cigre Chile

PLAN DIRECTOR de CIBERSEGURIDAD

para el Sector Eléctrico

2021 – 2023

1 INDICE

Elaboración y Producción: Comité Chileno del CIGRE
Editor: Grupo de Trabajo (WG) Ciberseguridad en Sistemas Eléctricos CIGRE CHILE.

Coordinador y líder WG Ciberseguridad:
Ingeniero Eduardo Morales Cabellos – Socio CIGRE y representante en CIGRE Mundial Comité de Estudio (SC D2) Information Systems and Telecommunication.
Coordinador Producción General:
Manuel Silva Pino.
Corrección / Luz Marina Fuenzalida Gutierrez
Diseño y Diagramación / Paulina Ventura Peillard
Traducción / Claudia Falardo R.
Impresión Digital /

Primera Edición / Septiembre 2020

PALABRAS PRELIMINARES 1

El Comité Chileno de CIGRE ha estado observando con atención lo que viene ocurriendo hace un tiempo a nivel mundial acerca de las potenciales amenazas y ciberataques que pudieran sufrir las infraestructuras de los sistemas eléctricos. Además, se observa el aumento de normas y políticas que se han estado llevando a cabo en el país relativas a lineamientos y recomendaciones tanto para instituciones públicas como privadas que tienen sus sistemas de información conectados a sus redes internas/externas e internet, y el riesgo que conlleva no tomar medidas de control, visibilidad y mitigación ante ciberincidentes de seguridad.

En este escenario y junto a la ausencia hoy en día de una ley de Infraestructuras Críticas (II.CC.) -que norme y regule los ámbitos de protección de las mismas- es que se propone formar un grupo de trabajo en agosto de 2018, de modo de generar una discusión y análisis sobre las normas, sistemas y arquitecturas de seguridad presentes en las redes eléctricas en Chile. Lo anterior bajo el prisma de estudio de las principales normativas internacionales y mejores prácticas en ciberseguridad industrial, considerando a la vez una mirada de ciber-riesgos para determinar su mayor o menor robustez y resiliencia frente a ciberataques. Todo ello permitiría elaborar propuestas para la ciberseguridad del sector eléctrico.

El presente trabajo es el esfuerzo de cerca de 40 ingenieros, técnicos y expertos que por más de un año se reunieron de manera periódica para analizar las brechas de ciberseguridad del sector, cuantificar el grado de madurez de ciberseguridad (basado en normativas internacionales) y proponer un Plan Director de Ciberseguridad para el sector eléctrico con medidas concretas de corto, mediano y largo plazo, que permita apoyar al gobierno y las empresas del rubro en conducir la gestión de la ciberseguridad de las infraestructuras críticas de una manera estratégica, colaborativa y proactiva.

Gabriel Olguín P.
Presidente
CIGRE Chile

GABRIEL OLGUÍN PARADA
Presidente CIGRE Chile

1 PALABRAS PRELIMINARES

En agosto de 2018 dimos el inicio como CIGRE Chile al grupo de trabajo de ciberseguridad para el sector eléctrico con un objetivo muy claro y ambicioso, aportar con análisis y reflexiones para generar un plan con medidas concretas para abordar la ciberseguridad del sector eléctrico desde la perspectiva de la gestión del riesgo y la ciber resiliencia. Todo esto luego de un año de haberse publicado en 2017 la Política Nacional de Ciberseguridad por el Gobierno de Chile, donde aparece el sector energía como una de las principales infraestructuras críticas de la información que deben resguardarse ante potenciales ataques cibernéticos.

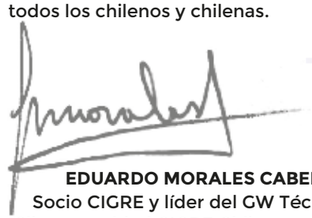
Eduardo Morales C.
Socio CIGRE
y líder del GW
Técnico de
Ciberseguridad
CIGRE Chile
Representante.

Representante
en CIGRE Mundial
Comité de Estudio
(SC D2) Information
Systems and
Telecommunication.

El grupo de trabajo conformado por cerca de 40 ingenieros especialistas tanto del sector público como privado, se reunieron periódicamente para ir avanzando con el análisis en cuestión. Con mucho orgullo debo recalcar que me siento privilegiado por haber liderado un equipo de esta calidad profesional. Gracias al aporte y visión de cada uno de ellos, hemos podido llegar a un documento con una mirada técnica consensuada que presenta un Plan Director de Ciberseguridad 2021-2023 que propone una ruta para abordar la protección de la infraestructura eléctrica en el ciberespacio, pero que también puede servir de guía para infraestructuras críticas de otros sectores del país.

Este documento plantea siete objetivos estratégicos de largo plazo, destinados a abordar los desafíos como sector eléctrico y también como país para la protección de las infraestructuras críticas enfrentadas a las amenazas del ciberespacio, incorporando medidas concretas tanto para las instituciones del sector público como privado. Adicionalmente, se acompaña un reporte de análisis de brechas en ciberseguridad en el sector eléctrico en Chile, que viene a complementar y entregar el sustento necesario para llegar al Plan Director. Para este trabajo ocupamos metodologías ágiles organizándonos en células de trabajo donde abordamos las brechas de ciberseguridad en los ámbitos legal, normativo técnico y gobierno organizacional. Creemos firmemente que un análisis exhaustivo de la situación actual del sector eléctrico con respecto a la ciberseguridad nos permitió llegar de manera más rápida y concreta a las recomendaciones y medidas específicas con respecto al tema.

El gran desafío que enfrentamos una vez terminado este trabajo será el cómo implementar y monitorear estas medidas y lineamientos estratégicos en el tiempo. Sin duda, resulta imprescindible contar con la colaboración de todos los actores del sector eléctrico, de manera que se coopere, tal como lo menciona nuestra Política Nacional de Ciberseguridad, en la construcción de un ciberespacio abierto, libre y seguro para todos los chilenos y chilenas.



EDUARDO MORALES CABELLO
Socio CIGRE y líder del GW Técnico de Ciberseguridad CIGRE Chile representante
Representante en CIGRE Mundial Comité de Estudio (SC D2) Information Systems and Telecommunication.

INTRODUCCIÓN 2

La masificación en el uso de tecnologías de la información y comunicaciones (TIC) genera múltiples beneficios en el quehacer de los ciudadanos como la utilización de sistemas cada vez más automatizados que otorgan mayores facilidades y accesos y la entrega de servicios que permiten a las personas un mejor estándar y calidad de vida. Si bien esta digitalización de las cosas aporta al desarrollo del país, también conlleva riesgos que pueden afectar la seguridad pública, los derechos esenciales de las personas y la seguridad exterior de Chile. Estos riesgos pueden provenir de múltiples fuentes y se pueden manifestar mediante actividades como espionaje, sabotaje, fraudes o ciberataques realizados por otros países, por grupos organizados o bien por particulares. Estos escenarios nos llevan a tener una mayor conciencia de lo que significa proteger no tan solo la información, como conceptualmente lo hemos asumido por años, sino también aquellas infraestructuras cuyo funcionamiento continuo y controlado resulta crítico para las comunidades, y que eventualmente, podrían ser objeto de ataques cibernéticos en vista al efecto o reacción que esto puede producir.

