículo y una fuente

	2014	2015	2016	2017	2018	2019	2020
China	30.000	58.758	141.254	213.903	275.000	515.908	807.000
Estados Unidos		31.674	38.168	43.037	54.500	77.358	98.981
Noruega	5.293	5.513	7.541	9.209	10.559	14.307	16.976
Reino Unido	7.706	9.240	13.260	15.241	17.424	27.094	33.470
Francia	1.814	10.445	19.618	21.184	24.282	29.701	46.045
Alemania	2.722	5.058	23.901	24.014	26.464	39.291	44.669
Japón	11.511	22.091	24.321	28.762	29.971	30.394	29.855
Países Bajos	4.028	4.030	32.524	33.282	36.829	50.153	65.633
Canadá	2.321	3.424	4.035	5.841	7.940	8.951	13.194
Suecia	2.130	2.502	3.474	3.364	4.139	5.066	10.412
Corea	1.407	1.436	2.014	13.676	27.352	44.792	64.188
Finlandia	383	836	847	847	931	2.124	4.260
Portugal	1.195	1.260	1.295	1.605	1.786	1.961	2.801
Australia				476	727	1.930	2.300
Nueva Zelanda				104	293	389	458
México				1.486	1.486	1.820	2.154
Sudáfrica				124	239	245	305
Chile	18	27	27	41	69	170	352
Total	106.871	184.291	331.757	441.127	550.602	895.553	1.307.894

Tabla 3.2. Infraestructura de carga: cargadores (lentos y rápidos) de acceso público por país del 2014 al 2020.

Fuente: IEA, 2021

de alimentación eléctrica. Estas estaciones de carga se pueden instalar en residencias, aparcamientos públicos y estaciones de servicio, entre otros lugares.

En Chile, el Pliego Técnico Normativo RIC: N°15 especifica los diferentes tipos de instalaciones de carga permitidas en el territorio. Como se ilustra en la Tabla 3.3 y en la Figura 3.1, se distinguen varios modos de carga, cada uno con sus características particulares. Entender estos modos es crucial, ya que el tipo de carga disponible en una instalación determina la potencia a la que el usuario puede cargar su vehículo eléctrico.

Posibilidades de la IRVE	Clasificación Instalaciones				
	Instalaciones Individuales	Edificios Privados	Autoservicio Acceso Público	Electrolineras	Electroterminales o Centros de carga para servicio público
➤ <u>Modo de Carga permitidos</u> 2 3 4	Todos	Todos	3 o 4	3 y 4 (ambos)	Todos
➤ <u>Conectores permitidos</u> AC Tipo 1 AC Tipo 2 DC CCS 1 DC CCS 2 CHAdeMO GB/T DC	Todos	Todos	AC o DC (BNUP) Al menos 22kW	AC V DC (Al menos 22kW)	Todos *Sistema RED
➤ <u>Protocolo Comunicación e Identificación Usuario</u>	No Obligatorio	N. O.	Min. 1.6 RFID o QR	Min. 1.6 RFID o QR	No Obligatorio
➤ <u>Gestión de Carga</u>	SAVE >100kW	Todos	SAVE >100kW	SAVE >100kW	SAVE >100kW
➤ <u>Otros</u>	Doble empalme	Diseño Ed.	Señalética	Señalética	Aprovecha holguras red

Figura 3.1. Definiciones para distintos tipos de instalación.

Fuente: SEC, 2021

Modos de carga	Descripción
Modo 1	Recarga mediante la conexión de un vehículo eléctrico a la red de alimentación de corriente alterna (CA) de la instalación mediante una toma de corriente común, con una intensidad inferior o igual a 10A y tensión en el lado de la alimentación no superior a 220V. Este modo de recarga no se permitirá en Chile.
Modo 2	Corresponde a la conexión de un vehículo eléctrico a un punto de alimentación de la red eléctrica de CA a través de un cable de carga IC-CPD conectado a un punto de carga simple. Este modo de carga no está permitido en instalaciones de autoservicio con acceso a público, ni electrolinerías.
Modo 3	Conexión directa de un vehículo eléctrico a la red de alimentación de corriente alterna utilizando un Sistema de Alimentación de Vehículos Eléctricos (SAVE), que provee de energía eléctrica en CA al convertidor Corriente Alterna(CA)/Corriente Continua (CC) a bordo del vehículo eléctrico y además realiza las funciones de control piloto y proximidad.
Modo 4	Conexión indirecta de un vehículo eléctrico a la red de alimentación de corriente alterna utilizando un SAVE que incorpora un convertidor CA/CC externo, que provee de energía eléctrica en CC a la batería del vehículo eléctrico y además realiza las funciones de control piloto, proximidad y comunicaciones

Tabla 3.3. Modos de carga para vehículos eléctricos.**Fuente:** Pliego Técnico Normativo RIC: N°15

3.2. Impulso hacia la Electromovilidad

Entre las iniciativas globales más destacadas se encuentra el compromiso de diversos países por alcanzar metas ambientales específicas, tales como promover la venta exclusiva de vehículos eléctricos, impulsar el uso de energía eléctrica en el transporte público y reducir la dependencia de vehículos con motores de combustión interna, estableciendo plazos claros para estos objetivos.

De acuerdo con la Agencia Internacional de Energía (IEA por sus siglas en inglés) [5], aunque las ventas globales de automóviles disminuyeron un 16 % en el año 2020 debido a la desaceleración económica provocada por

la pandemia, las matriculaciones de vehículos eléctricos experimentaron un aumento del 41 % en el mismo período. La IEA atribuye este crecimiento a tres factores principales:

- **Políticas de fomento regulatorio:** numerosos países adoptaron nuevas políticas públicas para promover el uso de vehículos eléctricos, incluyendo la modificación de los estándares de emisión de CO₂. Hacia finales de 2020, más de 20 naciones, incluyendo Noruega, Dinamarca, Islandia e Irlanda, anunciaron prohibiciones a la venta de vehículos de combustión interna o establecieron que todos los nuevos vehículos debían ser de emisión cero.
- **Incentivos económicos:** en China y varios países europeos se otorgaron incentivos financieros para incrementar las ventas de vehículos eléctricos.
- **Avances en modelos y tecnología:** el mercado ha visto un aumento en la variedad de modelos de vehículos eléctricos disponibles, al mismo tiempo que el coste de las baterías de ion-litio, esenciales para estos vehículos, ha disminuido de manera constante.

Además, la IEA ha compilado los compromisos asumidos por distintos países para lograr un sistema de transporte, ya sea público o privado, con cero emisiones de gases de efecto invernadero, destacando las metas y plazos definidos por cada nación, como se muestra en la Figura 3.2.

3.2.1. Contexto nacional

Aunque Chile no lidera en cantidad de vehículos eléctricos en el transporte privado, según se observa en la Tabla 3.1, ha destacado en América Latina por su avance hacia la electromovilidad en el contexto de la transición energética y la búsqueda de soluciones sostenibles para el transporte.

Este liderazgo se ha consolidado gracias a diversas iniciativas y compromisos, como el “Compromiso público privado por la electromovilidad” [6], que se actualiza anualmente desde 2017 (excepto en 2019) incorporando nuevos actores y compromisos.

Estos compromisos representan el esfuerzo conjunto de entidades públicas y privadas para avanzar hacia un transporte más sostenible, involucrando a

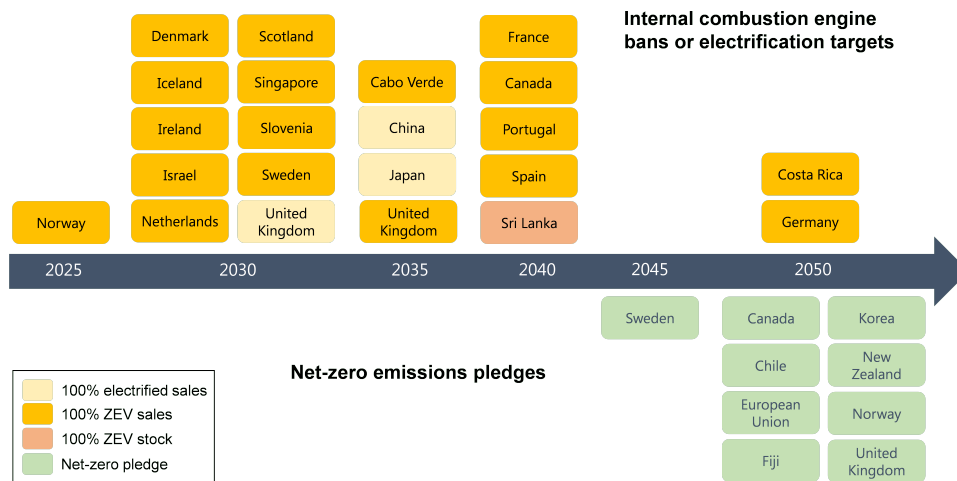


Figura 3.2. Prohibiciones de venta de ICE u objetivos de electrificación.

Fuente: IEA, 2021

ministerios clave y al sector privado. El último de estos compromisos se formalizó el 18 de enero de 2022 con la participación de 142 actores, quienes reafirmaron su apoyo a la electromovilidad.

A través de estos esfuerzos, Chile busca promover el desarrollo de proyectos que, a corto plazo, potencien los beneficios de la electromovilidad y propicien cambios significativos en el transporte nacional.

Además, la “Ruta Energética” [7] y la “Estrategia Nacional de Electromovilidad” [8] son documentos fundamentales para el impulso de esta tecnología en el país. La primera aborda los retos energéticos de Chile, destacando el rol de la electromovilidad para reducir el consumo energético y las emisiones de gases de efecto invernadero. La Estrategia Nacional define etapas y plazos para el avance de la electromovilidad, incluyendo el reglamento de interoperabilidad en la carga de vehículos eléctricos.

El interés internacional por Chile se manifiesta en proyectos como el anunciado por el Presidente Gabriel Boric, con una inversión de más de 200 millones de dólares por parte de la empresa China Yongqing Technology Co. Ltd para 2025 en la Región de Antofagasta, enfocado no solo en la extracción de litio sino también en la creación de valor agregado y transferencia de conocimiento, incluyendo la formación de profesionales chilenos en China.

La “Estrategia Nacional de Electromovilidad” [8] destaca los beneficios de esta transición y propone un plan de trabajo articulado en torno a cuatro ejes principales para los próximos 4-5 años.

La expansión de la electromovilidad en Chile se ve impulsada por el consenso entre el sector público y privado, con el objetivo de que para 2035 todos los vehículos nuevos sean eléctricos. Este ambicioso plan incluye el desarrollo de infraestructura necesaria, como la ampliación de puntos de carga y la revisión de regulaciones e incentivos fiscales. Un hito importante fue la incorporación de 10 buses eléctricos de dos pisos al sistema de transporte público de Santiago, situando a la ciudad como líder fuera de China en la adopción de buses eléctricos.

El reglamento de interoperabilidad [9] tiene como objetivo regular la interoperabilidad de los sistemas de carga, estableciendo los estándares para la información relevante y promoviendo la compatibilidad entre redes de carga mediante conexiones estandarizadas y protocolos de comunicación normados.

La Ley N°21.305 “Sobre Eficiencia Energética” busca promover el uso eficiente de la energía, incluyendo la regulación de la interoperabilidad en los sistemas de recarga de vehículos eléctricos. Tras la consulta pública, se realizaron ajustes al borrador de reglamento basados en los comentarios recibidos, flexibilizando algunos requisitos e introduciendo cambios significativos en las definiciones y en las condiciones para cargadores públicos y privados.

Estos cambios han generado preocupación respecto a la seguridad y privacidad de los datos, ya que la sustitución de la certificación ISO/IEC 27001:2005 por la Ley 19.628 podría no garantizar la protección adecuada de los datos personales frente a riesgos cibernéticos. Esto contrasta con iniciativas como el esquema “Cyber Essential” en el Reino Unido, que busca proteger la información en infraestructuras de TI, demostrando la importancia de adoptar estándares rigurosos de seguridad de la información.

3.3. Conclusiones

Ante la crisis climática que enfrenta nuestro planeta, se hace imperativo adoptar tecnologías más sostenibles que disminuyan la contaminación generada por los sistemas actuales.

Como indican las fuentes [2, 5], una estrategia efectiva para reducir la contaminación, especialmente las emisiones de gases de efecto invernadero, es la promoción de vehículos eléctricos. Esta medida está siendo adoptada gracias a las iniciativas y compromisos de diversos países.

Según [10], para fomentar la adopción generalizada de transporte eléctrico es esencial contar con una infraestructura de carga adecuada y abordar cuestiones técnicas, regulatorias y de modelos de negocio, para así asegurar la fiabilidad del sistema de vehículos eléctricos. Por tanto, la electromovilidad no solo comprende a los vehículos eléctricos sino también la infraestructura de carga necesaria, los avances tecnológicos y el intercambio de información entre los componentes del sistema.

Regular la interoperabilidad en los sistemas de carga para vehículos eléctricos representa un avance significativo. No obstante, según se detalla en [9], aún quedan aspectos por mejorar, especialmente en lo que respecta a la seguridad de la red. La protección ofrecida por la Ley 19.628 es insuficiente; se deberían incluir pruebas de interoperabilidad más exhaustivas. Además, el borrador no especifica a quién deben reportarse los incidentes de seguridad que ocurran en la red, un aspecto crucial para facilitar correcciones futuras.

Capítulo 4

Interoperabilidad

Ante la crisis climática actual, es crucial adoptar tecnologías más sostenibles que minimicen la contaminación producida por los métodos convencionales.

Los vehículos eléctricos (VE), al recargar sus baterías, tienen la capacidad de intercambiar información con la Infraestructura de Recarga de Vehículos Eléctricos (IRVE), como destaca [11]. Esta información puede compartirse con el operador de la estación de carga, el operador del sistema de distribución eléctrica y terceros interesados en datos sobre medición, facturación y preferencias de recarga del vehículo.

Para facilitar este intercambio de información, es necesaria una coordinación y entendimiento claros entre los distintos actores involucrados, asegurando la **interoperabilidad** en el sistema de recarga.

La interoperabilidad ha sido definida de varias maneras, como señala [12]. La IEEE la describe como "la capacidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada" [13], enfatizando la cooperación efectiva entre componentes o subsistemas. De manera similar, el Joint Research Centre [14] la define como la capacidad de dispositivos de un mismo proveedor o de distintos proveedores para intercambiar y utilizar información para una cooperación adecuada. Además, se menciona que si los sistemas pueden comunicarse e intercambiar datos,

muestran interoperabilidad sintáctica, siendo los formatos de datos y los protocolos de comunicación herramientas clave para esta [15].

El reglamento de interoperabilidad [9] amplía esta definición, considerándola como la capacidad de diferentes componentes y sistemas asociados a la infraestructura de carga para intercambiar información, permitiendo que los distintos agentes la integren y utilicen cooperativamente.

4.1. Modelos de arquitectura de sistemas de electromovilidad

La transición del petróleo a la electricidad como fuente de energía en el transporte requiere considerar las limitaciones de esta última, como la producción insuficiente de energía en momentos pico. Esto introduce nuevas necesidades en la red eléctrica, como la optimización del consumo de energía y los procesos de recarga de los VE.

Para abordar estas necesidades, se han propuesto modelos de arquitectura para la gestión de información y uso óptimo de la red eléctrica, siendo el "Smart Grid Architecture Model"(SGAM) [15] uno de los más referenciados.

El SGAM es un modelo tridimensional de interoperabilidad que utiliza capas, dominios y zonas para diseñar, gestionar, visualizar y validar arquitecturas de redes inteligentes de manera estructurada, como se muestra en la Figura 4.1. Este modelo facilita una presentación clara y manejo simplificado de datos, actores, funciones y responsabilidades a través de cinco capas:

- **Capa de Negocio:** Define la visión empresarial del intercambio de información en la red inteligente, mapeando estructuras, políticas, modelos comerciales y actores involucrados.
- **Capa de Función:** Describe arquitectónicamente casos de uso, funciones y servicios del sistema y sus interrelaciones, desde una perspectiva independiente de implementación.
- **Capa de Información:** Detalla la información a utilizarse e intercambiarse entre funciones, servicios y componentes.

- **Capa de Comunicación:** Se enfoca en los protocolos y mecanismos para el intercambio de información.
- **Capa de Componente:** Describe la distribución física de todos los componentes de la red inteligente, incluyendo aplicaciones, equipos, dispositivos de control y otros.

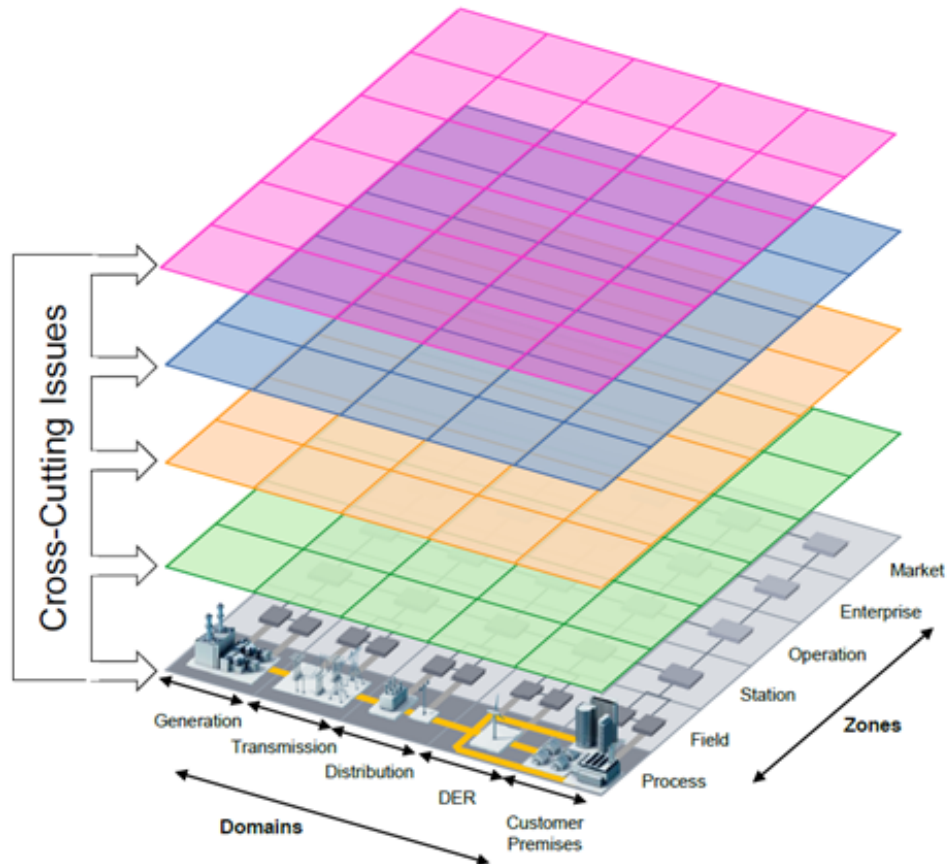


Figura 4.1. Marco SGAM.

Fuente: [15].

Además, como se mencionó previamente, el modelo SGAM integra tanto dominios como zonas en sus cinco capas, lo que facilita una representación clara y simplifica su manejo.

Los dominios se diseñan para clasificar la cadena de conversión de energía eléctrica en cinco segmentos esenciales. Estos comprenden la **generación masiva**, que incluye la producción de energía eléctrica a gran escala, sea

mediante centrales que utilizan combustibles fósiles, energía nuclear, solar, entre otras.

El dominio de la **transmisión** abarca la infraestructura y organización encargadas del transporte de energía eléctrica. Por su parte, el dominio de la **distribución** se refiere a la red y organización por medio de las cuales se entrega la energía eléctrica a los consumidores finales.

El penúltimo dominio, denominado **recursos energéticos distribuidos** (DER), representa a aquellos recursos conectados a la red de distribución que participan en la generación de energía a menor escala. Finalmente, el dominio **instalaciones del cliente** incluye instalaciones industriales, comerciales y residenciales, así como la generación de electricidad por medios fotovoltaicos, almacenamiento en vehículos eléctricos, baterías, entre otros.