Se define como Infraestructura Crítica (II.CC) a las instalaciones, sistemas o parte de estos que son esenciales para el mantenimiento de las funciones sociales básicas, y cuya perturbación o destrucción, afectaría gravemente la salud, la integridad física, la seguridad y el bienestar social y económico de la población . De hecho, hablar de infraestructura crítica es hablar de un asunto estratégico y de seguridad de la defensa nacional, tanto en ambientes físicos como en el ciberespacio.

A nivel latinoamericano, el tema de la infraestructura crítica es un pendiente, así como lo revela el reporte “Protección a infraestructura crítica en Latinoamérica y el Caribe 2018” , lanzado por la Organización de Estados Americanos (OEA) y Microsoft. Se encuestó a cerca de 500 dueños y operadores de infraestructura crítica y se constató que un 57% no cuenta con un presupuesto dedicado para medidas en ciberseguridad. Esto devela que la legislación es débil y que aún falta conciencia en los países latinoamericanos para trabajar en una política nacional de infraestructuras críticas que permita poner este tema en la relevancia que se merece.

En Chile, la Política Nacional de Ciberseguridad ya menciona la importancia de la protección de las denominadas Infraestructuras Críticas de la Información (ICI) desde la perspectiva de su protección en el ciberespacio, definiendo los siguientes sectores como críticos: energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa.

Sin duda, esto es un avance pero se requiere un esfuerzo aún mayor para poder generar una política de II.CC. y una ley que sustente las bases de protección tanto en el ámbito físico como en el ciberespacio. En nuestro país, un porcentaje alto de nuestra II.CC. está en manos de privados, quienes deben adaptarse a la incorporación de criterios definidos, estándares y buenas prácticas en materia de ciberseguridad de manera coordinada con los intereses de una política de II.CC. de largo plazo.

Es por ello que debe construirse una base sólida de información comenzando por los

http://www.cigre.cl/wp-content/uploads/2018/08/CARLOS-LANDEROS.pdf
https://www.oas.org/es/sms/cicte/cipreport.pdf
https://www.ciberseguridad.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf

2 INTRODUCCIÓN

planes estratégicos sectoriales que permitan identificar cuáles son los activos críticos que deben ser protegidos y cuáles son sus amenazas y vulnerabilidades específicas, para determinar luego los eventuales impactos. Todo esto con el fin de ir midiendo los niveles de madurez y hacer el seguimiento del cumplimiento de las medidas de protección.

Claramente existen soluciones de base que se recomiendan para la protección de la infraestructura crítica como asegurar una clara división de responsabilidades a nivel organizacional; un enfoque holístico (que aborde aspectos técnicos, sociales, económicos, organizativos, cumplimiento de la ley y de la política de seguridad, entre otros); desarrollo de referencias (frameworks, guías, procedimientos); capacitación en seguridad física y digital del personal que opera II.CC.; conformar equipos de respuesta ante incidentes sectoriales (CSIRT); gestión de proveedores en materia de seguridad de la información (terceros) e; intercambio de conocimiento a nivel nacional (privado-público) e internacional (acuerdos de colaboración), entre otras soluciones.

Para los propietarios de infraestructura crítica, la toma de conciencia se constituye finalmente en un deber que se conecta con su misión institucional y que permite afianzar la seguridad nacional y la sustentabilidad del servicio que otorgan a todos los habitantes del país. Mientras no exista una ley de infraestructura crítica, no habrá forma de obligar a los propietarios a subir los estándares de seguridad y la sociedad se arriesga a vulnerabilidades en el suministro de los servicios básicos que van desde errores humanos por negligencia, ataques terroristas y ciberataques que podrían afectar a una parte importante de la población.

Por lo tanto, es un deber de todos tomar acción en esta materia de tal forma de igualarnos a los países más desarrollados que, a través de un marco legal y lineamientos bien definidos para los propietarios de infraestructura crítica, obligan a proteger los servicios que se están proveyendo por un bien superior que es “asegurar la estabilidad económica y social de los países”. Es allá donde se apunta con la publicación de este plan director y el reporte de análisis de brechas en ciberseguridad.

El presente trabajo es el esfuerzo de cerca de 40 ingenieros, técnicos y expertos que por más de un año se reunieron de manera periódica para analizar las brechas de ciberseguridad del sector, cuantificar el grado de madurez de ciberseguridad (basado en normativas internacionales) y proponer un Plan Director de Ciberseguridad para el sector eléctrico con medidas concretas de corto, mediano y largo plazo, que permita apoyar al gobierno y las empresas del rubro en conducir la gestión de la ciberseguridad de las infraestructuras críticas de una mnera estratégica, colaborativa y proactiva.

Este trabajo responde a la siguiente visión y misión:

Visión

- Aportar al sector eléctrico chileno con lineamientos estratégicos y recomendaciones para llegar a ser, en el mediano y largo plazo, una infraestructura crítica ciber-resiliente ante nuevas amenazas y vulnerabilidades en un mundo digital.

Misión

- En un plazo acotado entregar las recomendaciones en ciberseguridad para el sector eléctrico a nivel gubernamental y empresarial para aportar a una futura ley de infraestructuras críticas en el ciberespacio.

3 LA IMPORTANCIA DE LA CIBERSEGURIDAD ESTRATÉGICA

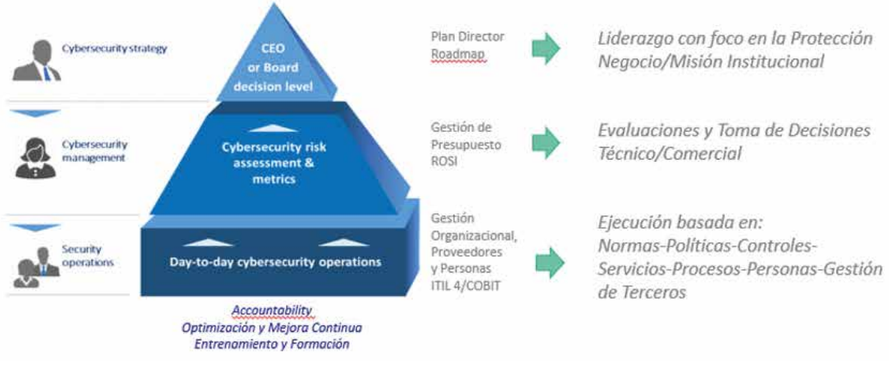
Si bien la ciberseguridad, definida en la actualidad como la protección de los sistemas de información en el ciberespacio, posee una componente técnica basada en normativas, frameworks y buenas prácticas que se ocupa de acciones operacionales y tácticas del día a día, tiende a dejar de lado la componente más estratégica y de gestión.

Para los expertos en materia de ciberseguridad, una visión estratégica de management y liderazgo organizacional es primordial para obtener una protección efectiva y resiliente frente a los ciberataques a infraestructuras críticas. Sin una planificación estratégica de ciberseguridad, se augura un duro camino para quien esté a cargo de esta materia al interior de la organización ya que tendrá que gestionar los riesgos y la continuidad del negocio atendiendo solo a eventos críticos del día a día o a acciones tácticas de mediano plazo, careciendo de una visión de más largo plazo que permita medir los niveles de madurez en seguridad y anticiparse a los ciberataques con medidas defensivas y ofensivas de seguridad combinadas con ciberinteligencia.