En cuanto a las zonas, estas delinean niveles jerárquicos en la gestión del sistema para la “integración del sistema de control empresarial”. Las zonas y sus respectivas descripciones son las siguientes:

Zona	Descripción
Proceso	Incluye la generación de energía de cualquier tipo (solar, eólica, hidráulica, etc.) y el equipo utilizado para esta.
Campo	Incluye los equipos utilizados para proteger, controlar y monitorear los procesos en la red.
Estación	Representa el nivel de agregación de área para el nivel de campo.
Operación	Se compone del control de los sistemas de energía en los dominios respectivos, por ejemplo: sistemas de gestión de energía, sistemas de gestión de distribución, etc.
Empresa	Incluye los procesos, servicios e infraestructuras comerciales y organizativos para empresas.
Mercado	Maneja las posibles operaciones de mercado a lo largo de la cadena de conversión de energía.

Tabla 4.1. Zonas y su descripción del marco SGAM.

Fuente: [15].

Originalmente, el modelo SGAM no se concibió para ser aplicado exten-

samente en escenarios de movilidad eléctrica, ni para abordar directamente sus casos de uso y sistemas. Así, la secuencia de procesos vinculada a la electromovilidad no encaja de manera íntegra en los dominios específicos de la SGAM, que están enfocados en la cadena de conversión de energía eléctrica. La movilidad eléctrica demanda, además, la interacción entre múltiples dominios, tales como la infraestructura de carga y los vehículos eléctricos, así como interfaces hombre-máquina diseñadas para usuarios, con casos de uso que se centran específicamente en aspectos de movilidad.

Viendo a los vehículos eléctricos (VE) como catalizadores de la electromovilidad, y al usuario de estos vehículos como el consumidor final, las interacciones entre ellos se representan en el SGAM principalmente a través del vehículo. Por ejemplo, las estaciones de carga son ubicadas dentro del SGAM en más de una ocasión, asignándolas tanto al dominio de recursos energéticos distribuidos como al de instalaciones del cliente, lo que puede resultar confuso.

Aunque la SGAM puede utilizarse de forma independiente, también es posible integrarla con modelos asociados a otros sectores, como el *Modelo de Arquitectura Genérica de Ciudades Inteligentes* (GSCAM, por sus siglas en inglés), para aplicaciones más amplias y multidisciplinarias.

4.1.1. E-Mobility Architecture Model (EMAM)

- Año de presentación del modelo, 2015:

En [16] se introduce el modelo EMAM, desarrollado por Uslar, Trefke y Gottschalk, y divulgado a través de dos publicaciones en el año 2015. Este modelo, inspirado en el previamente mencionado SGAM, adopta una estructura tridimensional enfocada en los vehículos eléctricos, aunque introduce variaciones en términos de zonas y dominios.

Respecto a las zonas, EMAM incluye: el automóvil, enchufe, cable, poste, punto común de acoplación (pcc) y la red. En cuanto a los dominios, el modelo incorpora: distribución, recursos energéticos distribuidos (DER), construcción, sistema de gestión de energía (que incluye la interfaz hombre-máquina) y baterías de vehículos eléctricos. La representación tridimensional de esta arquitectura se ilustra en la Figura 4.2.

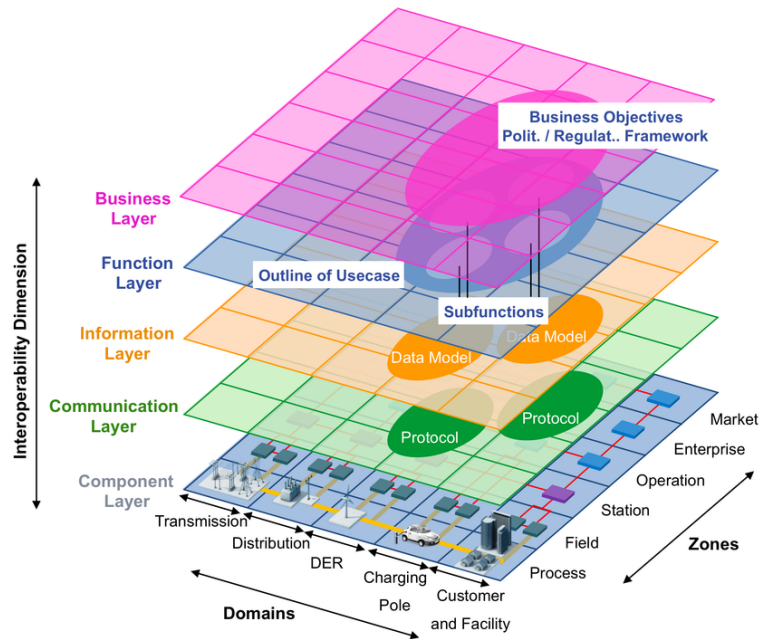


Figura 4.2. Marco EMAM.

Fuente: [16].

El modelo EMAM no detalla adecuadamente los dominios y zonas, aspectos cruciales en su estructura. Las zonas propuestas reflejan el proceso de carga de un vehículo eléctrico, sugiriendo que serían más apropiadas dentro del eje de dominio.

A pesar de que EMAM hace referencia a diversos estándares, como el “Mandato M/490” de la Unión Europea, estos no se integran explícitamente en las dimensiones del modelo. Esta omisión resulta en un marco incompleto, ya que no se definen las especificaciones técnicas correspondientes a cada capa, zona o dominio. Esta falta de especificidad otorga a los participantes del sistema la libertad de seleccionar los protocolos y estándares a emplear, sin una guía detallada.

4.1.2. E-Mobility -Information System Architecture (EM-ISA)

- Año de presentación del modelo, 2013:

En [17], los desarrolladores del modelo resaltan la importancia de la interoperabilidad en el ámbito de la electromovilidad y presentan el EM-ISA, diseñado específicamente para este sector. Este modelo se deriva de una

variedad de arquitecturas de Sistemas de Información (IS) genéricas, adaptándolas al esquema del SGAM.

El EM-ISA redefine la capa de información como capa de datos y la capa de componente como capa de elemento, integrando al usuario del vehículo eléctrico como un actor clave dentro del modelo. Esta aproximación, sin embargo, resulta en una menor separación de preocupaciones, ya que, al contar con menos dominios en comparación con otros modelos, no distribuye de manera equitativa los componentes y actores a través de las diferentes capas, zonas y dominios, provocando así una concentración excesiva de funciones en determinadas áreas.

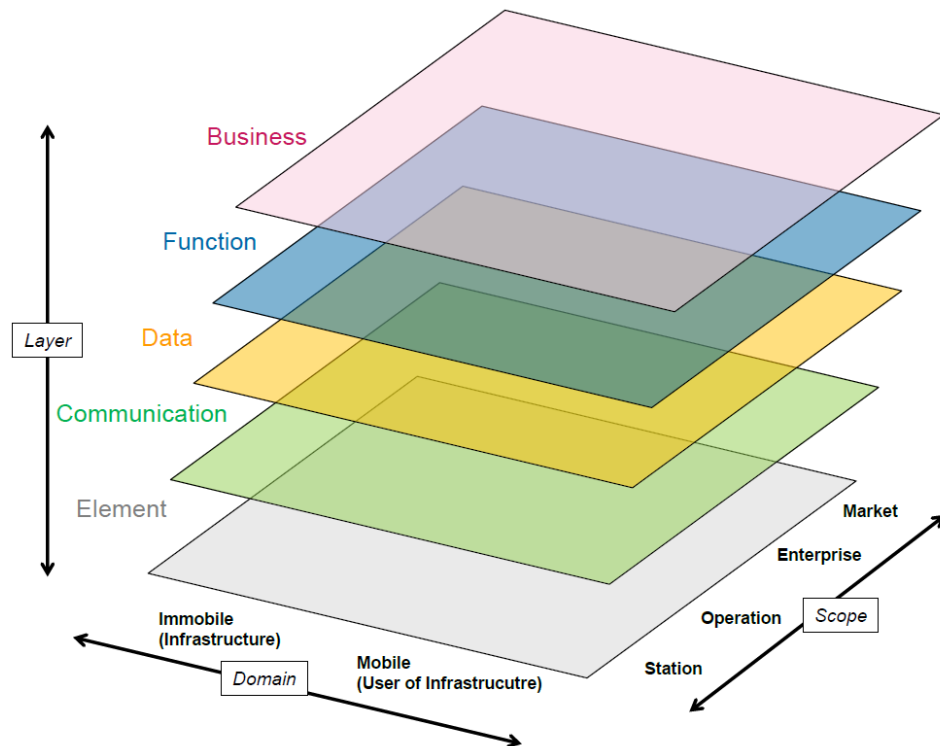


Figura 4.3. Marco EM-ISA.

Fuente: [17]

Por último, el modelo tan solo contempla la electromovilidad en la intersección entre movilidad y electricidad.

4.1.3. Smart City Infrastructure Architecture Model (SCIAM)

- Año de presentación del modelo, 2014:

Este modelo fue introducido en forma de borrador preliminar en [18]. Al igual que el SGAM, persigue la interoperabilidad dentro del contexto de una Smart City. Como se puede observar en la Figura 4.4, los dominios del modelo abarcan las diversas necesidades urbanas, como agua, salud, energía y seguridad, entre otros. Por lo tanto, no se enfoca exclusivamente en la electromovilidad, sino que la integra como un componente más dentro de los sectores de electricidad y movilidad de una ciudad inteligente.

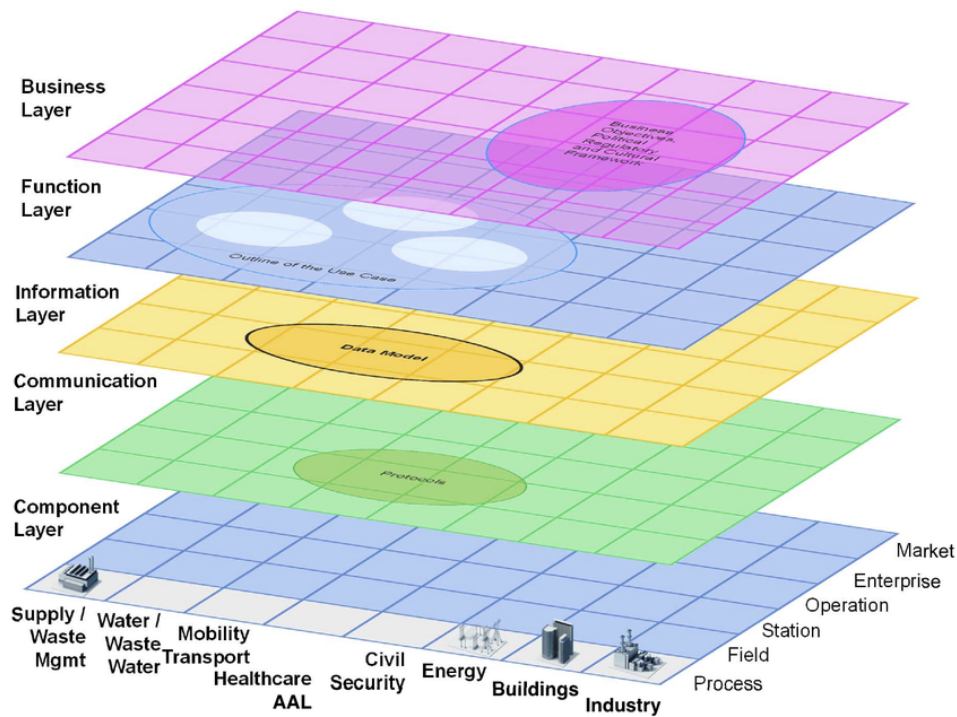


Figura 4.4. Marco SCIAM.

Fuente: [18].

4.1.4. Interoperability Reference Architecture for E-Mobility

- Año de presentación del modelo, 2015:

La “Interoperability Reference Architecture for E-Mobility” (Arquitectura de Referencia de Interoperabilidad para la Electromovilidad) [19] se crea para facilitar la integración de los vehículos eléctricos en el sistema eléctrico. Presenta una estructura unidimensional dividida en cuatro capas (ver Figura 4.5). Aunque esta estructura permite abordar la complejidad y promover la interoperabilidad a un nivel teórico, no establece estándares específicos. Las entidades implicadas están organizadas en las capas correspondientes.

Este marco puede operar de manera autónoma y sirve como referencia para el desarrollo de sistemas de movilidad eléctrica interoperables, pero no se orienta directamente a la ingeniería de sistemas complejos al carecer de herramientas y directrices concretas para su implementación.

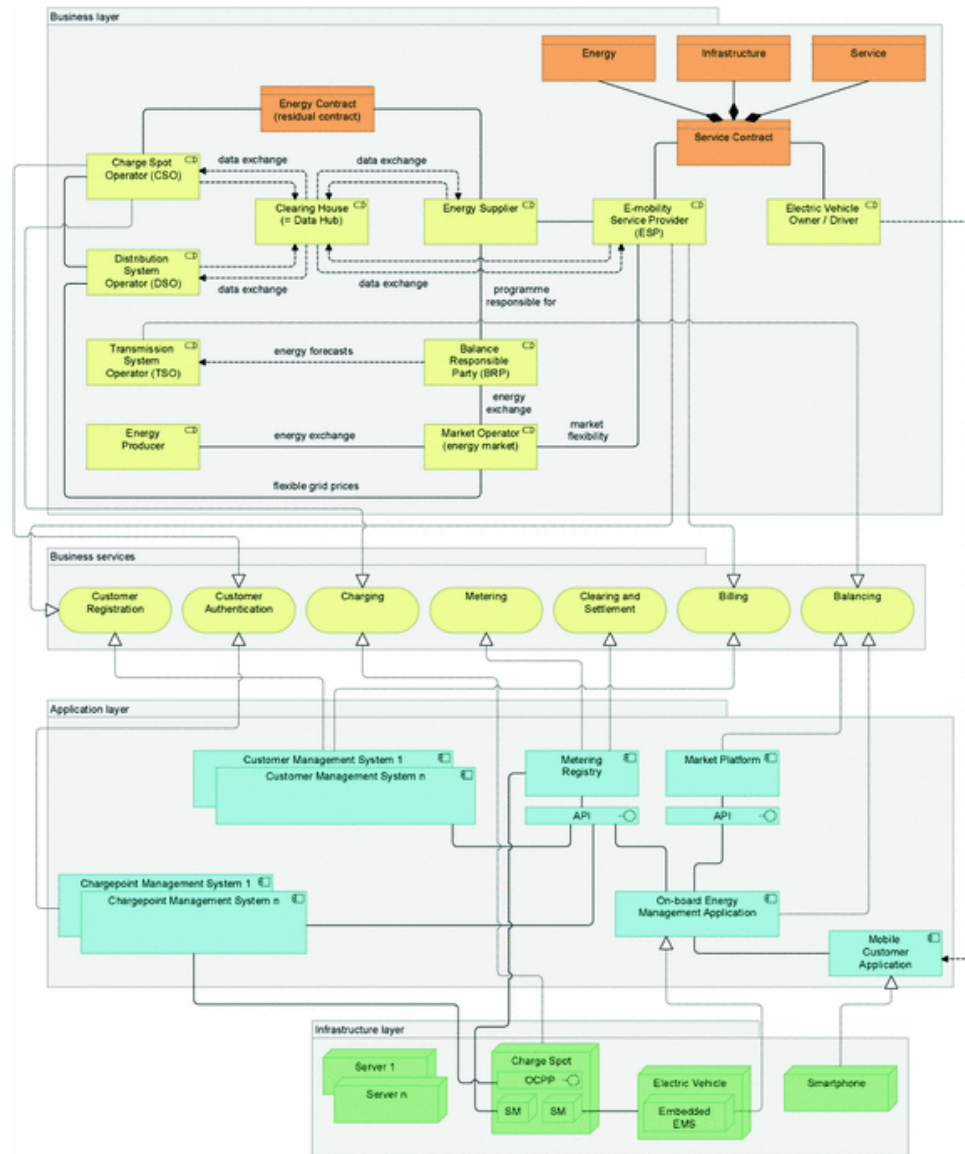


Figura 4.5. Marco Interoperability Reference Architecture for E-Mobility.

Fuente: [19].

4.1.5. E-Mobility Systems Architecture (EMSA)

- Año de presentación del modelo, 2019:

Según se menciona en [20], este modelo, al igual que el SGAM, ha servido de base para otros modelos y ha sido aplicado en diversos documentos para el diseño de sistemas de reserva de estaciones de carga y sistemas de carga inteligente, los cuales serán detallados posteriormente.

El EMSA se basa en principios derivados de los modelos previamente mencionados, estructurándose alrededor de cinco principios fundamentales:

1. El modelo debe abarcar de manera integral la electromovilidad, siendo aplicable de forma independiente, y considerando casos de uso y sistemas ajenos a otros sectores.
2. Debe especificar el número de dimensiones necesarias para el sector, ajustando únicamente aspectos específicos de la cadena de valor del dominio para proporcionar una abstracción clara.
3. Debe asegurar una asignación adecuada de todas las entidades de movilidad eléctrica dentro de su estructura, identificando y especificando la ubicación correcta para cada una en todas las dimensiones.
4. Debe ser independiente de la tecnología y no favorecer arquitecturas preexistentes, ofreciendo flexibilidad en sus capas para admitir casos de uso alternativos, y respaldando el desarrollo futuro mediante escalabilidad y extensibilidad.
5. Debe permitir la incorporación de nuevos dominios y zonas a medida que el sector evolucione.

El modelo EMSA es compatible con otros, como el SGAM, lo que significa que permite el uso concurrente de varios modelos dentro de una red eléctrica. No obstante, también puede funcionar como un marco de arquitectura independiente.

Este modelo comparte las capas de interoperabilidad y las zonas del SGAM, pero se centra más específicamente en la electromovilidad, a diferencia del SGAM, que aborda la red de distribución eléctrica en su conjunto. Por otra parte, los dominios del EMSA difieren al estar exclusivamente orientados hacia la electromovilidad.

Los dominios específicos del EMSA incluyen: conversión de energía, transferencia de energía hacia y desde el vehículo eléctrico, el vehículo eléctrico en sí, y las instalaciones para usuarios de vehículos eléctricos.

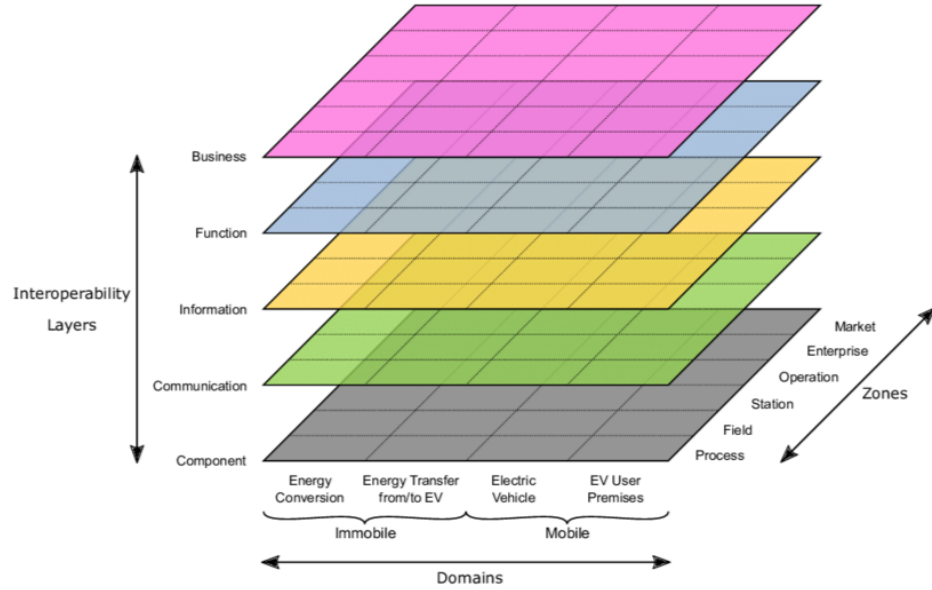


Figura 4.6. Marco EMSA.

Fuente: [20].

4.1.6. A Blockchain Based Electric Vehicle Smart Charging System with Flexibility

- Año de presentación del modelo, 2020:

Este modelo de carga inteligente para vehículos eléctricos, basado en la tecnología Blockchain [21], introduce una arquitectura distintiva a lo habitual, no siendo tridimensional como la mayoría.