La ciberseguridad estratégica plantea de una manera simple los principales puntos a poner énfasis desde lo estratégico, táctico y operacional, partiendo de la base que la ciberseguridad estratégica requiere de un líder con habilidades técnicas y de gestión que permitan definir y llevar a cabo un plan director que marque la ruta en materia de niveles de madurez en ciberseguridad y que procure que la organización alcance mayores grados de ciber-resiliencia y gestión de riesgos.

Un enfoque integral y en 360° es el requerido como metodología para llevar a cabo un plan director de ciberseguridad sectorial con medidas concretas en el corto, mediano y largo plazo. Por otro lado, se visualiza que el nivel estratégico es quien debe apalancar todos los lineamientos de este plan director y hacer la correspondiente bajada organizacional. Un plan director de este tipo está dirigido a los tomadores de decisión de la organización.

Finalmente, el enfoque de ciberseguridad estratégica garantiza a las empresas y organizaciones una transformación digital eficiente y segura, alineada con el negocio o la misión institucional.



Fuente: Adaptación WG Ciberseguridad C Chile de https://www.brookings.edu/blog/africa-in-focus/2018/06/04/cybersecurity-in-africa-securing-businesses-with-a-local-approach-with-global-standards/

ANÁLISIS DE ENTORNO Y BRECHAS DE CIBERSEGURIDAD EN EL SECTOR ELÉCTRICO 4

El trabajo realizado por el equipo técnico de ciberseguridad de CIGRE Chile está basado principalmente en un análisis de entorno y brechas de ciberseguridad que permitió conocer la realidad de la ciberseguridad del sector eléctrico del país y cuyos aspectos más relevantes se listan a continuación:

- La normativa vigente en el sector eléctrico no contempla la ciberseguridad de manera explícita en sus exigencias prácticas, ni la mención de los incidentes de seguridad de la información como un elemento de riesgo bien definido.

- La institucionalidad en el sector eléctrico existe y se deben fijar de manera clara y explícita las responsabilidades de cada institución en materia de ciberseguridad en las actividades normativas que pueden ser recomendaciones, buenas prácticas, definición de criterios, actividades de concienciación y gestión de incidentes de ciberseguridad.

- Existe adherencia parcial a algunas normativas internacionales como NIST, NERC CIP e ISO 27.000, entre otras, pero falta aún agregar estas normas a la regulación existente y, sobre todo, sumar algunas más estrictas en materia de infraestructura crítica para la protección de la seguridad de la información y de los datos como IEC 62443, ISO27019, ISO 27005, 27014, 27017 (Controles en la Nube), ISO 22301, Ley 19.628 y GDPR, entre otras.

- Modelos de iSOC y arquitecturas de seguridad en profundidad están siendo recién conocidas para la visibilidad, protección y monitoreo integral de las redes eléctricas, en pro de la seguridad de suministro y continuidad del servicio.

- Se mantiene la estructura organizacional basada en silos y se requiere un responsable de alto nivel en cada empresa, un CISO (Chief Information Security Officer).

- Nuevas tecnologías para enfrentar nuevas y avanzadas amenazas como Sandboxing, UBA (User Behavior Analytics), Anti-malware, EDR (Endpoint Detection and Response) y herramientas de Ciberinteligencia, Simuladores de Ataques (ciberejercicios), plataformas de Análisis de Malware y Análisis Forense, son escasas en el sector aún sobre todo para las Redes OT.

- Se requiere de una planificación y coordinación de ejercicios de ciberseguridad en el sector, donde participe el TSO (Transmission System Operator), empresas coordinadas del sistema (empresas del sector) y con la observancia de la autoridad reguladora del mercado y la autoridad fiscalizadora, en vista a evaluar impactos, lecciones aprendidas, buenas prácticas o bien desafíos a enfrentar.

- Arquitecturas Convergentes TI/TO integradas de manera segura, que permitan la visibilidad y protección tanto de la red TI como TO, comienzan recién a vislumbrarse en proyectos tecnológicos.

- Mayor inversión en capacitación y formación de ingenieros del rubro, así como también en herramientas de entrenamiento y concienciación.

- Proyectos eléctricos de gran envergadura deben comenzar a contemplar la ciberseguridad embebida desde su diseño.

Una mayor cantidad de hallazgos y brechas más específicas se pueden encontrar en el Reporte de Análisis de Brechas en Ciberseguridad en el Sector Eléctrico en Chile que es el documento base que acompaña este trabajo.

https://www.smart-energy.com/wp-content/uploads/2014/02/EPRI-Planning-ISOC-report.pdf

5 ESTRUCTURA DE CAPAS EN CIBERSEGURIDAD RECOMENDADA PARA EL SECTOR ELÉCTRICO

Actualmente, el sector eléctrico está gobernado por organismos en tres niveles (estratégico, táctico y operacional) que cumplen un rol fundamental en la concreción de los planes y políticas del sector eléctrico.

Capas Organizacionales del Sector Eléctrico en Chile.

Fuente:WG Ciberseguridad CIGRE Chile "El poder distinguir y conocer el rol de las principales instituciones organizacionales del sector eléctrico en Chile en cada una de las capas permite comprender y definir mejor el papel que jugarán cada una de las instituciones en materia de ciberseguridad". De acuerdo con este nivel de organización bien estructurado y con capas funcionales definidas, podemos deducir que, en materia de ciberseguridad, cada capa también tiene funciones que deben ser desarrolladas en cada nivel. A continuación, algunas recomendaciones:

Capa Estratégica

- Fijar las normas técnicas y de calidad bajo el prisma de la ciberseguridad y privacidad, indispensables para el funcionamiento y la operación de las instalaciones energéticas.

- Futuras actualizaciones a los reglamentos de ley y normativas técnicas deben considerar agregar la componente de ciberseguridad y protección de datos personales.

Capa Táctica

- Mejoramiento de la normativa y sistemas de fiscalización en materia de ciberseguridad.

- Crear planes de concienciación en ciberseguridad para la educación de las empresas del sector, empleados y usuarios.

Capa Operacional

- Poner en marcha exigencias en materia de ciberseguridad en la coordinación de la operación de las instalaciones del Sistema Eléctrico Nacional (SEN).

- Preservar la seguridad del servicio en el sistema eléctrico no solo en el plano físico, sino que también supervigilar en el ciberespacio de su competencia en coordinación con las instalaciones de los agentes coordinados, haciendo uso de herramientas de visibilidad, ciberinteligencia, gestión de riesgos e incidentes y capas de protección de ciberseguridad en los elementos y/o actores que componen el sistema.

"Solamente un trabajo en conjunto y coordinado entre todas las capas permitirá abordar la ciberseguridad de manera integral para la protección y ciber-resiliencia del SEN, cuyo funcionamiento está basado hoy no solo en un plano físico, sino también en uno virtual".

Capas Organizacionales del Sector Eléctrico en Chile

CIBERATAQUES A LOS SISTEMAS SCADA EN EL SECTOR ELÉCTRICO 6

Los sistemas de control que se usan en el mundo para el monitoreo y la operación de los sistemas eléctricos también se han vuelto un blanco de los ciberatacantes, debido a la gran cantidad de información sensible que manejan y la relación directa que tienen con la seguridad de suministro en el país. Los especialistas coinciden en que el big data que posee la industria energética se ha transformado en un activo crítico, por ende, está pasando a formar parte de las estrategias de ciberseguridad en varios países, especialmente en aquellos que cuentan con un mayor desarrollo tecnológico en generación, transmisión y distribución eléctrica.

Hace algún tiempo a nivel mundial, se observa con mucha atención tanto las amenazas como ciberataques a sistemas eléctricos. Un caso emblemático y de estudio que se debería analizar en Chile son los ciberataques a los sistemas de la red eléctrica ocurridos en diciembre de 2015 y diciembre de 2016 en la zona oeste de Ucrania, operada por empresas privadas de transporte y distribución eléctrica.

En el primer ciberataque de 2015, varias subestaciones eléctricas fueron afectadas dejando cerca de 700.000 residentes sin electricidad por cerca de 7 horas. Expertos indican que en este ciberataque se utilizó el malware KillDisk cuya variante incluía funcionalidades adicionales que permitían al troyano de puerta trasera BlackEnergy no sólo borrar archivos del sistema para evitar cualquier posibilidad de reinicio, sino que también portaba códigos específicos para sabotear sistemas industriales.

Industroyer, el primer malware modular y altamente customizable que podría adaptarse a cualquier infraestructura crítica (como suministro de luz, agua y gas), es el responsable de que Ucrania se quedara a oscuras nuevamente en diciembre de 2016, una especie de cyber arma que no se veía desde Stuxnet. Industroyer es una amenaza particularmente peligrosa dado que es capaz de controlar los interruptores de una subestación eléctrica directamente. Para hacerlo, utiliza protocolos de comunicación industrial implementados mundialmente (estándares IEC 60870-5-101, IEC 60870-5-104, IEC 61850 y OLE for Process Control Data Access, OPC DA).

Los últimos antecedentes recopilados en ciberataques a sistemas eléctricos a nivel mundial develan que van en aumento, destacándose el ciberataque a la Northwest Territories Power Corporation (NTPC), empresa generadora y distribuidora de electricidad en Canadá, que sufrió un ataque de ransomware. Sin embargo, NTPC no es la única organización que enfrenta incidentes de violación o ransomware puesto que varias otras entidades a nivel mundial en el sector de energía han enfrentado tales incidentes. A continuación, se listan :

- En junio de 2020 el fabricante de automóviles Honda y una división de la eléctrica italiana Enel son las nuevas víctimas del ransomware SNAKE que atacó sus servicios financieros y de atención al cliente.

- En abril de 2020, el gigante energético multinacional Energias de Portugal (EDP) recibió el ransomware Ragnar Locker a través del cual los piratas informáticos robaron 10 TB de archivos confidenciales de la empresa pidiendo además 1580 BTC (US$ 10,9M) en rescate.

https://cyware.com/news/cyberattack-on-ntpc-further-exposes-the-cybersecurity-risks-of-energy-sector-6896de5e

6 CIBERATAQUES A LOS SISTEMAS SCADA EN EL SECTOR ELÉCTRICO

• En marzo de 2020, la European Network of Transmission System Operators for Electricity (ENTSO-E) fue blanco de un incidente de intrusión cibernética, aunque no se revelaron más detalles sobre el incidente.

• En febrero de 2020, el Reading Municipal Light Department (RMLD) de Massachusetts, Estados Unidos, fue blanco de ciberdelincuentes quienes intentaron pedir dinero mediante el cifrado de datos en el sistema informático de la estación.

• En enero de 2020, se observó una campaña de piratas informáticos iraníes dirigida al sector energético europeo, en la que los atacantes intentaron robar información confidencial utilizando el malware PupyRAT.

"Todo esto nos devela que una gestión de riesgos adecuada con una visión integral permitirá en forma periódica ir revisando las diferentes vulnerabilidades y amenazas presentes en los sistemas SCADA. Es importante reconocer también que nada podrá evitar un ataque cibernético a las instalaciones eléctricas, pero si podemos disminuir el impacto de la criticidad de los incidentes de ciberseguridad con una preparación adecuada, se podrá mitigar y responder de manera rápida ante cualquier ataque cibernético".

COVID-19

Finalmente, cabe decir, que los efectos de la pandemia covid-19 también han dejado un impacto a nivel de ciberseguridad, como lo demuestra el último informe de Deloitte que señala que los ciberdelincuentes de todo el mundo están sacando provecho de esta crisis. Se ha observado un aumento de ataques de phishing, malspams y ransomware, dirigidos no solo a empresas, sino que también a usuarios finales (trabajadores remotos) que descargan las aplicaciones relacionadas con covid-19.

Sin duda, la pandemia cambiará nuestras vidas para siempre emergiendo nuevos estilos de trabajo, nuevos problemas de ciberseguridad y nuevas políticas sanitarias, entre otras. La lucha contra el covid-19 será un esfuerzo conjunto y evidentemente las organizaciones necesitarán repensar su gestión de riesgos cibernéticos, así como también sus planes de continuidad del negocio.

https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html

CAUSA RAÍZ DE LOS ATAQUES A INFRAESTRUCTURAS CRÍTICAS 7

A nivel mundial, si analizamos el sinnúmero de ataques tanto a la infraestructura física como a la virtual asociada al ciberespacio, se observan al menos tres principales motivos de la causa raíz que son dinero, poder y subversión, importantes de entender ya que darán luces para las futuras leyes que se tengan que dictar o modificar en el país:

1) Dinero: asociado principalmente a la delincuencia y al crimen organizado que hoy en día ve en el ciberespacio la oportunidad de cometer delitos sin dejar rastros evidentes ya que es más difícil la pesquisa y trazabilidad del delito. Los delitos informáticos asociados son generalmente fraude electrónico, violación de propiedad intelectual, uso indebido de tarjetas de crédito o débito, etc.

Según el fabricante Symantec en su último Norton Cyber Security Insights Report 2017, Global Results , durante ese año fueron robados 172.000 millones de dólares en ciberataques y más de 978 millones de personas en el mundo perdieron dinero el año anterior (2016), en promedio alrededor de 142 dólares por persona, debido al cibercrimen organizado. El 20% de las víctimas usó la misma contraseña entre múltiples cuentas y al menos el 58% de las víctimas compartió sus contraseñas con otros. En la legislación chilena existe una ley que data de 1993 que sanciona los delitos cibernéticos a través de 4 artículos. Sin embargo, según el Convenio de Budapest , que es el primer tratado internacional que busca hacer frente a los delitos informáticos y a los delitos en internet, al cual Chile se adhirió en abril de 2017, se requiere modificar la ley actual. En ninguno de los 4 artículos se menciona explícitamente (según Claudio Maglio na, 2018) el "fraude informático, como una figura dolosa, en la cual se exija como elemento subjetivo del tipo el ánimo de lucro, y como elemento objetivo la obtención mediante una manipulación informática de una transferencia indebida de cualquier activo patrimonial en perjuicio de tercero".