Describe detalladamente los participantes y su interacción a través del flujo de energía, información o relaciones contractuales.

El artículo distingue tres tipos de carga para los vehículos eléctricos:

1. **Incontrolada:** conexión hasta completar la carga o hasta que el usuario decida desconectarlo.
2. **Retrasada:** se incentiva a los usuarios a cargar durante periodos de baja demanda en la red eléctrica, mediante tarifas diferenciadas.

3. **Inteligente:** regulada por algoritmos de optimización.

Blockchain se presenta como una estructura de datos distribuida y una red computacional, segura mediante firmas criptográficas y mecanismos de consenso. Los Smart Contracts, basados en Ethereum, facilitarían las solicitudes de recarga y la gestión de pagos en las estaciones de carga, incentivando a los usuarios mediante tokens (OLI Coin) para preferencias específicas de carga.

Inicialmente, se toma el modelo EMSA como referencia, dada su capacidad para gestionar cargas inteligentes a través del protocolo Online Certificate Status Protocol (OCSP), que verifica el estado de revocación de un certificado digital. Este enfoque basado en Blockchain requiere identificar los actores implicados en el intercambio de información para la carga inteligente y cómo reemplazar estos actores o la información sin recurrir al protocolo OCSP.

Los actores en el modelo EMSA incluyen:

- **Usuarios de VE:** individuos que usan vehículos eléctricos.
- **Operador del punto o estación de carga (CPO):** administra la estación.
- **eMSP:** gestiona la información entre usuarios de VE y CPO, facilitando localización, reserva de puntos de carga y pagos.
- **E-Mobility Clearing House:** gestiona los pagos de los usuarios de VE a los CPO.
- **Operador del sistema de distribución (DSO):** opera la red de distribución eléctrica y suministra electricidad a usuarios finales.
- **Comercializadora de suministros eléctricos:** vende electricidad a consumidores y compra energía al DSO.

Los Smart Contracts, en la plataforma Blockchain, reemplazarían funciones de la eMSP y E-Mobility Clearing House.

Este modelo es unidimensional, centrado en actores, procesos y flujos, en lugar de capas.

La arquitectura de recarga propuesta podría implementarse en una plataforma Blockchain, como se muestra en la Figura 4.7, siendo esta centralizada o descentralizada. En el modelo centralizado, un agregador actuaría como intermediario comprando energía para los usuarios de VE, mientras que en el descentralizado, las preferencias de carga del usuario influirían directamente en la flexibilidad de la operación de carga, en respuesta a la información de mercado disponible.

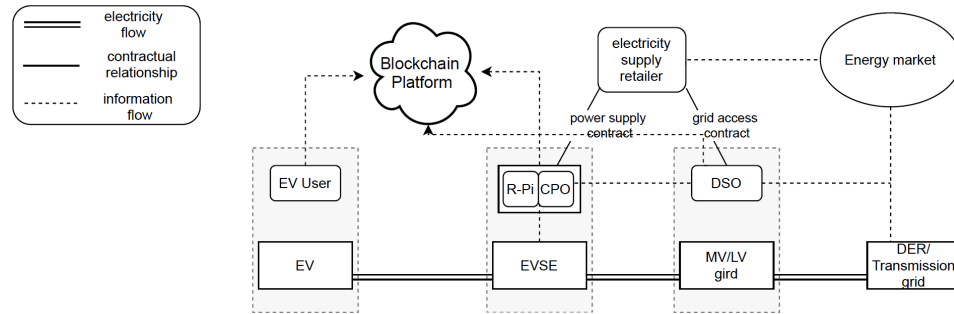


Figura 4.7. Arquitectura del sistema de carga utilizando la plataforma Blockchain.

Fuente: [21].

Las solicitudes de carga enviadas a la plataforma Blockchain deben incluir la cantidad de energía requerida y el tiempo máximo para la carga del vehículo eléctrico (VE), permitiendo así que la plataforma determine la viabilidad de realizar la carga, conforme al diagrama mostrado en la Figura 4.8. Cada 15 minutos, se revisan las solicitudes recibidas durante ese intervalo y se inician las cargas de aquellas que han sido aprobadas para el próximo período.

Estas solicitudes provienen de las infraestructuras de carga, las cuales están equipadas con una Raspberry Pi. Esta ejecuta un script en Python diseñado para interactuar con la red Blockchain cada 15 minutos.

Aunque los autores se centran en generar incentivos para opciones de carga como la carga inteligente que busca aliviar la congestión en la red eléctrica y en evaluar el impacto de estas medidas, el modelo actual no aborda la posibilidad de reservar estaciones de carga. Incorporar la reserva podría mejorar la previsión de demanda energética en momentos específicos y aumentar la satisfacción de los usuarios de VE que deseen planificar sus viajes mediante una aplicación móvil, una funcionalidad presente en otros

modelos que sí consideran la reserva de estaciones de carga.

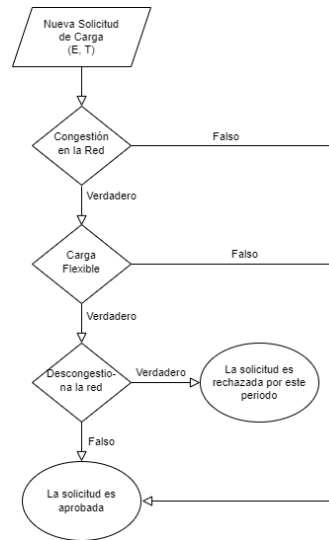


Figura 4.8. Diagrama de decisión de evento de solicitud carga.

Fuente: [21].

4.1.7. Applying Enterprise Architecture for Digital Transformation of Electro Mobility towards Sustainable Transportation

- Año de presentación del modelo, 2020:

En la publicación [22] se expone cómo esta arquitectura utiliza la Arquitectura Empresarial para facilitar la transformación digital de los servicios de electromovilidad, permitiendo la interacción de los vehículos eléctricos con la red de energía para asegurar la interoperabilidad y el adecuado flujo de información.

Desde su conceptualización por John Zachman en 1987, la Arquitectura Empresarial se ha consolidado como un pilar fundamental en la gestión empresarial y de sistemas de Tecnología de la Información (TI), facilitando la comunicación, documentación, planificación y diseño de soluciones para problemas comerciales y de TI.

El modelo IDS-RAM se propone como marco de Arquitectura Empresarial para la transformación digital en el ámbito de la electromovilidad. Este modelo se basa en la creación de un espacio de datos virtuales que integra

tecnologías y estándares existentes, junto con modelos de gobernanza para la economía de datos, promoviendo el intercambio seguro de datos en un ecosistema empresarial confiable.

Este modelo consta de 5 capas:

- **Capa de Negocios:** Define roles, interacciones y actividades principales, representando la perspectiva empresarial en el intercambio de información.
- **Capa de Funciones:** Describe los requerimientos y principales características del sistema digital.
- **Capa de Proceso:** Detalla las interacciones entre componentes, ofreciendo una visión dinámica del ecosistema.
- **Capa de Información:** Proporciona una vista conceptual de las fuentes de datos, tanto estáticas como dinámicas.
- **Capa de Sistema:** Incluye el hardware, infraestructura de TI y software relacionados con la generación y recopilación de datos.

Adicionalmente, incluye tres perspectivas esenciales: Seguridad, Certificación y Gobernanza, como se muestra en la Figura 4.9. Sin embargo, la ausencia de zonas o dominios compromete la separación de preocupaciones en el sistema, dificultando la gestión de la complejidad inherente a la separación de actores, funciones y áreas de interés dentro de la arquitectura.

En resumen, este modelo representa una adaptación de un marco existente hacia el sector de la electromovilidad, de manera similar a lo que se realiza con el SGAM. Su principal objetivo es apoyar la integración de datos de servicios de electromovilidad, aunque no enfatiza suficientemente en la interoperabilidad. Además, el modelo no detalla el modelado de componentes desde una perspectiva arquitectónica ni valida los datos reales, limitando su aplicación práctica.

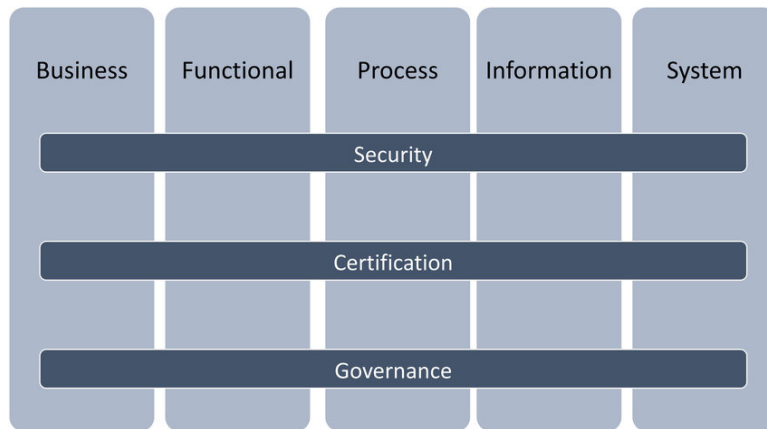


Figura 4.9. Marco IDS-RAM.

Fuente: [22].

4.2. Referencias hacia el modelo EMSA

Tras la presentación de este modelo, ha servido de ejemplo y/o fundamento para el desarrollo de otros modelos en el ámbito de la electromovilidad. Sin embargo, han surgido críticas relacionadas con él, destacando principalmente las vulnerabilidades detectadas en el sistema. A pesar de estas críticas, el modelo también ha sido aplicado en la implementación de diversas funcionalidades dentro de sistemas de electromovilidad, demostrando su utilidad práctica a pesar de los desafíos identificados.

4.2.1. Crítica: Vulnerabilidades de comunicación en un sistema

Robert Basmadjian, en [23], ofrece una crítica detallada al modelo EMSA, resaltando vulnerabilidades asociadas a la comunicación entre los diferentes actores involucrados en el sistema de electromovilidad.

Este sistema, concebido como un sistema ciberfísico centrado en el ser humano (HCPS), incluye cinco entidades clave: Vehículos Eléctricos (VE), Estaciones de Carga para Vehículos Eléctricos (EVSE), Operador de Punto de Carga (CPO), Operador del Sistema de Distribución (DSO) y eMSP. La comunicación dentro del sistema sigue patrones específicos: VE-EVSE, EVSE-CPO, CPO-eMSP, así como DSO-CPO y DSO-eMSP.

Las vulnerabilidades en la recarga inteligente son de particular preocupación, ya que los ciberataques podrían forzar a las estaciones de carga a consumir más energía de la asignada, potencialmente causando daños a transformadores y líneas de alimentación.

Cada par de entidades comunicantes enfrenta sus propias amenazas y vulnerabilidades, con impactos variados en el sistema. La evaluación de riesgos utiliza escalas cualitativas (bajo, medio, alto) y semicuantitativas (1 a 10) para su análisis.

Los ataques potenciales al sistema incluyen:

- **Man-in-the-Middle:** intervención en las comunicaciones para insertar información falsa o suplantar la identidad de alguna entidad.
- **Suplantación de identidad:** uso ilegítimo de credenciales de alguna entidad para autenticación y validación.
- **Escuchas ilegales:** interceptación de información entre dos entidades para análisis no autorizado.
- **Denegación de servicio:** saturación del canal de comunicación, impidiendo o retrasando solicitudes legítimas.
- **Manipulación de mensajes:** alteración de información perteneciente a otra entidad.
- **Repudio:** fallo en la ejecución adecuada de sistemas, servicios o procesos, ya sea de manera deliberada o involuntaria.

El artículo destaca las vulnerabilidades presentes en la implementación del modelo EMSA y subraya la importancia de considerar estas vulnerabilidades al implementar sistemas de electromovilidad.

Se enfatiza la necesidad de abordar las vulnerabilidades del sistema, buscando estándares y protocolos que aseguren la seguridad del HCPS, especialmente considerando las altas calificaciones de riesgo obtenidas en algunas comunicaciones entre las entidades principales del sistema.

4.2.2. Referencia a la arquitectura para sistemas de reserva interoperables

En el trabajo de [24], se introduce un innovador sistema de reserva para estaciones de carga basado en el modelo EMSA, buscando garantizar la interoperabilidad del sistema con el propósito de ofrecer una experiencia de usuario mejorada, minimizar la ansiedad por la posibilidad de quedarse sin batería durante el trayecto y reducir el tiempo total de viaje.

Este sistema propone cuatro modalidades de recarga, ilustradas en la Figura 4.10, de las cuales dos requieren el uso del sistema de reserva para operar. Las modalidades de carga son:

- **Ad-Hoc incierto:** no garantiza la disponibilidad de una estación de carga al momento de la llegada del usuario.
- **Planeado incierto:** implica una planificación previa sin asegurar la disponibilidad de la estación de carga.
- **Ad-Hoc garantizado:** asegura la disponibilidad inmediata de una estación de carga sin necesidad de una planificación previa.
- **Planeado garantizado:** combina la planificación previa con la garantía de disponibilidad de la estación de carga.

Las modalidades garantizadas ofrecen la certeza de que el usuario podrá cargar su vehículo de manera inmediata al llegar a la estación, tanto para recargas Ad-Hoc como planeadas. Por otro lado, las modalidades inciertas no ofrecen garantía de disponibilidad del cargador en la estación, ya sea por falta de información o por la imposibilidad de reservar con antelación.

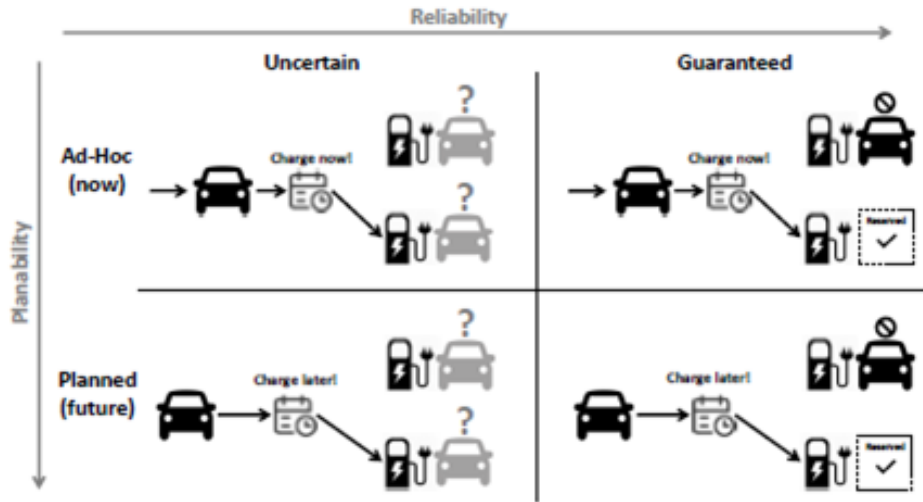


Figura 4.10. Enfoques de reserva factibles.

Fuente: [24].

Las recargas *Ad-Hoc* se caracterizan por ser inmediatas y no planificadas, en contraste con las recargas *Planeadas*, que se organizan anticipadamente mediante una aplicación en la que el usuario indica su ruta y selecciona las estaciones de carga donde se detendrá, permitiendo así su reserva previa.

El sistema debería ofrecer información en tiempo real sobre la disponibilidad de las estaciones de carga y su programación para futuras reservas de recargas *Planeadas*, aprovechando la estructura del modelo EMSA, incluyendo sus capas, dominios y zonas.

Las simulaciones presentadas en el artículo comparan el uso de recargas *Ad-Hoc* frente a recargas *Planeadas*, mostrando que estas últimas contribuyen a reducir tanto el tiempo total del viaje como el tiempo de espera por disponibilidad en las infraestructuras de recarga.

4.3. Conclusiones

Al abordar la electromovilidad, es crucial considerar un proceso de diseño e ingeniería adecuado para sistemas de ingeniería, con el fin de alinear casos de uso, modelos de negocio y políticas públicas. En este contexto, el modelo SGAM se ha propuesto como un marco de arquitectura de sistemas para facilitar el diseño y desarrollo en el sector energético.

Para la electromovilidad, se han propuesto diversos modelos, como se muestra en la Tabla 4.2. Algunos, como el SGAM, incluyen la electromovilidad dentro del ámbito de ciudades inteligentes, mientras que otros, como el modelo EMSA, se centran específicamente en este sector.

Sin embargo, es importante resaltar que estos modelos no abordan de manera explícita la seguridad. No definen protocolos específicos para el intercambio de información entre los actores involucrados, ni designan un ente regulador para asegurar la protección de los datos, representando un desafío significativo para la confiabilidad de los sistemas de electromovilidad.

Se realiza un análisis comparativo sobre el alcance de la electromovilidad, estructura, asignación de entidades y aplicabilidad, considerando aspectos como:

- **Bases:** Fundamentos de modelos de interoperabilidad previos.
- **Alcance:** Enfoque específico del modelo.
- **Estructura:** Dimensiones arquitectónicas del modelo.
- **Asignación de entidades:** Estándares, protocolos y actores involucrados.
- **Independencia:** Capacidad del modelo para operar de manera autónoma.
- **Acoplamiento Sectorial:** Aplicabilidad en sectores adicionales a la electromovilidad.
- **Contemplación de Vulnerabilidades:** Reconocimiento de riesgos y amenazas.
- **Complejidad:** Estrategias para la gestión y reducción de la complejidad.
- **Interoperabilidad:** Facilidades para asegurar la compatibilidad de sistemas.
- **Validación:** Proceso de corroboración del modelo.

La revisión destaca una carencia general en la consideración de vulnerabilidades y sus soluciones, lo que incrementa el riesgo de ataques al sistema eléctrico.

Por tanto, se identifica una oportunidad significativa de contribución en el ámbito de la seguridad, ya sea abordando las vulnerabilidades generales de los sistemas o centrándose en un modelo específico para profundizar en sus vulnerabilidades y soluciones.

INTEROPERABILIDAD

Nombre	Bases	Alcance	Estructura	Asignación de entidades en las dimensiones	Independiente	Acoplamiento Sectorial	Contempla Vulnerabilidades	Complejidad	Interoperabilidad	Validación
EV Smart Charging Report (for SGAM) (CEN-CENELEC 2015)	SGAM	Carga inteligente de vehículos eléctricos	3 dim.	+	+	+	-	AC, SC, RU, EP	+	+ (Estudio)
E-Mobility Architecture Model (EMAM) (Uslar and Gottschalk 2015)	SGAM	VE	3 dim.	-	+	(+)	-	AC, SC, RU	(+)	-
E-Mobility Information System Architecture (EM-ISA) (Schuh et al. 2013)	SGAM, ISA	Sistema de Información de electromovilidad	3 dim.	(+)	+	-	-	AC, SC, RU	(+)	-
Smart City Infrastructure Architecture Model (SCIAM) (DKE/DIN/VE 2014)	SGAM	Ciudades Inteligentes (Movilidad, Energía)	3 dim.	-	(+)	(+)	-	AC, SC	-	-
Interoperability Reference Architecture for E-Mobility (Brand et al. 2015)	Arquitectura Empresarial	Integración de una red de VE	1 dim.	(+)	+	-	-	AC, SC, RU	(+)	+ (Entrevistas)
E-Mobility Systems Architecture (EMSA) (Kripes et al. 2019)	SGAM	Arquitectura de un sistema para la electromovilidad	3 dim.	+	+	+	-	AC, SC, RU, EP	+	+ (Estudio)
A Blockchain Based Electric Vehicle Smart Charging System with Flexibility (Gowin et al. 2020)	EMSA	Sistema de carga inteligente	1 dim.	-	+	-	-	AC, SC	-	-
Applying Enterprise Architecture for Digital Transformation of Electro Mobility towards Sustainable Transportation (IDS-RAM) (Bokolo 2020)	IDS-RAM	Integración de datos de los servicios de electromovilidad	1 dim.	+	+	-	-	AC, RU	-	-

Valido: +, Parcialmente Valido: (+), Invalido: -

AC - abstracción y conceptualización (basado en modelos), SC - separación de preocupaciones (puntos de vista), RU - reutilización (estandarización y armonización), EP - reducir la complejidad del proceso de ingeniería (orientación, documentación)

Tabla 4.2. Descripción general de los modelos de arquitectura y marcos para la movilidad eléctrica

Capítulo 5

Seguridad

La seguridad en los sistemas de carga para vehículos eléctricos representa un aspecto crítico, dada la naturaleza sensible de la información intercambiada entre sus componentes. Conforme a [11], este intercambio puede incluir contratos, credenciales, certificados, entre otros, lo cual subraya la importancia de proteger dicha información para prevenir vulneraciones al sistema de carga.