2) Poder: asociado principalmente a estados (el Informe Anual PandaLabs 2017 , menciona como un ejemplo claro el ataque a empresas con oficinas en Ucrania a través del Petya/Goldeneye, con un motivo claramente político donde el propio gobierno ucraniano acusó abiertamente al gobierno ruso de estar detrás del mismo) o poderes fácticos (de acuerdo con el Diccionario de la Real Academia Española, el poder fáctico es "el que se ejerce en la sociedad al margen de las instituciones legales, en virtud de la capacidad de presión o autoridad que se posee; p. ej., la banca, la Iglesia, la prensa, etc.") , que en la actualidad intentan controlar y manejar la información para su propio beneficio. Los delitos asociados a este tipo de causa raíz pueden ser sabotaje informático, espionaje industrial o intervención maliciosa de los sistemas de control SCADA, entre otros.

Esto debería ser un antecedente para considerar en una futura ley de protección de infraestructuras críticas ya que podrían ser afectadas tanto por conductas de ciberespionaje o sabotaje informático de parte de grupos fácticos, como también por ciberataques de países enemigos que afecten a la soberanía nacional. La Política Nacional de Ciberdefensa chilena deja expresamente claro en su Artículo 1°, punto 3.2, el recurso del uso de la fuerza en legítima defensa en elciberespacio: "La Política de Ciberdefen-

https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf
https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
https://www.pandasecurity.com/spain/mediacenter/src/uploads/2017/11/Informe_Anual_PandaLabs_2017.pdf
http://www.revistas.unam.mx/index.php/rmcpys/article/viewFile/42190/38336

7 CAUSA RAÍZ DE LOS ATAQUES A INFRAESTRUCTURAS CRÍTICAS

sa es parte de la Política de Defensa Nacional, y forma parte integral de los objetivos y principios de ésta, en especial en lo referido a:

- Las operaciones de defensa en el ciberespacio constituyen una dimensión específica del espectro contemporáneo del empleo de las capacidades de defensa.

- La planificación, conducción y ejecución de las operaciones en el ciberespacio se ceñirá estrictamente al respeto del Derecho Internacional Público, con especial consideración al Derecho Internacional de los Derechos Humanos y al Derecho Internacional Humanitario. Por tanto, Chile se abstendrá de recurrir a la amenaza de uso o al uso de la fuerza en una forma que contravenga el Derecho Internacional y podrá hacer uso de la fuerza en legítima defensa en el ciberespacio, de conformidad con lo dispuesto en el artículo 51 de la Carta de Naciones Unidas".

3) Subversión: asociado principalmente a grupos terroristas o activistas políticos antisistema que recurren al ciberterrorismo o hacktivismo para hacer presión a los gobiernos y causar temor en la población para imponer sus ideologías y desestabilizar el sistema político o económico de un país.

Según la U.S. Federal Bureau of Investigation, el ciberterrorismo es "cualquier ataque premeditado y políticamente motivado en contra de la información, los sistemas informáticos, programas computacionales y datos que resultan en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos".

Algunos ejemplos de ciberterrorismo son:

- Irrupción de sitios web para crear molestias o inconvenientes públicos, o también para detener el tráfico a páginas web que publican contenido con el que los hackers no están de acuerdo.

- Ciberterroristas internacionales acceden e inhabilitan o modifican las señales que controlan la tecnología militar.

- Ciberataques que se dirigen a los sistemas de infraestructura crítica, por ejemplo, para deshabilitar una planta de tratamiento de agua, provocan un corte de energía regional o interrumpen un oleoducto o una refinería de petróleo. Este tipo de ataque cibernético podría afectar a las principales ciudades, causar una crisis de salud pública, poner en peligro la seguridad de millones de personas y suscitar pánico y muertes masivas.

El término hacktivismo fue acuñado en el año 1996 por el grupo Cult of the Dead Cow (cDc), una organización internacional de hackers y otros manifestantes dedicados a los derechos humanos. En lugar de lanzar ciberataques, el hacktivismo usó sus habilidades de programación para desarrollar herramientas de software para respaldar la libertad de expresión y la privacidad. Ellos criticaron el uso de ataques DoS (Denegation of Service) y alteraciones web como antiéticas a la libertad de voz.

Tanto el ciberterrorismo como el hacktivismo, están o podrían estar presente con mayor fuerza en un futuro cercano en nuestro país.

http://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf
https://www.military.com/defensetech/2011/09/12/cyber-terrorism-now-at-the-top-of-the-list-of-security-concerns

https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism

MEDICIÓN DEL NIVEL DE MADUREZ EN CIBERSEGURIDAD 8

La medición de los niveles de madurez en ciberseguridad es vital para asegurar un óptimo plan director que provea una hoja de ruta para cualquier organización. De acuerdo a lo anterior y detectada su importancia en el sector eléctrico chileno, el grupo de trabajo de CIGRE decidió buscar una metodología de medición.

Así, se decidió utilizar el Modelo de Madurez de Capacidad de Ciberseguridad del Subsector de Electricidad (ES-C2M2) Versión 1.1 desarrollado por el Departamento de Energía (DOE) de Estados Unidos en colaboración con el Departamento de Seguridad Nacional (DHS), el sector privado y expertos del sector público.

El programa C2M2 es una iniciativa público-privada estadounidense que se estableció como resultado de los esfuerzos de la administración para mejorar las capacidades de seguridad cibernética del subsector de electricidad y comprender el estado de ciberseguridad de la red. El C2M2 ayuda a las organizaciones, independientemente de su tamaño, tipo o industria, a evaluar, priorizar y mejorar sus propias capacidades de ciberseguridad.

El modelo se centra en la implementación y gestión de las prácticas de ciberseguridad asociadas con la operación y el uso de los activos de tecnología de la información y operacionales y sus entornos. El objetivo es apoyar el desarrollo continuo y la medición de las capacidades de seguridad cibernética dentro de cualquier organización mediante:

- Fortalecimiento de las capacidades de ciberseguridad de las organizaciones.
- Permitir que las organizaciones evalúen sus capacidades de ciberseguridad de manera efectiva y consistente.
- Compartir conocimientos, mejores prácticas y referencias relevantes entre organizaciones como un medio para mejorar las capacidades de ciberseguridad.
- Permitir que las organizaciones prioricen acciones e inversiones para mejorar la ciberseguridad.
- Apoyar la adopción del Marco de Seguridad Cibernética del Instituto Nacional de Estándares y Tecnología (NIST).

El ES-C2M2 está diseñado para usarse como una metodología de autoevaluación y dispone de un kit de herramientas para que una organización mida y mejore su programa de ciberseguridad.

Fuente: ES-C2M2, https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf
https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

8 MEDICIÓN DEL NIVEL DE MADUREZ EN CIBERSEGURIDAD

Esta metodología fue utilizada para la medición del sector eléctrico chileno en los siguientes dominios:

Para cada dominio se midió el nivel de madurez en ciberseguridad en una escala de 0 a 3, según la característica indicada por la metodología:

horizonte de brechas o gaps existentes a fin de completar cada nivel. Este indicador de madurez circular incorpora en el centro la cantidad total de actividades gestionables propuestas por la metodología ES-C2M2 y que se deben cumplir para alcanzar el MILX del dominio específico.

Level	Characteristics
MIL0	• Practices are not performed
MIL1	• Initial practices are performed but may be ad hoc
MIL2	*Institutionalization characteristics:* • Practices are documented • Stakeholders are identified and involved • Adequate resources are provided to support the process • Standards or guidelines are used to guide practice implementation *Approach characteristic:* • Practices are more complete or advanced than at MIL1
MIL3	*Institutionalization characteristics:* • Activities are guided by policy (or other directives) and governance • Policies include compliance requirements for specified standards or guidelines • Activities are periodically reviewed for conformance to policy • Responsibility and authority for practices are assigned to personnel • Personnel performing the practice have adequate skills and knowledge *Approach characteristic:* • Practices are more complete or advanced than at MIL2

**MIL: Maturity Indicator Level*

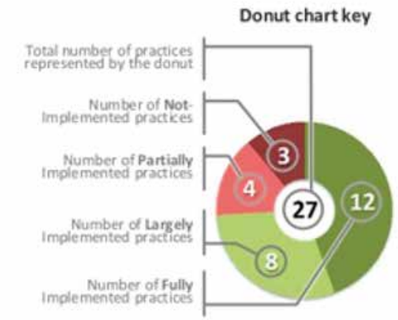
Fuente: ES-C2M2, https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

Cada dominio de ciberseguridad exige un listado de prácticas del C2M2. De esta manera, para alcanzar el estatus MIL2 se requiere haber implementado el total de prácticas de los niveles MIL1 y MIL2 y así sucesivamente hasta el MIL3.

De esta forma, por cada dominio y cada nivel de madurez tendremos una medición del conocimiento alcanzado y el

En la siguiente figura, se refleja en color verde oscuro el número de actividades que se cumplen al 100% (full), en color verde claro el número de actividades que se cumplen al 75% (ampliamente), en color rojo el número de actividades que se cumplen al 50% (parcialmente) y en color café el número de actividades que no se cumplen 0% (no cumplimiento).

MEDICIÓN DEL NIVEL DE MADUREZ EN CIBERSEGURIDAD 8



Fuente: ES-C2M2 https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

Al final, se obtuvo un dashboard del nivel de madurez en ciberseguridad de cada organización que accedió a esta autoevaluación y mediante un análisis estadístico haciendo uso del promedio y en algunos casos la moda, según el criterio aplicado para cada práctica, se obtuvo una muestra del nivel más representativo de madurez en ciberseguridad del sector eléctrico chileno.

De un total de alrededor de 40 empresas que se convocó a esta medición entre marzo y agosto de 2019, solo 5 organizaciones del mundo público y privado (equivalente al 12,5% del total de las empresas), decidieron entregar sus resultados. Cabe destacar, que la baja participación expone el hecho que la ciberseguridad no es necesariamente una acción que se monitoree permanente. Así, resulta imprescindible hacia el futuro fortalecer la colaboración y una mayor toma de conciencia entre los actores del sector en esta materia.

“Si bien el sector continuamente incorpora tecnologías y actualiza sus sistemas, el no contar con un patrón o estándar de medición que rescate las realidades, o bien el nivel efectivo con que la ciberseguridad está incorporada como parte de los procesos de las compañías fueron parte de las razones observadas de la baja participación.

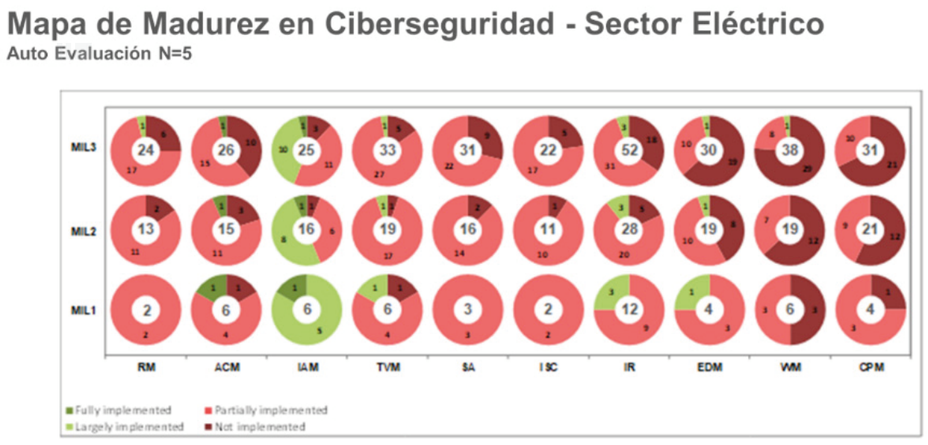
Es relevante destacar las dificultades en este proceso de autoevaluación ya sea por no contar con una documentación que evidenciara el cumplimiento de las actividades identificadas por la herramienta de autoevaluación, la asimetría en tamaños de las compañías en algunos casos, el disponer o no de profesionales especializados que facilitaran esta medición y la carencia de sistemas que evidenciaran el tratamiento o atención a la materia de ciberseguridad por sobre un tratamiento TI convencional, entre otras.

Por otro lado, si la muestra es representativa o no de la madurez del sector eléctrico en materia de ciberseguridad, por la baja participación de las empresas en las autoevaluaciones, creemos que efectivamente es cuestionable la representatividad del indicador

8 MEDICIÓN DEL NIVEL DE MADUREZ EN CIBERSEGURIDAD

de madurez. Sin perjuicio de ello, destacamos que es el primer indicador de madurez en ciberseguridad que se mide en el sector eléctrico chileno y que permite disponer de una base para trabajar desde allí en aumentar las capacidades y concienciación en ciberseguridad".

Finalmente, y considerando la muestra obtenida en las autoevaluaciones, se generó un primer mapa de madurez de capacidades de ciberseguridad del sector eléctrico presentado a continuación:



RM: Risk Management ACM: Asset, Change, and Configuration Management IAM: Identity and Access Management TVM: Threat and Vulnerability Management SA: Situational Awareness	ISC: Information Sharing and Communications IR: Event and Incident Response, Continuity of Operations EDM: Supply Chain and External Dependencies Management WM: Workforce Management CPM: Cybersecurity Program Management

Fuente: WG Ciberseguridad CIGRE Chile de Toolkit ES-C2M2

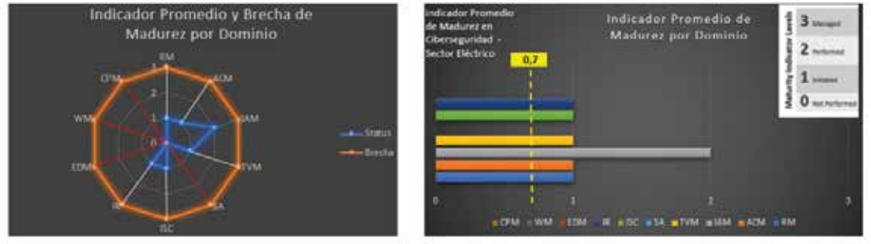
MEDICIÓN DEL NIVEL DE MADUREZ EN CIBERSEGURIDAD 8

El dashboard muestra la gran mayoría de los dominios en rojo, que indica un cumplimiento parcial (50%) de las actividades gestionables exigidas para cada nivel de madurez en cada dominio. Se destaca el dominio IAM (Gestión de Accesos e Identidad) con el mejor índice de madurez debido a que históricamente el sector eléctrico ha cumplido con la normativa técnica de manera rigurosa en lo que respecta a la seguridad física de las instalaciones, a través de un riguroso control de accesos e identidades.