Como se destacó en [23], se ha llevado a cabo un análisis de las vulnerabilidades presentes en el modelo EMSA, así como de los riesgos asociados a estas. En este segmento, se abordará la ciberseguridad y las vulnerabilidades específicas de los sistemas de carga de vehículos eléctricos.

Se hará referencia a diversos artículos, estudios e investigaciones que han sido desarrollados con el objetivo de identificar y analizar las vulnerabilidades existentes en los sistemas de carga de vehículos eléctricos, destacando la importancia de este ámbito en la investigación de la seguridad informática aplicada a la electromovilidad.

5.1. Ciberseguridad en el sistema de carga de vehículos eléctricos

La seguridad en el sistema de carga de vehículos eléctricos es crucial, especialmente por el intercambio de información sensible entre sus componentes. Según [29], se propone una metodología para estimar la generación de energía eólica y la demanda energética para cargar vehículos eléctricos, con el objetivo de gestionar las recargas de manera inteligente y mitigar problemas en la red eléctrica. Sin embargo, la presencia de vulnerabilidades podría permitir a atacantes causar cortes de energía, comprometiendo la efectividad del método.

Desde 2016, la Red Europea de Seguridad Cibernética y la Asociación Europea de Operadores de Sistemas de Distribución para Redes Inteligentes, según [30], han establecido requisitos de ciberseguridad para infraestructuras de carga, proporcionando un marco práctico para municipios y operadores de redes en toda Europa. Estos requisitos incluyen:

- Diseño adaptable para actualizaciones futuras.
- Uso restringido de algoritmos y protocolos criptográficos para encriptar la información.
- Protección de comunicaciones, especialmente en puntos de carga vulnerables.
- Endurecimiento del sistema, limitando funciones y accesos no esenciales.
- Resiliencia, con medidas para proteger datos críticos y restaurar rápidamente el servicio tras fallas.

Además, [28] analiza en profundidad las estaciones de carga, identificando vulnerabilidades críticas que podrían causar inestabilidades e interrupciones en el servicio eléctrico.

Ref. [25] propone el uso de un entorno de emulación para sistemas de carga rápida, incorporando los distintos componentes del sistema. Según el artículo, este enfoque facilita la escalabilidad para satisfacer demandas analíticas futuras, mejorando simultáneamente la seguridad y la interoperabilidad

del sistema.

Por otro lado, [27] explora la aplicación de la tecnología blockchain para incrementar la seguridad en el manejo de datos del sistema. A diferencia de [21], este trabajo se enfoca en desarrollar “BlockEV”, un protocolo basado en blockchain para la selección eficiente de estaciones de carga para vehículos eléctricos. Este protocolo tiene como objetivo asegurar la seguridad y privacidad de los usuarios, garantizar la disponibilidad de estaciones de carga y mejorar la experiencia general del usuario. Se propone un marco basado en blockchain para la implementación de servicios de reserva y carga segura mediante contratos inteligentes, abordando también el desafío de optimizar la selección de la estación de carga.

Varias fuentes, incluyendo [23, 25, 28], discuten las vulnerabilidades específicas de los sistemas de carga, ya sea como sistemas independientes o en conjunto con modelos de interoperabilidad. Estas vulnerabilidades se detallan en la Tabla 5.4, indicando su impacto potencial en las capas, dominios y zonas del modelo EMSA, las cuales se buscará detectar y/o corregir en la capa que será propuesta más adelante.

Id	Vulnerabilidad	Referencia
1	Ataques de intermediario (Man-in-the-Middle, MiM) pueden ser ejecutados al introducir un punto de carga falso entre el VE y el punto de carga autorizado, redirigiendo la comunicación y desviando parte de la energía hacia un VE no autorizado. Esto resulta en un robo parcial de energía, con el VE legítimo recibiendo solo una fracción de la energía adquirida.	[23, 32]
2	Posibilidad de que atacantes intercepten información confidencial de autenticación y autorización durante las transacciones de cobro y las señales de control entre el VE, el punto de carga y el proveedor de servicios de movilidad eléctrica, incluyendo el número de identificación del vehículo.	[23, 32, 33]
3	Atacantes pueden hacer uso de información confidencial robada para suplantar la identidad de un VE autorizado y acceder a la red del sistema de carga.	[23, 32, 33]
4	Inserción de dispositivos lector de tarjetas falsos en puntos de carga o el uso de teléfonos con NFC para capturar en secreto datos de tarjetas RFID, como el número de identificación.	[23, 34]
5	Atacantes pueden ingresar al sistema suplantando un VE usando certificados válidos, claves privadas o certificados expirados, aprovechando desincronizaciones horarias en el sistema.	[23, 35]
6	Atacantes, mediante la colaboración de un VE y un punto de carga, pueden alterar los mensajes relacionados con el suministro de energía o la tarifa de cobro, permitiendo a un usuario recibir más energía de la solicitada o alterar los detalles de pago para obtener beneficios ilícitos.	[23, 35]

Tabla 5.1. Vulnerabilidades identificadas en los sistemas de carga para vehículos eléctricos del Id 1 al 6.

Id	Vulnerabilidad	Referencia
7	Ataques que vuelven inaccesible un punto de carga mediante el retraso o manipulación de mensajes de medición de carga, afectando la disponibilidad del servicio.	[23, 32, 33]
8	Manipulación de la comunicación entre el punto de carga y el operador de la estación, permitiendo la inserción de datos falsos o la suplantación de identidades, con potenciales efectos adversos en el sistema.	[23, 36, 37]
9	Eliminación o reproducción selectiva de mensajes en la comunicación entre el punto de carga y el operador, causando interrupciones en el servicio de carga y afectando la estabilidad del sistema.	[23, 36, 37]
10	Riesgo de robo de credenciales estáticas por empleados deshonestos o escuchas no autorizados durante la fase de configuración del protocolo, lo que podría facilitar ataques MiM y de suplantación de identidad.	[23, 38]
11	Vulnerabilidades debido a la insuficiente seguridad de TLS, permitiendo a atacantes alterar datos en tránsito entre subsistemas, lo que podría comprometer la integridad de la información recibida por los usuarios.	[23, 38]
12	El operador del punto de carga tiene acceso a datos transmitidos entre los puntos de carga y los vehículos eléctricos, como el ID de contrato del usuario y las tarifas de energía específicas, que son reenviados al proveedor de servicios de movilidad eléctrica. Esto compromete la privacidad y la seguridad de los datos de los usuarios del sistema de carga.	[23, 38]

Tabla 5.2. Vulnerabilidades adicionales identificadas en los sistemas de carga para vehículos eléctricos del Id 7 al 12.

Id	Vulnerabilidad	Referencia
13	Empleados con malas intenciones del operador del sistema de distribución o del proveedor de servicios de movilidad eléctrica pueden manipular planes de carga y alterar los datos de medición para beneficio personal o realizar acciones dañinas en el sistema.	[23, 38]
14	La combinación de dispositivos, protocolos de comunicación y aplicaciones desactualizadas e inseguras crea una postura de seguridad cibernética débil, poniendo en riesgo la información de carga y el control sobre ella.	[25, 38, 39]
15	La implementación insegura de protocolos en sistemas obsoletos hace que la nueva infraestructura de carga sea propensa a ciberataques, particularmente la comunicación crítica entre un vehículo eléctrico y la infraestructura de carga, debido a la coordinación necesaria del voltaje y los parámetros de carga.	[25]
16	Atacantes pueden revertir la funcionalidad del servicio de interfaz binaria para descubrir puntos de acceso y sus parámetros, permitiendo la inserción de XSS en aplicaciones web de control de puntos de carga. Esto podría llevar al control de sesiones de usuarios, permitiendo la manipulación de cuentas y configuraciones de puntos de carga. Un control de nivel administrador por parte del atacante implica acceso total a funciones y datos del operador de puntos de carga.	[28, 40, 41]
17	La explotación de vulnerabilidades SQLi en aplicaciones web de gestión de puntos de carga, debido a la falta de validaciones de datos ingresados por usuarios. Esto permite a atacantes acceder a bases de datos con registros de usuarios y credenciales de cuentas de alto privilegio, pudiendo modificar firmware o acceder a información confidencial a través de inyecciones SQL en formularios y endpoints.	[28]

Tabla 5.3. Vulnerabilidades identificadas en los sistemas de carga de vehículos eléctricos Id 13 al 17.

Id	Vulnerabilidad	Referencia
18	Uso de técnicas de CSRF para engañar a usuarios y realizar acciones no deseadas, lo que puede llevar al control de la cuenta del usuario y manipulación de la configuración del punto de carga. Esto posibilita al atacante acceder y controlar todas las funcionalidades del operador de la estación de carga si el usuario afectado posee privilegios administrativos.	[28]
19	Revelación de información confidencial a usuarios no autorizados por parte de puntos de carga y operadores de estaciones, debido a configuraciones incorrectas del sistema o a una inadecuada gestión de permisos en ciertos endpoints.	[28]
20	Realización de ataques de navegación forzada que permiten eludir la autenticación y acceder al panel de administración de los puntos de carga, exponiendo información de usuarios, detalles de procesos de carga y otros datos sensibles del sistema.	[28]
21	Posibilidad de que un atacante utilice puntos de carga comprometidos para formar una botnet y ejecutar diversos ataques cibernéticos, como denegaciones de servicio (DoS) o actividades de exploración en la red.	[28]
22	Explotación de vulnerabilidades como CORS y configuraciones incorrectas de FCDP en aplicaciones de gestión de puntos de carga, permitiendo la filtración y uso indebido de información confidencial de los usuarios para acceder a sus cuentas.	[28]
23	Vulnerabilidad de inyección CSV (CSV _i) en la funcionalidad de inicialización de configuración dentro del firmware EVlink, que permite incrustar y activar cargas útiles de XSS al cargar archivos CSV manipulados, facilitando la escalada de privilegios mediante el secuestro de tokens de sesión de administradores.	[28]

Tabla 5.4. Vulnerabilidades identificadas en los sistemas de carga de vehículos eléctricos Id 18 al 23.

En resumen, se han identificado varios artículos que destacan, analizan y evalúan las vulnerabilidades presentes en los sistemas de carga para vehículos eléctricos. En algunos de estos trabajos, se ofrecen soluciones y/o recomendaciones dirigidas a mejorar la seguridad de dichos sistemas. Sin embargo, no se encontraron estudios que propongan soluciones específicas a estas vulnerabilidades en el contexto de modelos de interoperabilidad para el sistema de carga de vehículos eléctricos. Por tanto, se identifica una oportunidad significativa para contribuir en esta área con investigaciones futuras.

Capítulo 6

Capa de seguridad

Considerando las vulnerabilidades de seguridad identificadas en modelos de interoperabilidad discutidos en capítulos anteriores, este capítulo introduce una capa de Seguridad, visualizable en la Figura 6.1. Esta capa está diseñada para ser aplicable a distintos modelos de interoperabilidad, existentes o futuros, con el propósito de evaluar y reforzar la seguridad del sistema.

Esta capa tiene como objetivo principal proteger información sensible, evitando el robo, clonación y suplantación de identidad durante transacciones de pago por carga.

Así, el enfoque de esta tesis se orienta a una aplicación a nivel nacional, priorizando la protección de datos de usuarios y estaciones de carga, sin abordar soluciones a vulnerabilidades que involucren ataques físicos a la red de distribución eléctrica.

6.1. Descripción de la capa

A pesar de la existencia de numerosos modelos de interoperabilidad en el sistema de carga de vehículos eléctricos, muchos de ellos no cubren de manera integral la seguridad requerida. Por ello, se propone una capa de seguridad aplicable a estos modelos para identificar, evaluar y, en lo posible, proponer soluciones a las vulnerabilidades detectadas mediante controles de seguridad. Esta implementación podría conllevar la introducción de nuevas funciones y/o actores para mitigar las vulnerabilidades identificadas.

La capa está enfocada en analizar casos de uso dentro del sistema en busca de potenciales vulnerabilidades, lo que implica un análisis exhaustivo de los intercambios de información entre los actores de los modelos propuestos.

Es relevante mencionar que esta capa se concentra exclusivamente en aspectos de seguridad relacionados con la infraestructura, el intercambio de información entre componentes y/o actores, estándares, protocolos y software, dejando fuera las estafas dirigidas directamente a los usuarios, como el envío de mensajes fraudulentos o el acceso a sitios web maliciosos.

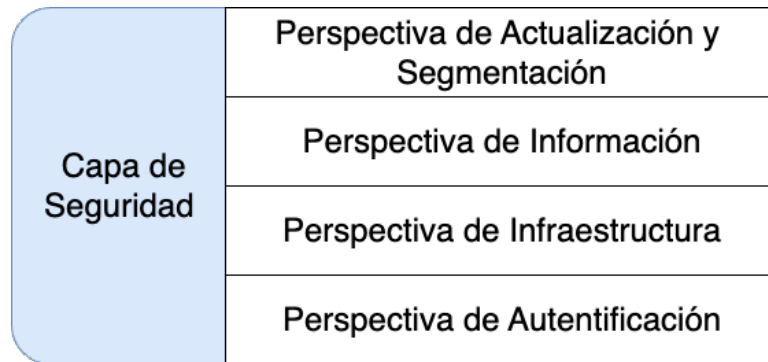


Figura 6.1. Capa de seguridad.

Esta capa contempla la generación de alertas ante la detección de vulnerabilidades o brechas de seguridad que expongan debilidades específicas en el sistema. Es esencial que el sistema de carga integre capacidades de Seguridad de la Información y Gestión de Eventos (SIEM por sus siglas en inglés), facilitando la identificación de comportamientos anómalos del usuario y aplicando inteligencia artificial para automatizar los procedimientos manuales relacionados con la detección de amenazas y la respuesta ante incidentes.

Además, resulta crucial implementar un mecanismo de sincronización horaria en el sistema para mitigar riesgos asociados con el uso de certificados expirados. La falta de sincronización entre las distintas infraestructuras del sistema podría permitir el uso no intencionado de certificados caducados, aumentando la exposición a vulnerabilidades.

La capa de seguridad sugerida en esta tesis se fundamenta en diversas estrategias de protección, indispensables para identificar y prevenir vulnerabilidades en modelos de interoperabilidad dentro del sistema de carga de vehículos eléctricos, particularmente en los procesos de pago por recarga.

Las perspectivas de la capa planteada son las siguientes:

- Actualización y segmentación.
- Información.
- Infraestructura.
- Autenticación.

6.1.1. Perspectiva de actualización y segmentación

En esta perspectiva, se enfatiza el control sobre la actualización de versiones de protocolos de seguridad y software esenciales para el intercambio de información, así como la adecuada segmentación de los estándares y protocolos utilizados por los componentes o agentes del modelo.

Es crucial optar por versiones con soporte a largo plazo (LTS) dado que estas suelen incluir soluciones a vulnerabilidades previamente identificadas, además de mejoras en rendimiento y seguridad.

Los autores en [26] subrayan la importancia de mantener actualizado el software de las infraestructuras de recarga EV, basándose en un estudio de Kaspersky que reveló cómo las vulnerabilidades en dicho software podrían comprometer la red eléctrica de un hogar. La actualización oportuna del software por parte de los proveedores es crucial para mitigar tales riesgos, ya que las nuevas versiones tienden a ofrecer mejoras significativas y soluciones a vulnerabilidades conocidas.

El Diagrama de la Figura 6.2 ilustra el proceso de evaluación para esta dimensión del sistema, destacando los riesgos de vulnerabilidades asociados con protocolos y software desactualizados, y proporcionando una guía para cuando es posible realizar actualizaciones.

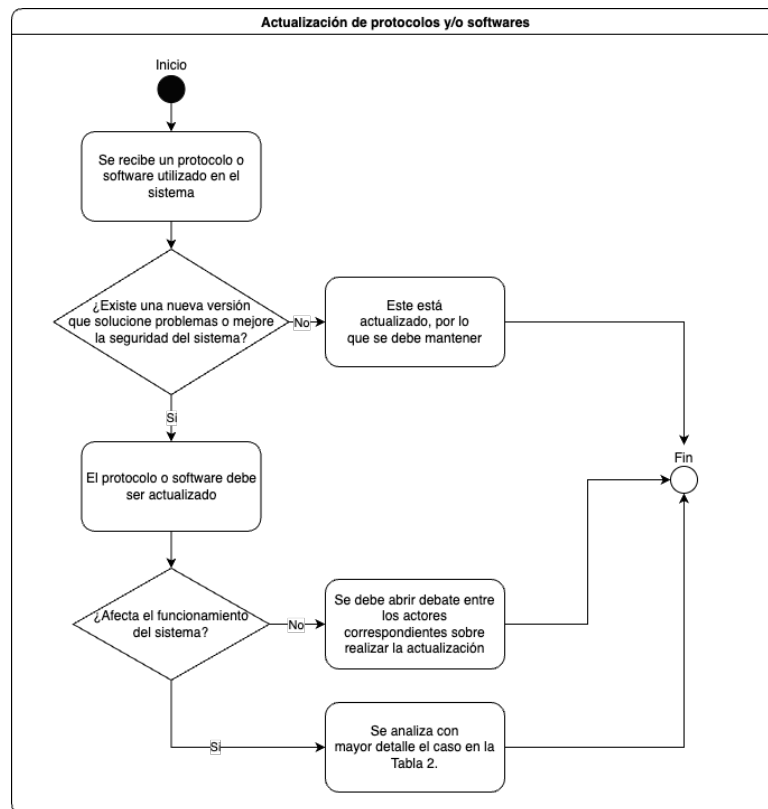


Figura 6.2. Diagrama de actualización de protocolos y/o softwares.

Caso	Acción
Actualización resuelve una vulnerabilidad	Es crucial debatir sobre la actualización y considerar la adaptación del sistema o el reemplazo del protocolo o software vulnerable por una opción segura.
Actualización mejora la seguridad	Aunque el sistema pueda operar sin actualizar mientras no existan vulnerabilidades críticas, se recomienda actualizar lo antes posible para mejorar la seguridad.

Tabla 6.1. Plan de acciones para caso especial de Figura 6.1.

La segmentación de estándares y protocolos tiene como objetivo establecer criterios técnicos y de calidad específicos para cada componente o sistema dentro del modelo, siguiendo normativas y estándares internacionales en la recarga de vehículos eléctricos. Esto asegura una operación eficiente y facilita la compatibilidad entre diferentes estándares y protocolos.

Según [31], la segmentación efectiva de estándares y protocolos, organizada en capas del modelo y dividida por dominios específicos, es esencial para la cohesión del sistema.

6.1.2. Perspectiva de información

Esta perspectiva garantiza que todo intercambio de información entre actores del sistema sea cifrado mediante encriptación asimétrica, evitando el uso de algoritmos obsoletos.

Además, se verifica que la información compartida sea relevante y no exponga datos innecesarios, siguiendo las recomendaciones de [26].

Finalmente, se implementan controles sobre los datos manejables por el usuario en servicios de backend para prevenir inyecciones de información, scripts maliciosos, o falsificación de solicitudes, utilizando parametrización y sanitización de datos. La Figura 6.3 muestra el diagrama correspondiente, incluyendo el uso de tokens CSRF para reforzar la seguridad en las solicitudes del cliente.