Existen 4 dominios críticos para los cuales el nivel de madurez es muy inferior a lo esperado: SA (Conciencia Situacional), EDM (Gestión de Terceros, Dependencias Externas y Cadena de Suministro), WM (Gestión Empleados y Fuerza Laboral) y CPM (Gestión de un Programa de Ciberseguridad).

El resto de los dominios -RM (Gestión de Riesgos), ACM (Gestión de Activos, Cambios y Configuraciones), IR (Continuidad de Operaciones, Eventos y Respuesta ante Incidentes), ISC (Comunicaciones y Compartición de Información) y TVM (Gestión de Amenazas y Vulnerabilidades)- contribuye mayormente al indicador promedio de madurez de este estudio y la moda.

Esto nos lleva a obtener el siguiente indicador promedio de madurez en ciberseguridad para el sector eléctrico en Chile:



Fuente:WG Ciberseguridad CIGRE Chile

Un indicador promedio de 0,7 y una moda de 1 revelan que para la gran mayoría de los dominios se adoptan prácticas de ciberseguridad básicas, pero de manera ad hoc, mostrando que dependen mucho de la expertise de las personas encargadas más que de los procedimientos y documentación que evidencien dichas prácticas.

Esta medición cuantitativa nos devela una baja madurez en ciberseguridad para el sector eléctrico chileno que requiere no solo de un plan director claro y específico, sino que también de un seguimiento y gobernanza. De esta manera, en el corto y mediano plazo este sector podrá elevar rápidamente sus niveles de madurez.

9 PLAN DIRECTOR: LINEAMIENTOS ESTRATÉGICOS DE CIBERSEGURIDAD

El grupo de trabajo de CIGRE definió 7 lineamientos estratégicos específicos para el sector eléctrico que se apoyan en los lineamientos establecidos en la Política Nacional de Ciberseguridad:

	Lineamientos Estratégicos en Ciberseguridad para el Sector Eléctrico (2021-2023)	Concepto Clave
1.-	El sector eléctrico contará con una infraestructura ciber-resiliente ante amenazas y vulnerabilidades, preparada para resistir y recuperarse ante incidentes de ciberseguridad, bajo el enfoque de la gestión de riesgos.	Ciber-resiliencia
2.-	Desarrollar una cultura de ciberseguridad con el fin de generar conciencia en cada organización, mediante buenas prácticas, capacitación en áreas críticas y campañas periódicas de responsabilidad en el manejo de las tecnologías digitales, sea tanto en tecnologías de información (TI) como en tecnologías de operación (TO).	Cultura de Ciberseguridad
3.-	Conformar un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT) sectorial que permita alertar y apoyar la respuesta ante ciberataques, así como también coordinar con otros CSIRT públicos y privados para afrontar los ataques de manera coordinada.	CSIRT Sectorial
4.-	Establecer relaciones de cooperación en ciberseguridad entre todos los actores del mercado eléctrico y formar alianzas internacionales con entidades eléctricas expertas en el área.	Alianzas de Cooperación
5.-	Planificar y participar en ciberejercicios nacionales, internacionales y multisectoriales que permitan evaluar la ciber-resiliencia de la infraestructura de la información.	Ciberejercicios
6.-	Medir periódicamente los avances y la evolución de la madurez de la ciberseguridad a través de un plan de trabajo con base normativa y manejo de la privacidad, para alcanzar los niveles más altos de protección de los activos críticos de la información y de datos personales.	Medición de Madurez
7.-	Fomentar el desarrollo e innovación en ciberseguridad industrial tanto en la academia como en la industria eléctrica para alcanzar los lineamientos estratégicos definidos.	I+D+I

MEDIDAS DE CIBERSEGURIDAD PARA EL SECTOR ELÉCTRICO 2021-2023 10

Las presentes medidas forman parte del Plan Director de Ciberseguridad para el sector eléctrico que apalancan cada uno de los lineamientos estratégicos propuestos para su implementación en el corto plazo (CP) entre 6 meses y 12 meses, mediano plazo (MP) entre 13 meses y 24 meses y largo plazo (LP) entre 25 meses y 36 meses. Adicionalmente, se sugieren a modo de recomendación, las instituciones responsables y colaboradoras en el cumplimiento de las medidas y su seguimiento.

Ciber-Resiliencia	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
1	Implementar un listado de requerimientos mínimos en ciberseguridad exigibles en contratos para proveedores de servicio.	Coordinador / SEC	CP
2	Conformación de un comité de expertos en ciberseguridad del sector eléctrico que permita concretar las medidas de corto, mediano y largo plazo del Plan Director.	Ministerio de Energía / CNE / SEC / Coordinador / Empresas Eléctricas A.G. / CIGRE	CP
3	Revisión, ampliación y fiscalización de las 13 medidas urgentes de ciberseguridad impuestas por el Coordinador para los Coordinados.	SEC / Coordinador / Coordinados	CP
4	Solicitud a la CNE de la Revisión de la Norma Técnica y definición de requerimientos mínimos de ciberseguridad a cumplir.	Coordinador / CIGRE / Coordinados / Empresas Eléctricas A.G. / Otros	MP
5	Definir distintos escenarios de crisis ante ataques cibernéticos que requieran de ciber-resiliencia para la continuidad del servicio del sector eléctrico.	Ministerio del Interior / Coordinador / SEC / CNE / Ministerio de Energía / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	MP
6	Desarrollar programas de *pentesting* o *ethical hacking* para el equipamiento eléctrico (medidores inteligentes, plc, sensores, etc.) ante ciberataques.	Coordinador / Universidades-Institutos / Coordinados	MP
7	Elaborar y confeccionar un reporte tipo de incidentes de seguridad que permita tener la información adecuada en caso de registrarse en la empresa afectada un ciberataque.	SEC / Coordinador / Ministerio del Interior / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros)	MP
8	Establecer la institucionalidad con roles definidos y gobernanza en materia de incidentes de seguridad en caso de un ciberataque.	Ministerio de Energía / CNE / SEC / Coordinador	MP
9	Definir las instituciones públicas y privadas del sector que por su grado de criticidad de activos deben poseer un equipo de respuesta ante incidentes de seguridad (CSIRT) y un *Security Operation Center* (SOC).	Ministerio del Interior / Ministerio de Energía / CNE / Coordinador / SEC / Empresas Eléctricas A.G. / Ministerio del Interior	LP

10 MEDIDAS DE CIBERSEGURIDAD PARA EL SECTOR ELÉCTRICO 2021-2023

Cultura de Ciberseguridad	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
10	Programación anual de seminarios, congresos, charlas de ciberseguridad industrial, entre otros, para el sector eléctrico.	CIGRE / Ministerio de Energía / Empresas Eléctricas A.G. / Universidades-Institutos	CP
11	Diseñar planes periódicos de concienciación en ciberseguridad para todos los empleados de instituciones públicas y privadas del sector.	SEC / Coordinador / Coordinados	MP
12	Definir cursos de perfeccionamiento en ciberseguridad para los encargados de seguridad de la información en ambientes TI/TO para instituciones públicas y privadas del sector.	Ministerio de Energía / Coordinador / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	MP
13	Diseñar e implementar una campaña de ciberseguridad industrial de carácter masivo para empleados y empresas del sector, y fomentar la ejecución de programas de difusión y guías de buenas prácticas en acciones de sensibilización.	Ministerio de Energía / Coordinador / SEC / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	MP
14	Conformar una mesa intersectorial para fomentar la importancia de la protección de infraestructuras críticas. Creación de un Centro Nacional de II.CC.	Ministerio del Interior / Ministerio de Energía	MP
15	Acercamiento con universidades, institutos y centros de capacitación que permitan aumentar el conocimiento (cursos, diplomados, carreras) en ciberseguridad industrial para la creación de capital humano en el sector.	Coordinador / Ministerio de Energía / Universidades-Institutos	LP
16	Definir un mes para la protección de infraestructuras críticas que permita crear concienciación.	Ministerio del Interior / Ministerio de Energía	LP
17	Creación de un grupo de trabajo y alianzas con centros nacionales e internacionales de análisis de *malware*/forense para la compartición de información relevante ante ciberamenazas en el sector eléctrico.	SEC / Ministerio de Energía / Coordinador / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	LP