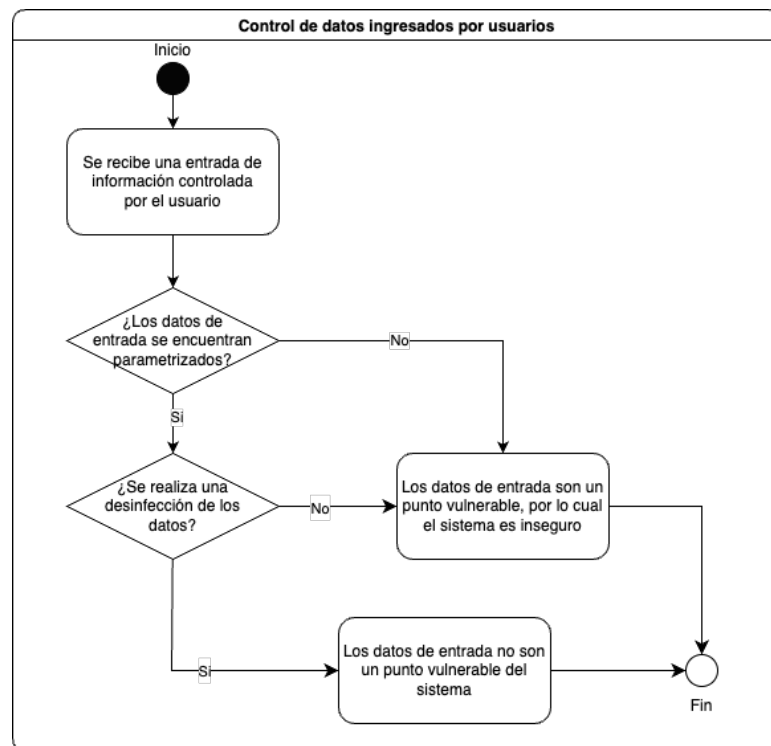


Figura 6.3. Diagrama de control de datos ingresados por el usuario.

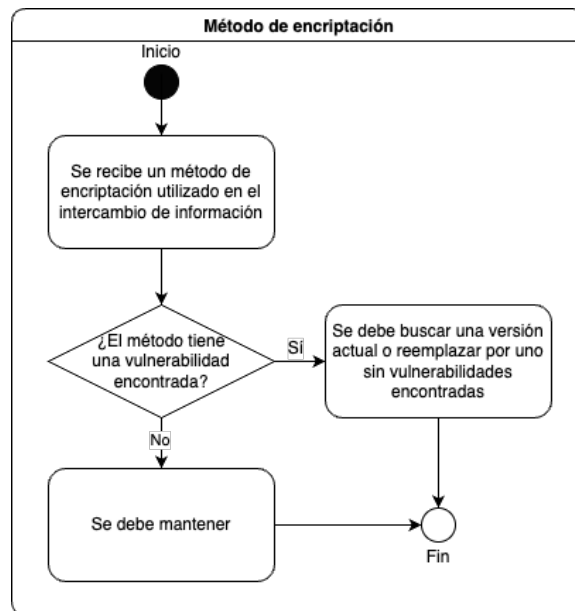


Figura 6.4. Diagrama de métodos de encriptación.

En el diagrama de la Figura 6.4, se presenta el procedimiento para evaluar los métodos de cifrado empleados en el sistema. Este proceso incluye la posibilidad de sustituir métodos vulnerables por versiones más recientes o con mayor complejidad criptográfica, mejorando así la seguridad del modelo.

Por otra parte, el diagrama de la Figura 6.5 tiene como objetivo filtrar y descartar la información irrelevante intercambiada entre los actores del sistema. Esta medida previene la divulgación innecesaria de datos sensibles que no requieren ser compartidos.

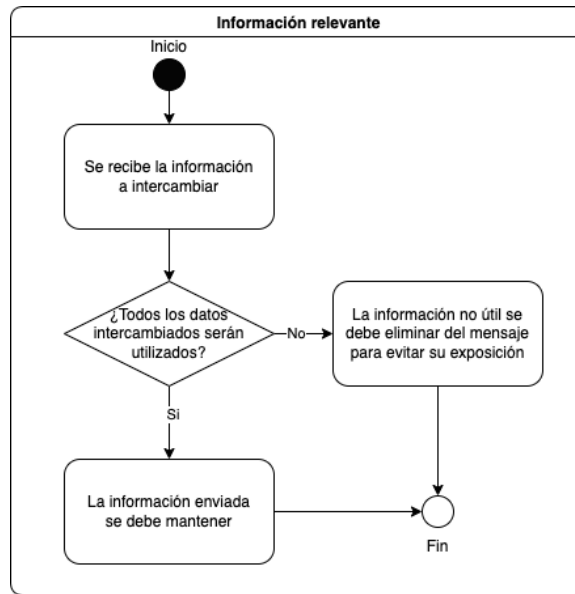


Figura 6.5. Diagrama de información relevante.

6.1.3. Perspectiva de infraestructura

Esta perspectiva se centra en el control de las infraestructuras del sistema, incluidas las estaciones de recarga, para prevenir escuchas ilegales, robos de información por interceptación de la comunicación entre actores del sistema y evitar sabotajes o manipulaciones no autorizadas.

Es esencial asegurar que el modelo incluya medidas como el uso de tapas de seguridad para los puertos de acceso y sensores de detección de manipulación indebida en las infraestructuras de carga. El sistema también debe estar equipado con alarmas para alertar sobre intentos de sabotaje o intervenciones físicas, permitiendo una respuesta oportuna a posibles ataques mediante la restricción o bloqueo de la comunicación con otros componentes o actores.

El diagrama de la figura 6.6 ilustra la evaluación de seguridad de las infraestructuras, enfatizando la importancia de restringir el acceso a puertos y conexiones, así como el aislamiento de infraestructuras comprometidas para prevenir el acceso no autorizado al sistema.

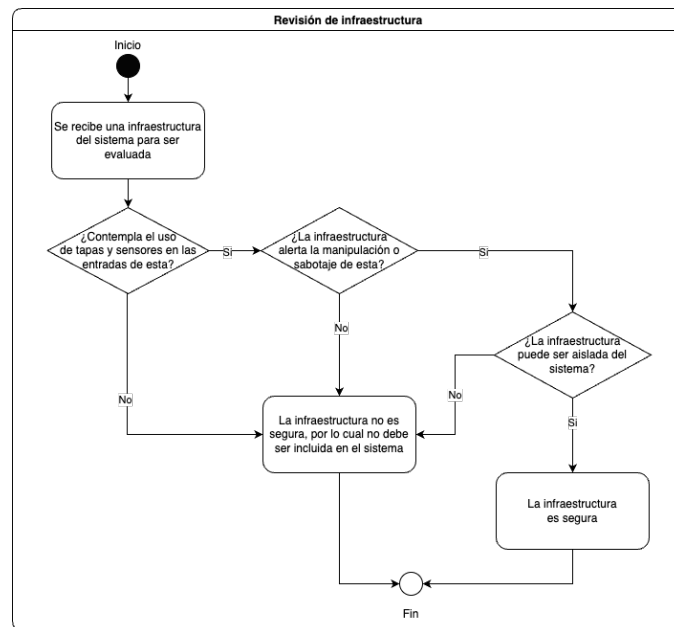


Figura 6.6. Diagrama de revisión de infraestructura.

Adicionalmente, se recomienda implementar análisis periódicos de diversos datos del sistema, como registros de carga, solicitudes, datos de facturación y mediciones de energía, entre otros. Estos análisis tienen como objetivo detectar robos de credenciales, suplantaciones de identidad, irregularidades en el proceso de carga y anomalías en las tarifas, identificando patrones sospechosos que puedan indicar un uso indebido del sistema.

La implementación de estos análisis periódicos es crucial para proteger la integridad y seguridad del sistema, detectar y prevenir ataques, y garantizar un uso adecuado de la infraestructura de recarga eléctrica, reforzando la confianza de los usuarios y asegurando un entorno seguro y confiable.

6.1.4. Perspectiva de autenticación

La autenticación es crucial, especialmente para habilitar la funcionalidad "Plug and Charge" en el sistema, que se basa en el intercambio de certificados entre el vehículo eléctrico y la estación de carga, conforme a los estándares de la ISO 15118.

Esta perspectiva se centra en la autenticación de los actores del sistema, asegurando que puedan recibir y procesar solicitudes adecuadamente. Es vital que el sistema sea capaz de rechazar cualquier solicitud que no cumpla con los requisitos de autenticación establecidos.

Un aspecto importante es la presencia de una entidad reguladora de certificados, responsable de emitirlos, verificar su validez y gestionar su caducidad.

6.1.4.1. Sistema de Certificados

De acuerdo con la ISO 15118, el sistema de recarga para vehículos eléctricos emplea el intercambio de certificados para la autenticación. Un certificado digital es un archivo firmado digitalmente por una autoridad de certificación reconocida, que vincula datos de autenticación con la entidad firmante para confirmar su identidad.

La estructura de un certificado contiene información sobre la entidad, como su clave pública y datos de identidad. La firma asegura la integridad de los datos, imposibilitando su alteración sin detección. La utilización de certificados garantiza la autenticación segura de los actores, la integridad de los documentos y el no repudio.

La criptografía asimétrica en los certificados asegura que solo el destinatario pueda leerlos, protegiendo contra ataques de tipo "Man-in-the-Middle".

Durante el proceso de recarga, se intercambian varios certificados entre los componentes del sistema, destacándose los siguientes:

- **Certificado raíz V2G:** Verifica la autenticidad de otros certificados mediante una infraestructura PKI. Su clave privada pertenece a la autoridad certificadora.
- **Certificado SECC:** Autentica el SECC con el EVCC. Deriva de los certificados raíz V2G.
- **Certificado raíz OEM:** Firma los certificados PROV OEM, validando la identidad del vehículo durante la recarga.
- **Certificado PROV OEM:** Deriva del certificado raíz OEM o puede ser firmado por un certificado raíz V2G.
- **Certificado de operador de movilidad:** Firma los certificados de contrato, representando el acuerdo entre un operador y un usuario.
- **Certificado CONT:** Acredita la existencia de un contrato con los EVSE. Deriva del certificado raíz del operador de movilidad.

- **Certificado raíz de operación privada:** Utilizado para redes privadas de recarga, almacenado en el vehículo.
- **Certificado SECC de operación privada:** Autentica un equipo de carga privado con el vehículo, derivando del certificado raíz de operación privada.

6.2. Intersecciones que cubrirá la capa en el modelo EMSA

En esta sección se detalla cómo aplicar la capa de seguridad descrita en este documento a los modelos de interoperabilidad para la recarga de vehículos eléctricos, tanto existentes como futuros, con el propósito de esclarecer su implementación.

A modo de ejemplo, se selecciona el modelo EMSA para demostrar cómo se integra la capa de seguridad propuesta, dado que este modelo demostró ser el más eficaz según el análisis realizado en la Tabla 4.2.

La Figura 6.7 ilustra el enfoque de la capa de seguridad, que consiste en inspeccionar sistemáticamente los puntos vulnerables del sistema, ya sean componentes, protocolos, o el tipo de información intercambiada. Esta inspección permite identificar y, en su caso, remediar vulnerabilidades identificadas, como las presentadas en la Tabla 5.4.

Las subsecciones siguientes describen el mapeo de la capa de seguridad dentro del modelo EMSA, abordando las distintas perspectivas de seguridad que este proporciona.

6.2.1. Perspectiva de actualización y segmentación

Esta perspectiva tiene como objetivo asegurar que todos los estándares, protocolos y softwares que impactan la seguridad del sistema estén actualizados y correctamente segmentados. Se aplicará principalmente en las capas de componentes y comunicación del modelo. La capa de componentes incluye los elementos del sistema y sus aplicaciones (software), mientras que la capa de comunicación abarca los protocolos utilizados para la interacción entre los componentes del sistema.

En la **capa de componentes**, esta perspectiva se implementa en casi todas las zonas y dominios, con excepción de aquellos que no involucran software, como la generación de energía y la zona de mercado, que no emplean software según se muestra en la Figura 6.8.

6.2.2. Perspectiva de información

La perspectiva de información busca asegurar la seguridad de la información intercambiada entre actores y componentes del sistema, mediante la revisión de métodos de encriptación, evitando la exposición innecesaria y aplicando la parametrización y sanitización de datos intercambiados. Se enfoca en las capas de información y negocio. La capa de información describe los datos a usar e intercambiar, mientras que la capa de Negocios ofrece una visión empresarial del intercambio de información.

En la **capa de información**, se implementa esta perspectiva en las intersecciones señaladas en la Figura 6.9, definiendo los datos que se intercambiarán.

Para la **capa de comunicación**, esta perspectiva afecta a las intersecciones de zonas y dominios que requieren de software, como se ilustra en la Figura 6.10.

En la **capa de negocio**, la perspectiva se aplica en las áreas mostradas en la Figura 6.11, reflejando la visión empresarial sobre el intercambio de información.

Es crucial definir y validar los métodos de encriptación para los intercambios de información, asegurando que estén actualizados y libres de vulnerabilidades conocidas.

CAPA DE SEGURIDAD

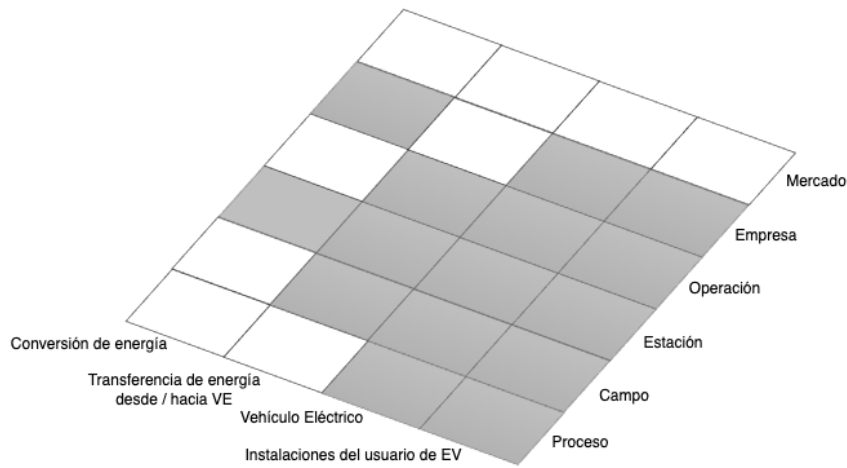


Figura 6.8. Aplicación de la perspectiva de actualización y segmentación en la capa de componentes.

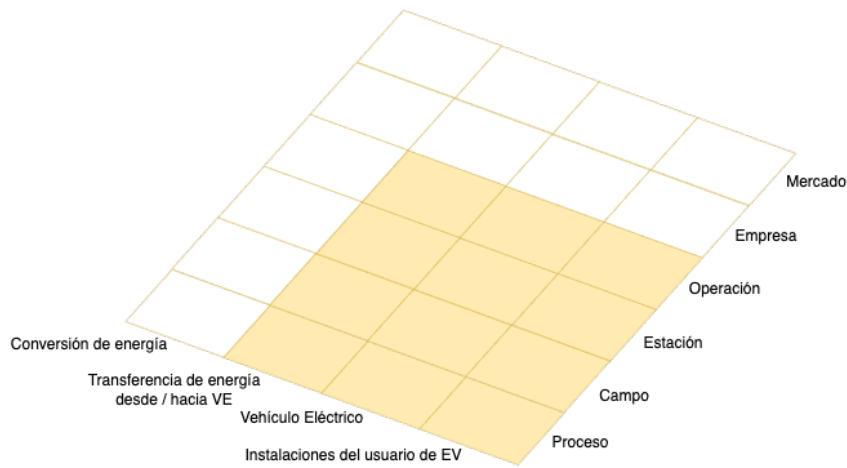


Figura 6.9. Aplicación de la perspectiva de información en la capa de información.

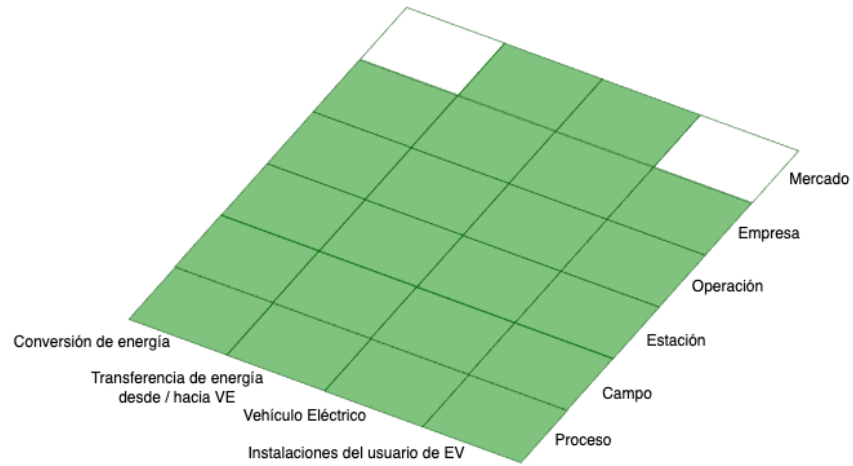


Figura 6.10. Aplicación de la perspectiva de información en la capa de comunicación.

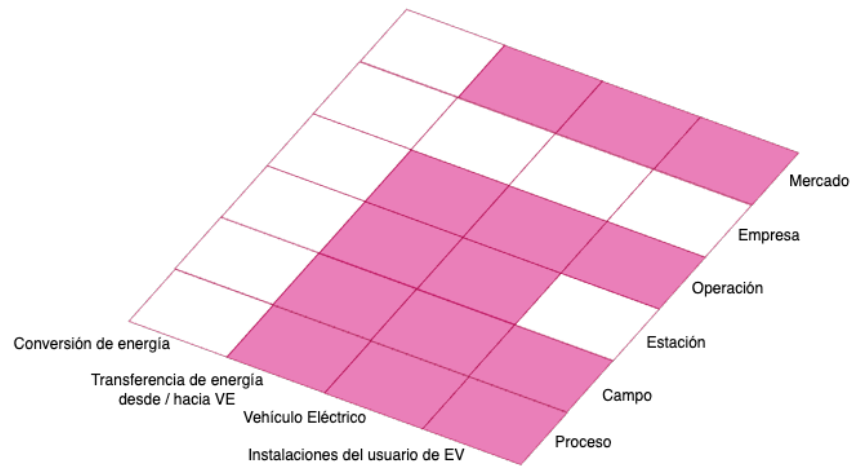


Figura 6.11. Aplicación de la perspectiva de información en la capa de negocio.

6.2.3. Perspectiva de infraestructura

Como se ha destacado anteriormente, la perspectiva de infraestructura se enfoca en proteger la seguridad del sistema mediante la evaluación de sus infraestructuras.

Consecuentemente, esta perspectiva se implementará en las capas de componentes y función dentro del modelo EMSA. La capa de componentes detalla la distribución física de los elementos del sistema, tales como equipos de potencia, dispositivos de control e infraestructura de red. Por otro lado, la capa de función se centra en describir las funciones y servicios disponibles en el sistema.

En la **capa de componentes**, esta perspectiva se aplicará en prácticamente todas las intersecciones de zonas y dominios, con la excepción de aquellas secciones que no incluyen una descripción de la distribución física de componentes, como la conversión de energía y la zona de mercado. Esta implementación se ilustra en la Figura 6.12.

Para la **capa de función**, la perspectiva de infraestructura se implementará en las intersecciones de zonas y dominios específicos, como se muestra en la Figura 6.13. Esta selección se debe a que dichas intersecciones detallan las funcionalidades relevantes para esta perspectiva, resaltando las áreas críticas en las que se debe prestar especial atención para proteger la infraestructura y garantizar la seguridad del sistema.

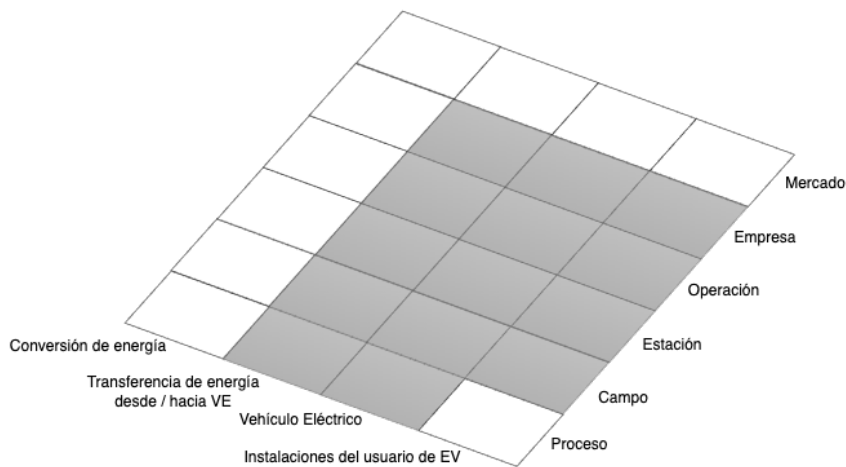


Figura 6.12. Aplicación de la perspectiva de infraestructura en la capa de componentes.