CSIRT Sectorial	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
18	Diseño y desarrollo de capacidades técnicas para un CSIRT Eléctrico.	Coordinador / Coordinados	CP
19	Acuerdo de colaboración con el CSIRT de Gobierno para establecer apoyo para la creación del CSIRT Eléctrico.	Coordinador / Ministerio del Interior / Ministerio de Energía	CP
20	Desarrollo de un RFI (Request for information) que permita a empresas de ciberseguridad nacionales e internacionales presentar posibles soluciones, dimensionamiento y presupuesto para proyectar a futuro el CSIRT sectorial.	Coordinador	MP
21	Definir, documentar e implantar un proceso para la gestión de los incidentes de seguridad en el sector eléctrico.	Coordinador / Ministerio de Energía / CNE / SEC / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	MP
22	Generar una base de conocimiento de incidentes de seguridad del sector, procedimientos y prácticas a aplicar para el monitoreo, detección y respuesta de incidentes.	Coordinador / SEC / Ministerio de Energía / CNE	MP
23	Definir un canal de comunicación oficial del sector eléctrico, para compartir información referente a los incidentes y amenazas de ciberseguridad.	SEC / Coordinador / Ministerio de Energía	MP
24	Liberación y adjudicación de RFP (Request for Proposal) de implementación del CSIRT Eléctrico.	Coordinador / Ministerio de Energía / CNE	MP

Alianzas de Cooperación	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
25	Alianza con el CSIRT de Gobierno	Ministerio de Energía / Coordinador / SEC	CP
26	Creación de alianzas con entidades de prestigio en ciberseguridad industrial, nacionales e internacionales, para compartir experiencias respecto a estándares y buenas prácticas en esta materia.	Coordinador / SEC / Coordinados / Universidades-Institutos	MP
27	Establecer alianzas multisectoriales (banca, defensa, Gobierno) que permita compartir mejores prácticas en seguridad de la información y protección de datos críticos.	Coordinador / SEC / Universidades-Institutos	MP
28	Alianzas con universidades, institutos y centros de formación para la creación de capital humano en pregrado/postgrado a formar parte de los CSIRT y SOC para el sector eléctrico.	Ministerio de Energía / SEC / Coordinador / Universidades-Institutos	MP
29	Alianzas con CSIRT nacionales o internacionales para la compartición y colaboración ante amenazas e incidentes de seguridad relacionados con el sector eléctrico.	Coordinador /SEC / Ministerio del Interior / Ministerio de Energía	LP

Ciberejercicios	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
30	Diseñar un Plan de Ciberejercicios basado en experiencias internacionales para el sector eléctrico.	Coordinador / SEC / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	CP
31	Acercamiento y acuerdo con universidades e institutos para programar en un mediano y largo plazo ciberejercicios que unan los talentos del mundo académico y privado.	Coordinador / Ministerio de Energía / Coordinados / Universidades-Institutos	MP
32	Realizar ejercicios de simulación de crisis y ciberejercicios al menos una vez al año, con la participación de las principales empresas eléctricas, Coordinador, Gobierno y entidades internacionales.	Coordinador / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros / SEC / Ministerio de Energía / CNE	LP
33	Crear un centro de entrenamiento con plataformas y simuladores especializados con el fin de estandarizar los conocimientos y experiencias de los directores de los CSIRT de ciberseguridad del sector.	Coordinador / Ministerio del Interior / Coordinados	LP

Medición de Madurez	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
34	Desarrollar una encuesta periódica para las empresas coordinadas que permita medir las brechas en ciberseguridad y en protección de datos críticos.	SEC	CP
35	Establecer un estándar anual de medición de madurez en ciberseguridad por dominios y protección de datos en el sector eléctrico, con el fin de conocer el nivel y los *gaps* y alcanzar niveles de madurez superiores en el sector.	SEC / Ministerio de Energía / Coordinador	MP
36	Actualizar la normativa técnica que permita exigir a las empresas reguladas la medición anual de las brechas de ciberseguridad y sus mejoras.	CNE / Ministerio de Energía / SEC / Coordinados / Agrupaciones o Asociaciones Gremiales / CIGRE / Otros	MP
37	Crear un Plan de Concienciación en Ciberseguridad Industrial para el sector eléctrico para empleados y proveedores (terceros) que permita prevenir delitos informáticos.	Coordinador / SEC / Coordinados / Ministerio de Energía / Agrupaciones o Asociaciones Gremiales / Otros	MP
38	Creación de una base de datos con los responsables de ciberseguridad de las empresas eléctricas que permita un canal de comunicación en caso de incidentes de seguridad críticos.	SEC / Coordinador	LP
39	Añadir un capítulo de ciberseguridad a la preparación y gestión de contratos en licitaciones públicas y privadas del sector eléctrico.	CNE / Ministerio de Energía / Coordinador / SEC	LP
40	Creación de un grupo de trabajo que permita dar continuidad y seguimiento a la medición de los niveles de madurez dentro de un marco normativo y de obligaciones para las infraestructuras críticas del sector eléctrico.	Coordinador / SEC / CIGRE / Coordinados / Agrupaciones o Asociaciones Gremiales / Otros	LP

10 MEDIDAS DE CIBERSEGURIDAD PARA EL SECTOR ELÉCTRICO 2021-2023

I+D+i	Medidas Propuestas	Responsables/Colaboradores Propuestos	Horizonte
41	Estudio, investigación y análisis de *malwares* de ataques cibernéticos a nivel internacional que permita sacar lecciones aprendidas en arquitecturas, procesos, concienciación, gestión y respuestas ante incidentes frente a ataques en el sector eléctrico.	Coordinador / Coordinados / Universidades-Institutos	CP
42	Elaborar programas o proyectos de inversión público-privado para el desarrollo de tecnología y *software* que permita el monitoreo, ciberinteligencia, *big* data e inteligencia artificial aplicada a la ciberseguridad del sector.	Ministerio de Energía / CORFO / ANID /Coordinador / Coordinados	MP
43	Promover iniciativas académicas, como memorias o concursos estudiantiles, donde se ofrezca como premio el financiamiento de proyectos que apoyen a la ciberseguridad y la protección de datos del sector.	Coordinador / SEC / Universidades-Institutos / CIGRE	MP
44	Desarrollo de una herramienta de visibilidad con un *dashboard* estratégico del sector en materia de incidentes de ciberseguridad para el CSIRT Eléctrico.	