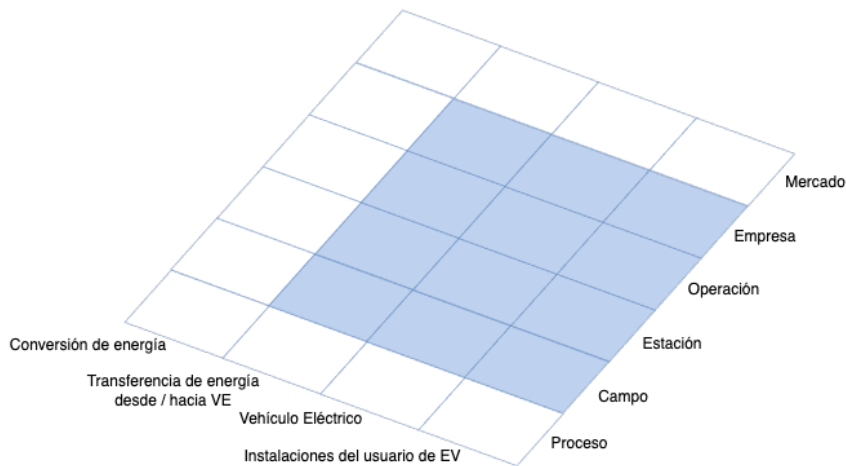


Figura 6.13. Aplicación de la perspectiva de infraestructura en la capa de función.

6.2.4. Perspectiva de autenticación

Esta perspectiva es crucial en contextos donde el sistema incorpora la funcionalidad de carga "Plug and Charge". Este método requiere el intercambio de certificados entre los componentes del sistema para validar y procesar correctamente las solicitudes de carga, así como para rechazar aquellas que no cumplan con los requisitos de autenticación establecidos.

Se implementará esta perspectiva en las capas de información, función y negocio dentro del modelo EMSA, adaptándose a las necesidades específicas de cada una:

- **Capa de información:** Aquí se describe la información intercambiada entre los componentes del sistema, incluyendo los certificados que validan la autenticación de los actores o componentes. La aplicación de esta perspectiva en esta capa se visualiza en las intersecciones de zonas y dominios específicos, mostrados en la Figura 6.14.

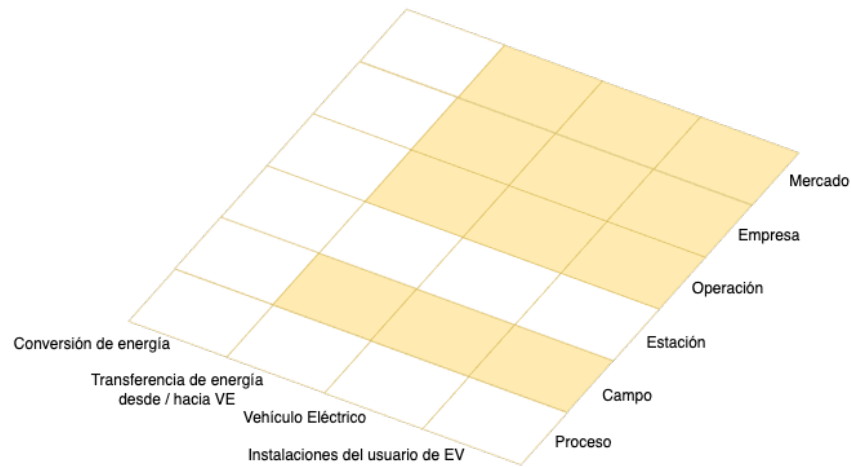


Figura 6.14. Aplicación de la perspectiva de autenticación en la capa de información.

- **Capa de función:** Detalla las funciones del sistema, donde la autenticación de los actores es esencial. La perspectiva se aplica en las intersecciones destacadas en la Figura 6.15, asegurando la integridad y seguridad de las operaciones.

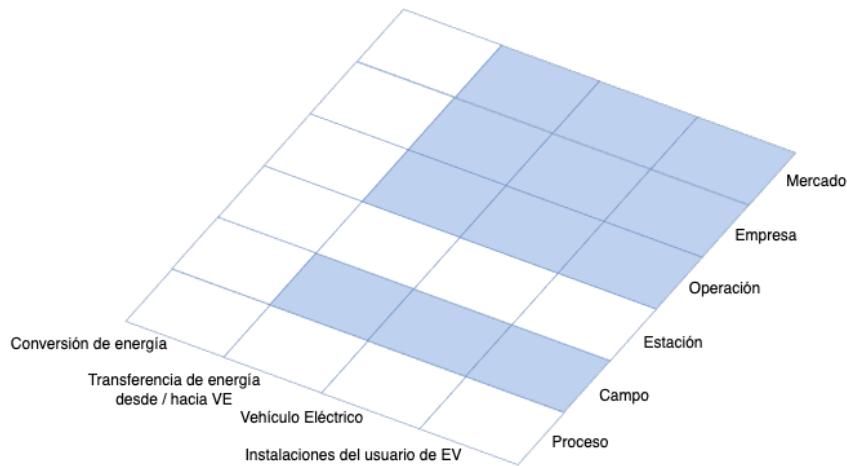


Figura 6.15. Aplicación de la perspectiva de autenticación en la capa de función.

- **Capa de negocio:** Presenta una visión empresarial sobre el intercambio de información, incluido el manejo de certificados. Esta capa establece cuáles certificados se utilizarán y qué actores tendrán acceso a ellos, como se detalla en la Figura 6.16.

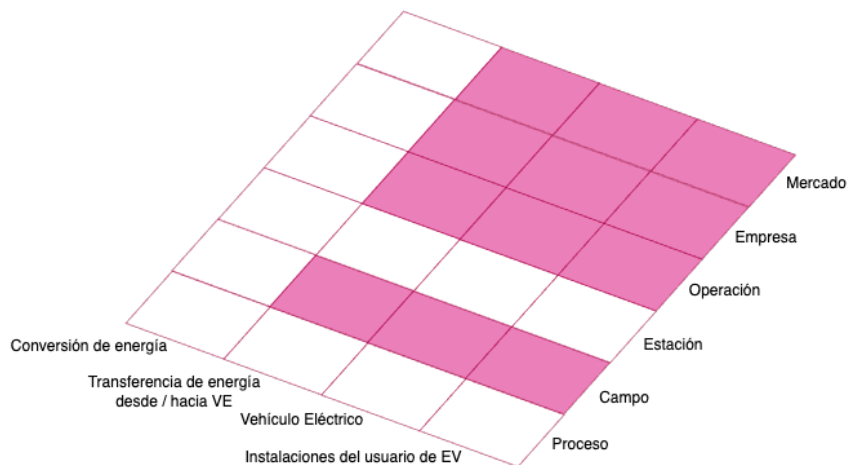


Figura 6.16. Aplicación de la perspectiva de autenticación en la capa de negocio.

La aplicación cuidadosa de esta perspectiva garantiza un sistema robusto y seguro, donde la autenticación juega un papel fundamental en la protección de las transacciones y la integridad de los datos intercambiados.

6.3. Testeo de la capa de seguridad

En esta sección, se procederá a testear la capa de seguridad introducida previamente en el contexto del “Modelo de interoperabilidad para la electromovilidad” propuesto en [31]. Este modelo, de estructura tridimensional similar al SGAM, incorpora capas, dominios y zonas, y fue desarrollado por la Comisión Nacional de Energía (CNE) con el objetivo de contribuir al desarrollo del mercado para facilitar una transición energética sostenible, apoyada en un marco regulatorio que acompaña el avance tecnológico en Chile.

6.3.1. Perspectiva de actualización y segmentación

La evaluación de la perspectiva de actualización y segmentación en el modelo se centrará en revisar los protocolos y estándares más relevantes que se utilizan. Dado que el modelo no especifica explícitamente el uso de softwares particulares, esta sección no aplicará para estos elementos.

Protocolo o Estándar	Estado de actualización
OCCP 1.6	Requiere actualización. Existen versionamientos superiores
ISO 15118: 2019	Requiere actualización. Existen actualizaciones de distintos capítulos del estándar

Tabla 6.2. Evaluación de actualización de protocolos y estándares en el modelo de interoperabilidad para la electromovilidad.

La Tabla 6.2 muestra los resultados de la evaluación, identificando que el modelo emplea versiones que podrían estar desactualizadas de algunos estándares, lo cual compromete la seguridad del sistema. Sin embargo, el modelo demuestra una adecuada segmentación de estándares y protocolos, empleando dos capas distintas para su organización según los dominios específicos de cada uno.

Para asegurar la implementación segura de este modelo, es imprescindible llevar a cabo una revisión de las versiones más recientes de los estándares y protocolos utilizados, verificar su compatibilidad con otros elementos del sistema, y proceder con las actualizaciones pertinentes.

6.3.2. Perspectiva de información

La revisión de la perspectiva de información en el modelo propuesto por la Comisión Nacional de Energía revela carencias significativas en aspectos cruciales para la seguridad del sistema. Se identifica que el modelo no especifica los métodos de encriptación para el intercambio seguro de información entre los actores del sistema. Además, falta claridad en la delimitación de la información esencial para el intercambio, evitando así la exposición innecesaria de datos sensibles.

Esta ausencia de especificaciones sugiere que el modelo, en su estado actual, no garantiza una seguridad integral. Para remediar estas deficiencias, es imperativo incorporar en el modelo los detalles sobre la información a intercambiar y los mecanismos de encriptación a emplear, o definir qué protocolos o estándares se encargarán de asegurar la confidencialidad y la integridad de la comunicación.

6.3.3. Perspectiva de infraestructura

La evaluación del modelo en cuanto a la perspectiva de infraestructura destaca la falta de medidas de protección física, tales como el uso de tapas para los puertos y conexiones, así como un sistema de alertas ante intentos de sabotaje o intervenciones no autorizadas. La ausencia de estas medidas preventivas deja al modelo vulnerable a ataques físicos, sin posibilidad de aislar infraestructuras comprometidas para proteger el sistema en su conjunto.

Para subsanar estas vulnerabilidades, es necesario implementar especificaciones que exijan la inclusión de estas medidas de protección en las estaciones de carga, así como desarrollar un protocolo dentro del modelo que detalle la respuesta ante intentos de sabotaje, garantizando así la seguridad de la infraestructura y, por extensión, del sistema completo.

6.3.4. Perspectiva de autenticación

Respecto a la perspectiva de autenticación, el modelo satisfactoriamente integra el uso de certificados digitales y otros métodos de autenticación que son cruciales para implementar la funcionalidad de carga “Plug and Charge”. Esto asegura que el sistema pueda procesar adecuadamente las solicitudes de carga, permitiendo el rechazo de aquellas que no cumplan con los requisitos de autenticación establecidos.

En este sentido, el modelo se considera seguro bajo la óptica de la autenticación, cumpliendo con los requisitos necesarios para garantizar un intercambio de información autenticado y seguro entre los actores involucrados en el proceso de carga de vehículos eléctricos.

6.4. Resultados obtenidos

En este segmento se presentan los resultados derivados de un análisis minucioso de las vulnerabilidades listadas en la Tabla 5.4, enfocándonos en su impacto y las estrategias de mitigación. El aporte fundamental de esta investigación radica en la formulación de una capa de seguridad comprehensiva, diseñada específicamente para la detección, alerta y corrección de dichas vulnerabilidades. Este enfoque promueve una implementación más robusta y segura de los sistemas de recarga de vehículos eléctricos.

A continuación, se exponen varias fichas técnicas que catalogan y detallan cada una de las vulnerabilidades identificadas a lo largo de este estudio. Estas fichas no solo explican el carácter y el origen de cada vulnerabilidad, sino que también presentan las medidas preventivas y correctivas propuestas por la capa de seguridad diseñada en la presente tesis para contrarrestarlas.

Cada ficha se organiza siguiendo una estructura estandarizada, la cual incluye información clave sobre la vulnerabilidad en cuestión, su contexto y las recomendaciones prácticas para su manejo. Dicha estructura facilita el entendimiento completo del desafío que representa cada vulnerabilidad, así como de las acciones sugeridas para su mitigación.

6.5. Resultados obtenidos al aplicar las distintas perspectivas

Para cada vulnerabilidad identificada en el estudio, se desarrolló una ficha técnica detallada, la cual permite una comprensión exhaustiva de la problemática y las estrategias de mitigación propuestas. La estructura de cada ficha es la siguiente:

- **N° de vulnerabilidad:** Identificador único para cada vulnerabilidad, facilitando su referencia y análisis.
- **¿Qué falla de seguridad causa la vulnerabilidad del sistema?:** Detalle de la falla de seguridad específica que introduce la vulnerabi-

lidad en el sistema, proporcionando una comprensión clara de la raíz del problema.

- **Acción:** Descripción de las acciones sugeridas por la capa de seguridad para detectar y/o mitigar la vulnerabilidad, contribuyendo a la mejora de la integridad del sistema.
- **Alerta(s):** Especificación de las alertas emitidas por la capa de seguridad al detectar la vulnerabilidad, incluyendo el tipo de alerta y su relación con la vulnerabilidad específica.
- **Accion(es) a tomar post-alerta:** Medidas recomendadas para implementar una vez generada la alerta, con el fin de mitigar el impacto de la vulnerabilidad.
- **Capa(s) afectada(s) (en el modelo EMSA):** Identificación de las capas del modelo EMSA impactadas por la vulnerabilidad, ofreciendo una visión clara de su alcance.
- **Dominio(s) afectado(s):** Indicación de los dominios del modelo EMSA comprometidos por la vulnerabilidad.
- **Zona(s) afectada(s):** Identificación de las zonas dentro del modelo EMSA susceptibles a la vulnerabilidad.
- **Perspectiva (de seguridad) relacionada:** Vinculación de la vulnerabilidad con una perspectiva específica de la capa de seguridad, destacando la relevancia de ciertas vulnerabilidades para aspectos concretos de la seguridad.
- **Actores:** Enumeración de los actores relacionados con la vulnerabilidad, ya sea como causantes, afectados, o encargados de su manejo.
- **¿En qué capa del modelo EMSA se debe trabajar la propuesta de prevención?:** Justificación de las capas del modelo EMSA donde se deben aplicar medidas de prevención, explicando la relevancia de dichas capas para la mitigación de la vulnerabilidad.
- **¿El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?:** Análisis de si la legislación y regulaciones vigentes en Chile consideran la prevención de la vulnerabilidad y, en caso afirmativo, descripción de cómo se aborda.

- **Antigüedad (de la vulnerabilidad):** Tiempo durante el cual la vulnerabilidad ha sido reconocida y documentada, aportando contexto sobre su permanencia y actualidad.

De esta manera, cada ficha técnica aporta un marco detallado para la discusión y manejo de las vulnerabilidades, integrando de manera efectiva las recomendaciones de seguridad propuestas en este estudio.

N° de vulnerabilidad	1
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	La ausencia de sensores para detectar manipulaciones, intervenciones o conexiones no autorizadas en los puntos de carga, así como la falta de análisis periódico de los registros de carga.
Acción	Al incorporar un nuevo punto de carga sin sensores que alerten sobre manipulaciones o conexiones no autorizadas, como la apertura indebida de tapas o la detección de dispositivos ilegítimos, la perspectiva de infraestructura identificará este punto como un riesgo. Además, se asegura la revisión periódica de los registros de carga para identificar discrepancias entre la energía suministrada por el punto de carga y la recibida por el vehículo eléctrico.
Alerta(s)	1- Manipulación no autorizada; 2- Apertura no autorizada de tapa(s); 3- Exceso de tiempo de conexión en periodos irregulares; 4- Discrepancia entre la energía suministrada y la recibida por el vehículo.
Acción(es) a tomar post alerta	Proceder con la desconexión y aislamiento del punto de carga hasta verificar y/o restaurar su integridad.
Capa(s) afectada(s)	Componentes y función
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE e instalaciones para usuarios de VE
Zona(s) afectada(s)	Campo, estación y empresa
Perspectiva relacionada	Infraestructura
Actores	1- Usuario del VE: afectado por el robo de energía; 2- Punto de carga: manipulado para sustraer energía; 3- VE del atacante: beneficiario del robo de energía.
¿En qué capa(s) EMSA se debe trabajar la propuesta de prevención?	Componentes
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2012

Tabla 6.3. Ficha vulnerabilidad N°1.

N° de vulnerabilidad	2
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	La ausencia de un método de encriptación asimétrico seguro para el intercambio de información entre el punto de carga y el vehículo eléctrico, sumado a la falta de sensores que alerten sobre manipulaciones no autorizadas en el punto de carga.
Acción	Si un intercambio de información entre el punto de carga y un vehículo eléctrico no implementa un método de encriptación robusto, esto expone al sistema a riesgos de integridad y confidencialidad de la información. Será esencial reemplazar o implementar un método de encriptación asimétrico para asegurar que solo el destinatario pueda descifrar la información enviada. Además, la incorporación de puntos de carga sin sensores para detectar manipulaciones no autorizadas será señalada por la perspectiva de infraestructura como un riesgo significativo para la seguridad del sistema.
Alerta(s)	1- Manipulación no autorizada; 2- Apertura no autorizada de tapa(s); 3- Necesidad de reemplazar o implementar un método de encriptación asimétrico.
Acción(es) a tomar post alerta	1- Solicitar la desconexión y aislamiento del punto de carga para verificar o restaurar su integridad; 2- Implementar un método de encriptación asimétrico entre el vehículo eléctrico y el punto de carga.
Capa(s) afectada(s)	Información y negocio
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el vehículo eléctrico y vehículo eléctrico.
Zona(s) afectada(s)	Campo y empresa
Perspectiva relacionada	Información e infraestructura
Actores	1- Vehículo eléctrico: expuesto a la divulgación de su número de identificación; 2- Atacante: adquiere el número de identificación del vehículo, lo que podría utilizar para suplantar su identidad.
¿En qué capa(s) EMSA se debe trabajar la propuesta de prevención?	Comunicación
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2013

Tabla 6.4. Ficha vulnerabilidad N°2.

N° de vulnerabilidad	3
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	El sistema no cuenta con un sistema de autenticación que impida el robo de credenciales, que incluya prácticas de autenticación sólidas, controles de acceso adecuados y la revocación de credenciales robadas o no válidas.
Acción	Al utilizar una credencial de un VE autorizado (robada), el sistema de autenticación no autorizará el uso del sistema de carga. Ello, debido a que el certificado robado fue cifrado a través de un proceso de autenticación de desafío-respuesta, requiriendo una respuesta diferente con cada intento. Así, el certificado se encuentra cifrado o hashado siendo el receptor de este el único que puede leer y validarlo. De igual manera, si se agrega un nuevo punto de carga al sistema y este no posea sensores que alerten la manipulación y/o intervención no autorizadas a este, tales como la apertura de tapas y skimming, la perspectiva de infraestructura alertará que es arriesgado incluir a este punto de carga dentro del sistema. Además, esta última perspectiva asegura el análisis periódico de los registros de carga con la finalidad de identificar irregularidades en los registros (ej: clonación)
Alerta(s)	1- Detección de suplantación de identidad 2- Manipulación no autorizada 3- Apertura de tapa(s) no autorizada
Acción(es) a tomar post alerta	1- Denegar acceso al sistema a las credenciales utilizadas hasta regular su situación 2- Solicitar desconexión y aislamiento hasta verificar y/o reparar la integridad de la estación de carga
Capa(s) afectada(s)	Información, función y negocio
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE, VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Campo y empresa
Perspectiva relacionada	Infraestructura y autenticación
Actores	1- Usuario del VE: le cobran en su cuenta una carga realizada por un suplantador 2- Atacante: obtiene energía suplantando la identidad del usuario
¿En qué capa(s) EMSA se debe trabajar la propuesta de prevención?	Negocio y comunicación
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	Sí, contempla el uso de la norma ISO 15118 para carga con configuración FF ¹
Antigüedad	2013

Tabla 6.5. Ficha vulnerabilidad N°3.

¹Configuración FF: Conector con cable que proviene de un sistema de alimentación específico de vehículo eléctrico, con modo de carga 4, que suministra energía eléctrica en corriente continua hacia la entrada de un vehículo eléctrico, estableciendo además las funciones de comunicación y seguridad entre el sistema de alimentación específico de vehículo eléctrico y vehículo eléctrico

N° de vulnerabilidad	4
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No existen sensores que detecten la manipulación, intervención o conexión no autorizada en la estación de carga en lectores NFC
Acción	Si se agrega un punto de carga al sistema y este no tiene sensores que alerten su manipulación, intervención o conexión no autorizada (ej: skimmers), la perspectiva de infraestructura alertará que es riesgoso incluir a este punto de carga dentro del sistema. Además, la perspectiva asegura un análisis periódico de los registros de carga con la finalidad de identificar irregularidades como diferencias entre la energía entregada por un punto de carga y la recibida por él.
Alerta(s)	1- Manipulación no autorizada
Acción(es) a tomar post alerta	Solicitar desconexión y aislamiento hasta verificar y/o reparar la integridad de la estación de carga
Capa(s) afectada(s)	Componentes y función
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Campo, estación y empresa
Perspectiva relacionada	Infraestructura
Actores	1- Usuario del VE: le roban datos de su tarjeta RFID
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Componentes
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2017

Tabla 6.6. Ficha vulnerabilidad N°4.

N° de vulnerabilidad	5
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	El sistema no cuenta con un mecanismo de autenticación que impida el robo de credenciales, que incluya prácticas de autenticación sólidas, controles de acceso adecuados, la implementación de un mecanismo de sincronización horaria y/o la revocación de credenciales robadas o no válidas
Acción	Así como se aprecia en la vulnerabilidad 3, al utilizar una credencial de un VE autorizado robada, el sistema de autenticación no autorizará el uso del sistema de carga, debido a que el certificado robado fue cifrado a través de un proceso de autenticación de desafío-respuesta. De igual manera, la perspectiva de infraestructura asegura el análisis periódico de los registros de carga con la finalidad de identificar irregularidades en los registros, tales como la clonación de credenciales. Por último, la capa contempla el uso de la implementación de un mecanismo de sincronización horaria en el sistema.
Alerta(s)	1- Detección de suplantación de identidad 2- Irregularidad detectadas en el análisis de registros de carga
Acción(es) a tomar post alerta	Denegar acceso al sistema a las credenciales utilizadas hasta regular su situación.
Capa(s) afectada(s)	Información, función y negocio
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE y VE.
Zona(s) afectada(s)	Campo y empresa
Perspectiva relacionada	Infraestructura y autenticación
Actores	1- Usuario del VE: le es cobrado en su cuenta una carga realizada por un suplantador 2- Atacante: obtiene energía suplantando la identidad del usuario
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Negocio y comunicación
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	Sí, contempla el uso de la norma ISO 15118 para carga con configuración FF
Antigüedad	2014

Tabla 6.7. Ficha vulnerabilidad N°5.

N° de vulnerabilidad	6
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No se cuenta con un análisis periódico que identifique irregularidades en los registros de carga
Acción	Cuando se tiene un VE y un punto de carga coludidos emitiendo información adulterada sobre la medición de la energía utilizada en el proceso de carga la perspectiva alertará estas irregularidades a través del análisis de los registros de carga identificando que el distribuidor de energía ha enviado más energía que la informada en esta carga o se hizo uso de tarifas que no corresponden.
Alerta(s)	1- Irregularidad detectada en el análisis de registros de carga
Acción(es) a tomar post alerta	Solicitar desconexión y aislamiento hasta verificar y/o reparar la integridad de la estación de carga
Capa(s) afectada(s)	Información
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Campo, estación y empresa
Perspectiva relacionada	Infraestructura
Actores	1- Distribuidor de energía: se le informa que es menor la cantidad o la tarifa de energía utilizada 2- VE atacante: recibe más energía de que la pagó
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Comunicación
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2014

Tabla 6.8. Ficha vulnerabilidad N°6.

N° de vulnerabilidad	7
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No existen sensores que detecten la manipulación, intervención o conexión no autorizada en la estación de carga en elementos de entrada y salida de información ni energía correspondientemente, ni un análisis periódico de los registros de carga.
Acción	Al añadir un punto de carga al sistema que no posee sensores para alertar la manipulación, intervención o conexión no autorizada a este la perspectiva de infraestructura alertará que incluir a este punto dentro del sistema traerá consigo ciertos riesgos. También, la perspectiva asegura un análisis periódico de los registros de carga con la finalidad de identificar irregularidades en los mismos, tales como diferencias entre la energía entregada por un punto de carga y la recibida por él
Alerta(s)	1- Llegan conexiones de múltiples direcciones IP 2- Irregularidad detectada en el análisis de registros de carga 3- Manipulación no autorizada 4- Apertura de tapa(s) no autorizada
Acción(es) a tomar post alerta	1- Rechazar mensajes del punto de carga 2- Inhabilitar la estación de carga hasta regularizar su situación
Capa(s) afectada(s)	Información, función y negocio
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Campo, operación y empresa
Perspectiva relacionada	Infraestructura
Actores	1- Punto de carga: se vuelve inaccesible para los usuarios
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Componentes
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	Sí, contempla una sincronización horaria entre los componentes y actores del sistema, por lo que al añadir fechas en los mensajes no importará que estos lleguen desfasados
Antigüedad	2013

Tabla 6.9. Ficha vulnerabilidad N°7.

N° de vulnerabilidad	8
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No existen sensores que detecten la manipulación, intervención o conexión no autorizada en la estación de carga en elementos de entrada y salida de información
Acción	Tal como en la vulnerabilidad 1, al agregar un punto de carga al sistema y este no tiene sensores que alerten la manipulación, intervención o conexión no autorizada, tal como la apertura de tapas, skimming y la detección de dispositivos ilegales en elementos de salida de energía en periodos irregulares (cuando el punto de carga está en desuso, por ejemplo), la perspectiva de infraestructura alertará que es riesgoso conectar a este punto de carga al sistema.
Alerta(s)	1- Manipulación no autorizada 2- Apertura de tapa(s) no autorizada
Acción(es) a tomar post alerta	Solicitar desconexión y aislamiento hasta verificar y/o reparar la integridad de la estación de carga
Capa(s) afectada(s)	Componentes y función
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Campo, estación y empresa
Perspectiva relacionada	Infraestructura
Actores	1- Punto de carga: es suplantada su identidad
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Componentes
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2018

Tabla 6.10. Ficha vulnerabilidad N°8.

N° de vulnerabilidad	9
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No existen sensores que detecten la manipulación, intervención o conexión no autorizada en la estación de carga en elementos de entrada y salida de información
Acción	Al incorporar a un punto de carga al sistema y este no tiene sensores que alerten la manipulación, intervención o conexión no autorizada a este, tal como skimming, la perspectiva de infraestructura alertará que es riesgoso conectar a este punto de carga al sistema. Por otro lado, la perspectiva asegura un análisis periódico de los registros de carga con la finalidad de identificar irregularidades en los mismos, tales como interrupciones
Alerta(s)	1- Manipulación no autorizada 2- Apertura de tapa(s) no autorizada 3- Interrupciones irregulares de forma periódica
Acción(es) a tomar post alerta	Solicitar desconexión y aislamiento hasta verificar y/o reparar la integridad de la estación de carga
Capa(s) afectada(s)	Información y función
Dominio(s) afectado(s)	Conversión de energía y transferencia de energía desde/hacia VE
Zona(s) afectada(s)	Campo, estación, operación y mercado
Perspectiva relacionada	Infraestructura
Actores	1- Usuario del VE: no consigue realizar su carga de forma exitosa 2- Punto de carga: se vuelve inaccesible para los usuarios
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Comunicación
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad	No
Antigüedad	2018

Tabla 6.11. Ficha vulnerabilidad N°9.

N° de vulnerabilidad	10
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No se cuenta con un análisis periódico que identifique irregularidades en los registros de carga
Acción	La irregularidad del uso de credenciales estáticas utilizadas en la fase de configuración del protocolo robadas por un empleado deshonesto será detectada por el análisis de registros de carga impuesto en la perspectiva de infraestructura
Alerta(s)	Detección de uso de credenciales de forma irregular
Acción(es) a tomar post alerta	Denegar acceso al sistema a las credenciales utilizadas hasta regular su situación
Capa(s) afectada(s)	Información y negocio
Dominio(s) afectado(s)	Conversión de energía y transferencia de energía desde/hacia VE
Zona(s) afectada(s)	Campo, estación y empresa
Perspectiva relacionada	Infraestructura
Actores	1- Atacantes: obtienen acceso a la información intercambiada y pueden realizar suplantación de identidad: 2- Proveedor de servicios de movilidad eléctrica: su proceso de facturación se ve vulnerado
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Comunicación
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2014

Tabla 6.12. Ficha vulnerabilidad N°10.

CAPA DE SEGURIDAD

N° de vulnerabilidad	11
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No se cuenta con un método de encriptación asimétrico adecuado para el intercambio de información entre diversos subsistemas con el proveedor de servicios de movilidad eléctrica
Acción	Cuando se agrega un nuevo intercambio de información entre diversos subsistemas y el proveedor de servicios de movilidad eléctrica, y este carece de la implementación de un método de encriptación adecuado para transmitir la información de manera íntegra y confidencial debido a la ausencia de un método de encriptación o a la obsolescencia del método utilizado, la perspectiva de información alertará que incluir este intercambio en el sistema presentará riesgos y será necesario reemplazar o agregar un método de encriptación asimétrico. En este método de encriptación, los participantes deben tener la llave pública del receptor para encriptar la información y este último tenga su llave privada para poder descryptar, de esta forma se asegura que no se podrá leer ni modificar la información enviada.
Alerta(s)	1- No cuenta con la aplicación de un método de encriptación adecuado para enviar la información encriptada de forma segura
Acción(es) a tomar post alerta	Agregar o reemplazar el método de encriptación asimétrico utilizado en el intercambio de información entre diversos subsistemas y el proveedor de servicios de movilidad eléctrica
Capa(s) afectada(s)	Información y función
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Campo, estación, operación y mercado
Perspectiva relacionada	Información
Actores	1- Usuario del VE: su proceso de facturación se ve afectado por los ataques realizados 2- Atacante: obtienen acceso al sistema permitiéndoles alterar datos en tránsito
¿En qué capa(s) EMSA se debe trabajar la propuesta de prevención?	Comunicación
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2014

Tabla 6.13. Ficha vulnerabilidad N°11.

N° de vulnerabilidad	12
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	Se expone información no relevante en los intercambios de datos entre el punto de carga y su operador
Acción	Si un operador de estaciones de carga puede obtener datos intercambiados entre un punto de carga y un VE, tales como los mencionados en la vulnerabilidad, sin que sean esenciales para la operación del sistema, significa que se esta realizando un intercambio de información no relevante entre el punto de carga y su operador. Ello será detectado y alertado por la perspectiva de información, bloqueando su ejecución.
Alerta(s)	1- Se está realizando intercambio de información no necesaria
Acción(es) a tomar post alerta	Remover la información no relevante en el intercambio entre el punto de carga y su operador
Capa(s) afectada(s)	Información y función
Dominio(s) afectado(s)	VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Campo, estación y empresa
Perspectiva relacionada	Información
Actores	1- VE: su id de contrato es expuesto 2- Atacante: obtiene el id del contrato del usuario, el cual podrá utilizar para suplantar identidad
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Información
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2014

Tabla 6.14. Ficha vulnerabilidad N°12.

N° de vulnerabilidad	13
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No se cuenta con un método de encriptación asimétrico adecuado para el intercambio de información diversos subsistemas y el proveedor de servicios de movilidad eléctrica
Acción	Si empleados deshonestos, ya sean del distribuidor de energía o del proveedor de servicios de movilidad eléctrica, generan planes de carga falsos o manipulan el proceso de carga, la irregularidad generada por estos será detectado y alertado por los análisis de los registros de carga impuesto por la perspectiva de
Alerta(s)	1- Detección de irregularidades en los procesos de carga 2- detección de irregularidades en el proceso de facturación
Acción(es) a tomar post alerta	Agregar o reemplazar el método de encriptación asimétrico utilizado en el intercambio de información sea seguro
Capa(s) afectada(s)	Información y función
Dominio(s) afectado(s)	Conversión de energía y transferencia de energía desde/hacia VE
Zona(s) afectada(s)	Campo, estación y empresa
Perspectiva relacionada	Infraestructura
Actores	1- Usuario del VE: su proceso de facturación se ve afectado por los ataques realizados 2- Atacante: obtienen acceso al sistema permitiéndoles alterar datos en transito
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Comunicación
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad	No
Antigüedad	2014

Tabla 6.15. Ficha vulnerabilidad N°13.

N° de vulnerabilidad	14
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	El uso de dispositivos, protocolos y/o aplicaciones desactualizadas dentro del sistema
Acción	Cuando se aplique la capa de seguridad o se quiera agregar un nuevo dispositivo, protocolo y/o software, la perspectiva de actualización detectará si estos se encuentran desactualizados, lo cual indica alto riesgo de conexión o mantención dentro del sistema
Alerta(s)	1- El dispositivo, protocolo o software se encuentra desactualizado
Acción(es) a tomar post alerta	Se abre debate entre los actores pertinentes sobre la realización de la actualización de versión
Capa(s) afectada(s)	Componentes y comunicación
Dominio(s) afectado(s)	Conversión de energía, transferencia de energía desde/hacia el VE, VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Campo, estación y operación
Perspectiva relacionada	Actualización
Actores	Pueden ser afectados múltiples actores
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Componentes y comunicación
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad	No
Antigüedad	2021

Tabla 6.16. Ficha vulnerabilidad N°14.

CAPA DE SEGURIDAD

N° de vulnerabilidad	15
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	El uso de dispositivos, protocolos y/o aplicaciones desactualizadas dentro del sistema
Acción	Tal como en la vulnerabilidad 14, cuando se aplique la capa de seguridad o se quiera agregar un nuevo dispositivos, protocolos y/o software la perspectiva de actualización detectará estos se encuentran desactualizados, lo cual presentaría riesgos para el sistema al añadir o mantener este en el sistema de
Alerta(s)	1- El dispositivo, protocolo o software se encuentra desactualizado
Acción(es) a tomar post alerta	Se abre debate entre los actores pertinentes sobre la realización de la actualización de versión
Capa(s) afectada(s)	Componentes y comunicación
Dominio(s) afectado(s)	Conversión de energía y transferencia de energía desde/hacia VE
Zona(s) afectada(s)	Campo, operación y empresa
Perspectiva relacionada	Actualización
Actores	Pueden ser afectados múltiples actores
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Componentes y comunicación
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2021

Tabla 6.17. Ficha vulnerabilidad N°15.

N° de vulnerabilidad	16
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No se cuenta con la parametrización, revisión ni sanitización de información a intercambiar entre los actores
Acción	Al agregar un nuevo dato de entrada controlable por el usuario al sistema, para este caso en ciertas aplicaciones web, la perspectiva de información debe verificar que este cuente con la parametrización, revisión y sanitización de los datos recibidos por los puntos de acceso
Alerta(s)	1- No cuenta con la parametrización, revisión y sanitización de un dato de entrada controlable por el usuario
Acción(es) a tomar post alerta	Se agrega la parametrización, revisión y/o sanitización necesaria para el dato de entrada controlable por el usuario
Capa(s) afectada(s)	Información y negocio
Dominio(s) afectado(s)	VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Campo, estación, operación y empresa
Perspectiva relacionada	Información
Actores	1- Punto de carga: se logra secuestrar la sesión de la cuenta de un usuario objetivo, modificar la cuenta y los ajustes/configuraciones 2- Atacante: obtienen acceso al sistema permitiéndoles alterar datos en tránsito
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Información
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2021

Tabla 6.18. Ficha vulnerabilidad N°16.

CAPA DE SEGURIDAD

N° de vulnerabilidad	17
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No se cuenta con la parametrización, revisión ni sanitización de información a intercambiar entre los actores
Acción	Al igual que en la vulnerabilidad 16, cuando se agregue un nuevo dato de entrada controlable por el usuario al sistema, para este caso en ciertas aplicaciones web, la perspectiva de información debe verificar que este cuente con la parametrización, revisión y sanitización de los datos ingresados
Alerta(s)	1- No cuenta con la parametrización, revisión y sanitización de un dato de entrada controlable por el usuario
Acción(es) a tomar post alerta	Se agrega la parametrización, revisión y/o sanitización necesaria para el dato de entrada controlable por el usuario
Capa(s) afectada(s)	Información
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE, VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Campo, estación, operación y empresa
Perspectiva relacionada	Información
Actores	1- Operador de punto de carga: su base de datos es vulnerada 2- Atacante: obtiene acceso privilegiado a la base de datos del operador de la estación de carga, de esta manera logrará realizar acciones maliciosas en el sistema
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Información
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad	No
Antigüedad	2021

Tabla 6.19. Ficha vulnerabilidad N°17.

N° de vulnerabilidad	18
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	El sistema no cuenta con un sistema de autenticación que impida el robo de credenciales, que incluya prácticas de autenticación sólidas, controles de acceso adecuados y la revocación de credenciales robadas o no válidas
Acción	Cuando se aplique la capa de seguridad o se requiera de un nuevo sistema de autenticación la perspectiva de autenticación debe evaluar que este haga uso del sistema de certificados, garantizando la autenticación de los actores, dado que la encriptación asimétrica de punto a punto empleada en el certificado permite asegurar que este solo puede ser leído por su destinatario, es decir, se detectaría que los puntos de carga no tienen los certificados necesarios
Alerta(s)	1- Detección de suplantación de identidad
Acción(es) a tomar post alerta	Denegar acceso al sistema a las credenciales utilizadas hasta regular su situación
Capa(s) afectada(s)	Información
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE, VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Campo, estación, operación y empresa
Perspectiva relacionada	Autenticación
Actores	1- Punto de carga: revela información confidencial 2- Atacante: obtiene información confidencial sin tener la autorización necesaria
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Negocio y comunicación
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	Sí, contempla el uso de la norma ISO 15118 para carga con configuración FF
Antigüedad	2021

Tabla 6.20. Ficha vulnerabilidad N°18.

N° de vulnerabilidad	19
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No se cuenta con la parametrización, revisión ni sanitización de información a intercambiar entre los actores
Acción	De la misma manera que en la vulnerabilidad 16, cuando se agrega un nuevo dato de entrada controlable por el usuario al sistema, para este caso en ciertas aplicaciones web, la perspectiva de información debe verificar que este cuente con la parametrización, revisión y sanitización de los datos ingresados junto la validación del token CSRF correspondiente a la solicitud
Alerta(s)	1- No cuenta con la parametrización, revisión y sanitización de un dato de entrada controlable por el usuario
Acción(es) a tomar post alerta	Se agrega la parametrización, revisión y/o sanitización necesaria para el dato de entrada controlable por el usuario
Capa(s) afectada(s)	Información
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Operación
Perspectiva relacionada	Información
Actores	1- Atacante obtiene acceso a controlar todos los datos y funcionalidades del operador de la estación de carga cuando el usuario objetivo tiene privilegios, como el ser un administrador
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Información
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2021

Tabla 6.21. Ficha vulnerabilidad N°19.

N° de vulnerabilidad	20
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No se cuenta con un análisis periódico que identifique irregularidades en las solicitudes en el sistema
Acción	Si se realiza un ataque de navegación forzada el análisis periódico propuesto en la perspectiva de infraestructura detectará esta irregularidad en las solicitudes y alertará que el sistema esta sufriendo un ataque
Alerta(s)	1- Detección de navegación forzada
Acción(es) a tomar post alerta	Denegar acceso al sistema a las credenciales utilizadas hasta regular su situación
Capa(s) afectada(s)	Información y función
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE, VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Proceso, campo, estación, operación y empresa
Perspectiva relacionada	Infraestructura
Actores	1- Atacante: interacción forzada omitiendo la autenticación, lo que puede otorgar acceso al panel de configuración de administración de energía y mantenimiento
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Negocio y comunicación
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2021

Tabla 6.22. Ficha vulnerabilidad N°20.

CAPA DE SEGURIDAD

N° de vulnerabilidad	21
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No se cuenta con un análisis periódico que identifique irregularidades en las solicitudes en el sistema
Acción	Si se realiza un ataque DoS el análisis periódico propuesto en la perspectiva de infraestructura detectará esta irregularidad en las solicitudes y alertará que el sistema esta sufriendo un ataque
Alerta(s)	1- Detección de ataque DoS
Acción(es) a tomar post alerta	Denegar acceso al sistema a las los puntos de carga comprometidos
Capa(s) afectada(s)	Información, función y negocio
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE, VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Proceso, campo, estación, operación y empresa
Perspectiva relacionada	Infraestructura
Actores	1- Atacante: deniega servicio de puntos de carga
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Negocio y comunicación
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	Sí, contempla el uso de la norma ISO 15118 para carga con configuración FF
Antigüedad	2021

Tabla 6.23. Ficha vulnerabilidad N°21.

N° de vulnerabilidad	22
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	Se expone información no esencial en los intercambios de información entre actores del sistema
Acción	De la misma manera que en la vulnerabilidad 16, cuando se agrega un nuevo dato de entrada controlable por el usuario al sistema, para este caso en ciertas aplicaciones web, la perspectiva de información debe verificar que este cuente con la parametrización, revisión y sanitización de los datos ingresados junto la validación del token CSRF correspondiente a la solicitud
Alerta(s)	1- No cuenta con la parametrización, revisión y sanitización de un dato de entrada controlable por el usuario
Acción(es) a tomar post alerta	Se agrega la parametrización, revisión y/o sanitización necesaria para el dato de entrada controlable por el usuario
Capa(s) afectada(s)	Componentes, información y función
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE, VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Proceso, campo, estación, operación y empresa
Perspectiva relacionada	Información
Actores	1- Usuario del VE: su cuenta es vulnerada 2- Atacante: obtiene acceso a la cuenta del usuario
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Información
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2021

Tabla 6.24. Ficha vulnerabilidad N°22.

N° de vulnerabilidad	23
¿Qué falla de seguridad causa la vulnerabilidad del sistema?	No se cuenta con la parametrización, revisión ni sanitización de información a intercambiar entre los actores
Acción	Al agregar un nuevo dato de entrada controlable por el usuario a un firmware, como EVlink lo es en este caso, la perspectiva de información debe verificar que este cuente con la parametrización, revisión y sanitización de los datos
Alerta(s)	1- No cuenta con la parametrización, revisión y sanitización de un dato de entrada controlable por el usuario
Acción(es) a tomar post alerta	Se agrega la parametrización, revisión y/o sanitización necesaria para el dato de entrada controlable por el usuario
Capa(s) afectada(s)	Comunicación, información y negocio
Dominio(s) afectado(s)	Transferencia de energía desde/hacia el VE, VE e instalaciones de usuarios de VE
Zona(s) afectada(s)	Campo, estación, operación y empresa
Perspectiva relacionada	Información
Actores	1- Usuario del VE: su cuenta es vulnerada 2- Atacante: obtiene acceso a la cuenta del usuario
¿En qué capa(s) EM-SA se debe trabajar la propuesta de prevención?	Información
El reglamento de interoperabilidad chileno ¿contempla la prevención de la vulnerabilidad?	No
Antigüedad	2021

Tabla 6.25. Ficha vulnerabilidad N°23.

Tomando en consideración las fichas de las Tablas 6.3 a la 6.25, que abordan aspectos tales como la descripción del problema, referencias, categorización y las medidas de mitigación propuestas, se identifican tendencias comunes en el manejo de las vulnerabilidades reportadas en la literatura a través de la capa de seguridad propuesta:

- **Autenticación y Acceso:**

- Gran parte de las vulnerabilidades están vinculadas con falencias

en la autenticación y control de acceso, evidenciando que sistemas y puntos de carga pueden exponer información sensible por configuraciones incorrectas o una gestión inadecuada de permisos.

- Problemas como la suplantación de identidad enfatizan la necesidad de implementar protocolos de seguridad robustos para asegurar una autenticación efectiva y segura.

■ Ataques a Aplicaciones Web:

- Las fichas destacan la susceptibilidad de las aplicaciones web a ataques como CSRF, la inyección SQL y otros, subrayando la importancia de la parametrización, sanitización de entradas y la adopción de mejores prácticas en el desarrollo web para proteger la integridad y confidencialidad de los datos.
- La vulnerabilidad a ataques basados en CORS y políticas de dominio cruzado en Flash resalta la necesidad de realizar evaluaciones de seguridad web y optimizar configuraciones de acuerdo con estándares de seguridad.

■ Infraestructura y Ataques de Red:

- La interconexión de los sistemas de carga con redes amplias introduce riesgos significativos, como ataques DoS/DDoS, si se explotan puntos de carga vulnerables. Vulnerabilidades en firmwares específicos permiten inyecciones maliciosas, comprometiendo la infraestructura. Es crucial una monitorización activa y una respuesta rápida para mantener la seguridad del sistema.

El análisis profundo de las vulnerabilidades y la presentación de soluciones a través de la capa de seguridad demuestra su capacidad no solo para identificar y alertar sobre riesgos potenciales sino también para ofrecer soluciones concretas y efectivas. Esta capa de seguridad representa un avance crucial en la protección de los sistemas de carga para vehículos eléctricos, contribuyendo a un entorno más seguro y resiliente.

6.6. Conclusiones

La transición hacia la movilidad eléctrica representa un pilar clave en la evolución hacia sistemas de transporte sostenibles y respetuosos con el medio

ambiente. A pesar de sus beneficios, la incorporación de tecnologías emergentes conlleva desafíos significativos, entre ellos, la necesidad de abordar riesgos y vulnerabilidades que puedan comprometer la seguridad y eficacia de su adopción.

Este trabajo se enfocó en la detección de vulnerabilidades en modelos de interoperabilidad para la electromovilidad, tanto actuales como futuros, con el objetivo de evaluar la capacidad de estos modelos para proteger la información confidencial del usuario, previniendo el robo, la clonación y la suplantación de identidad durante el proceso de recarga de vehículos eléctricos.

A través de la propuesta de una capa de Seguridad y sus distintas perspectivas, se evaluaron los componentes críticos de los modelos, identificando vulnerabilidades reportadas por diversos investigadores. La sección "Aplicación de la capa" demostró que esta abarca exhaustivamente el modelo evaluado, destacando su profundidad en cuanto a la seguridad.

Los resultados obtenidos a partir del modelo SGAM, que sirve como base para muchos otros modelos, sugieren que la aplicación de esta capa de seguridad podría generar mejoras significativas en la protección de sistemas similares.

En la sección "Testeo de la capa", se aplicó efectivamente esta capa, identificando vulnerabilidades específicas en un modelo y proponiendo recomendaciones para su resolución. Esta detección de falencias abre el camino hacia la mejora de la seguridad en los modelos existentes y futuros que incorporen esta capa de seguridad.

Las fichas de vulnerabilidad aportan una visión comprensiva de los riesgos asociados con los sistemas de carga de vehículos eléctricos, subrayando la importancia de implementar protocolos de seguridad robustos y de realizar evaluaciones constantes de las infraestructuras para mitigar posibles amenazas.

Este estudio no solo pone de relieve los problemas existentes sino que también orienta hacia soluciones prácticas, contribuyendo a la mejora de la seguridad en los sistemas de carga de vehículos eléctricos mediante la implementación de la capa de seguridad propuesta.

Capítulo 7

Conclusiones

La investigación expuesta en esta tesis aborda un aspecto crítico en la evolución hacia una movilidad sostenible y tecnológicamente avanzada: la seguridad en los sistemas de carga para vehículos eléctricos (VEs). Al analizar exhaustivamente los modelos de arquitectura existentes en la electromovilidad, se revela una significativa carencia en cuanto a la consideración y la implementación de protocolos de seguridad específicos, destacando una brecha crucial en la protección de la información y la infraestructura. Este hallazgo constituye el punto de partida para la integración de una capa de seguridad específica destinada a fortalecer la protección de la información y prevenir ataques cibernéticos tales como el robo de datos, la clonación y la suplantación de identidad. Esto es relevante dado que la adopción de vehículos eléctricos está en aumento, y con ello garantizar la seguridad de la infraestructura de carga es crucial para mantener ese ímpetu. Según la Agencia Internacional de Energía (AIE), el número de vehículos eléctricos está en camino de alcanzar casi 145 millones para el año 2030 bajo el escenario de políticas actuales, y hasta 230 millones si se implementan políticas más agresivas en línea con el Acuerdo de París.

En el tenor de lo antes descrito, la tesis ofrece un análisis crítico de los modelos de arquitectura orientados a la electromovilidad, como el modelo Smart Grid Architecture Model (SGAM) adaptado para el sector energético. Los resultados muestran que si bien estos modelos proporcionan un marco útil para el diseño e implementación de sistemas de electromovilidad,

adolecen de una especificidad necesaria en cuanto a medidas de seguridad, lo cual no solo incrementa el riesgo de vulnerabilidades sino que también afecta negativamente la confianza de los usuarios en los sistemas de carga de VEs.

Con el fin de abordar estas deficiencias, se propone la creación de una capa de seguridad diseñada específicamente para ser integrada en el diseño y operación de los sistemas de carga existentes y futuros. Este componente de seguridad busca la identificación proactiva de riesgos y vulnerabilidades, facilitando la generación de alertas y la implementación de medidas correctivas de manera oportuna. Esta propuesta representa un avance significativo en el campo de la electromovilidad, introduciendo una solución tangible a un problema previamente no resuelto.

Más allá de la mera detección de vulnerabilidades, se lleva a cabo un análisis exhaustivo sobre cómo esta capa de seguridad puede ser evaluada y aplicada en diversos modelos de interoperabilidad aplicables a la electromovilidad. A través de análisis teóricos, se demuestra la eficacia de la capa de seguridad en la mejora de la protección de la información confidencial del usuario, detectando vulnerabilidades y sugiriendo correcciones eficaces.

Los resultados de la investigación tienen importantes implicaciones para el futuro de la electromovilidad. La implementación de la capa de seguridad propuesta tiene el potencial de mejorar notablemente la seguridad de los sistemas de carga para VEs, contribuyendo a un entorno de electromovilidad más seguro y confiable. Esto no solo beneficia a los usuarios finales, protegiendo su información personal y financiera, sino que también refuerza la infraestructura crítica de carga de vehículos eléctricos, haciéndola más resistente a ataques cibernéticos.

Así, los resultados enfatizan la necesidad de integrar consideraciones de seguridad desde las fases iniciales de diseño e implementación de sistemas de carga para VEs. Ello debiera ser considerado por desarrolladores, reguladores y otros actores relevantes en la industria de la electromovilidad, adoptando un enfoque holístico y centrado en la seguridad, para abordar de manera efectiva los desafíos emergentes en esta área y asegurar un desarrollo sostenible y seguro de la electromovilidad.

Bibliografía

- [1] I. Furnes and M. Olsson, “Electric vehicles in norway: A qualitative study of the electric vehicle market in norway,” Master’s thesis, Copenhagen Business School, 2014.
- [2] N. García, “Electromovilidad,” in *Asesoría Técnica Parlamentaria*. BCN, 2019.
- [3] “Parque de autos se acelera y rozará los 5,5 millones de unidades este año,” *ISCI*, no. 17, Mar. 2021. [Online]. Available: <https://isci.cl/parque-de-autos-se-acelera-y-rozara-los-55-millones-de-unidades-este-ano/>
- [4] R. Hernández, C. Fernández, and P. Baptista, “Metodología de la investigación,” *McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.*, vol. 6, 2014.
- [5] IEA, “Global ev outlook 2021,” *IEA, Paris*, 2021. [Online]. Available: <https://www.iea.org/reports/global-ev-outlook-2021>
- [6] “Compromiso público privado por la electromovilidad,” *Ministerio de Energía*, 2022.
- [7] “Ruta energética 2018-2022,” *Ministerio de Energía*, 2022.
- [8] “Estrategia nacional de electromovilidad,” *Ministerio de Energía*, 2022. [Online]. Available: https://energia.gob.cl/sites/default/files/documentos/estrategia_nacional_de_electromovilidad_2021_0.pdf
- [9] M. de Energía, “Borrador reglamento interoperabilidad.” Santiago, Chile: Diario Oficial, 2022.
- [10] F. Cabrera and N. García, “Políticas de fomento a la electromovilidad,” in *Asesoría Técnica Parlamentaria*. BCN, 2019.
- [11] L. Ahumada, J. Frez, E. Gil, D. Godoy, and P. Dominguez, “Informe de estandarización en sistemas de medición, monitoreo y control,” Diciembre 2019.
- [12] L. Ahumada, J. Frez, D. Dujovne, and J. Vial, “Estudio de interoperabilidad en sistemas de recarga de vehículos eléctricos segundo informe:

BIBLIOGRAFÍA

- Definiciones, estudio técnico comparado y propuesta de arquitectura,” 2019.
- [13] IEEE, “Ieee standard computer dictionary: A compilation of ieee standard computer glossaries,” *IEEE Std 610*, 1991. [Online]. Available: <https://doi.org/10.1109/IEEESTD.1991.106963>
- [14] P. I, T. S, R. P. L. A, K. E, M. A, G. M, M. M, and O.-G. M, “Smart grid interoperability testing methodology,” no. KJ-NA-29416-EN-N (online), 2018.
- [15] J. Bruinenberg, L. Colton, E. Darmois, J. Dorn, J. Doyle, O. Elloumi, H. Englert, R. Forbes, J. Heiles, P. Hermans, and M. Uslar, “Cen - cenelec - etsi: Smart grid coordination group - smart grid reference architecture report 2.0,” Enero 2012.
- [16] M. Uslar and D. Engel, “Towards generic domain reference designation: How to learn from smart grid interoperability,” 11 2015.
- [17] G. Schuh, J. Fluhr, M. Birkmeier, and M. Sund, “Information system architecture for the interaction of electric vehicles with the power grid,” in *2013 10th IEEE INTERNATIONAL CONFERENCE ON NETWORKING, SENSING AND CONTROL (ICNSC)*, 2013, pp. 821–825.
- [18] DKE/DIN/VDE, “The german standardization roadmap smart city,” 2014. [Online]. Available: <https://www.dke.de/resource/blob/778248/d2afdaf62551586a54b3270ef78d2632/the-german-standardization-roadmap-smart-city-version-1-0-data.pdf>
- [19] A. Brand, M.-E. Iacob, and M. J. van Sinderen, “Interoperability architecture for electric mobility,” in *Enterprise Interoperability*, M. van Sinderen and V. Chapurlat, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 126–140.
- [20] B. Kirpes, P. Danner, R. Basmadjian, H. d. Meer, and C. Becker, “E-mobility systems architecture: a model-based framework for managing complexity and interoperability,” *Energy Informatics*, vol. 2, 2019. [Online]. Available: <https://doi.org/10.1186/s42162-019-0072-4>
- [21] G. C. Okwuibe, Z. Li, T. Brenner, and O. Langniss, “A blockchain based electric vehicle smart charging system with flexibility**this project

- is sponsored by oli systems gmbh, stuttgart.” *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 13 557–13 561, 2020, 21st IFAC World Congress. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2405896320311241>
- [22] A. Bokolo, “Applying enterprise architecture for digital transformation of electro mobility towards sustainable transportation,” in *Proceedings of the 2020 on Computers and People Research Conference*, ser. SIGMIS-CPR’20. New York, NY, USA: Association for Computing Machinery, 2020, p. 38–46. [Online]. Available: <https://doi.org/10.1145/3378539.3393858>
- [23] R. Basmadjian, “Communication vulnerabilities in electric mobility hcp systems: A semi-quantitative analysis,” *Smart Cities*, vol. 4, no. 1, pp. 405–428, 2021. [Online]. Available: <https://www.mdpi.com/2624-6511/4/1/23>
- [24] R. Basmadjian, B. Kirpes, J. Mrkos, and M. Cuchý, “A reference architecture for interoperable reservation systems in electric vehicle charging,” *Smart Cities*, vol. 3, no. 4, pp. 1405–1427, 2020. [Online]. Available: <https://www.mdpi.com/2624-6511/3/4/67>
- [25] A. Sanghvi and T. Markel, “Cybersecurity for electric vehicle fast-charging infrastructure,” Jun. 2021. [Online]. Available: <https://www.nrel.gov/docs/fy21osti/75236.pdf>
- [26] Z. Pourmirza and S. Walker, “Electric vehicle charging station: Cyber security challenges and perspective,” in *2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)*, 2021, pp. 111–116.
- [27] S. M. Danish, K. Zhang, H.-A. Jacobsen, N. Ashraf, and H. K. Qureshi, “Blockev: Efficient and secure charging station selection for electric vehicles,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4194–4211, 2020.
- [28] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, “Power jacking your station: In-depth security analysis of electric vehicle charging station management systems,” *Computers Security*, vol. 112, 11 2021.

BIBLIOGRAFÍA

- [29] G. Kim and J. Hur, “Methodology for security analysis of grid- connected electric vehicle charging station with wind generating resources,” *IEEE Access*, vol. 9, pp. 63 905–63 914, 2021.
- [30] ENCS, E.DSO, and ElaadNL, “Ev charging systems security requirements,” vol. 1, 2016.
- [31] P. Foix and F. Palma, “Metodología para la construcción del modelo de datos para la interoperabilidad de vehículos eléctricos e hidrógeno verde,” *CNE*, 2021.
- [32] R. Falk and S. Fries, “Electric vehicle charging infrastructure-security considerations and approaches,” *In Proceedings of the Fourth International Conference on Evolving Internet (INTERNET)*, 6 2012.
- [33] H. Lim, J. Ko, S. Lee, J. Kim, M. Kim, and T. Shon, “Security architecture model for smart grid communication systems,” *In Proceedings of the 2013 International Conference on IT Convergence and Security (ICITCS)*, 12 2013.
- [34] K. Bao, H. Valev, M. Wagner, and H. Schmeck, “A threat analysis of the vehicle-to-grid charging protocol iso 15118,” *Comput Sci Res Dev*, 2017.
- [35] S. Lee, Y. Park, H. Lim, and T. Shon, “Study on analysis of security vulnerabilities and countermeasures in iso/iec 15118 based electric vehicle charging technology,” *In Proceedings of the 2013 International Conference on IT Convergence and Security (In Proceedings of the 2014 International Conference on IT Convergence and Security)*, 10 2014.
- [36] J. Rubio, C. Alcaraz, and J. Lopez, “Addressing security in ocpp: Protection against man-in-the-middle attacks,” *In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2 2018.
- [37] B. Vaidya and H. Mouftah, “Deployment of secure ev charging system using open charge point protocol,” *In Proceedings of the 2018 14th International Wireless Communications Mobile Computing Conference (IWCMC)*, 6 2018.
- [38] J. Van Keulen, “Smart charging: A privacy and security analysis,” *Radboud Universiteit*, 2014.

- [39] J. White, “Cybersecurity for the future electric grid,” *National Renewable Energy Laboratory*, 5 2019.
- [40] C. Alcaraz, J. Lopez, and S. Wolthusen, “Ocpp protocol: Security threats and challenges,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2452–2459, 2017.
- [41] J. E. Rubio, C. Alcaraz, and J. Lopez, “Addressing security in ocpp: Protection against man-in-the-middle attacks,” in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2018, pp. 1–5.
- [42] R. Olave, “La hoja de ruta para la expansión de la electromovilidad,” *La Tercera*, 10 2023. [Online]. Available: <https://www.latercera.com/laboratoriodecontenidos/noticia/la-hoja-de-ruta-para-la-expansion-de-la-electromovilidad/GYHYAWYXVBD5XM6NRSIVDQGRB4/>
- [43] “Proyecto de inversión chino inyectará más de 200 millones de dólares para impulsar estrategia nacional del litio,” *Gobierno de Chile*, 10 2023. [Online]. Available: <https://www.gob.cl/noticias/proyecto-de-inversion-chino-inyectara-mas-de-200-millones-de-dolares-para-impulsar-estra>

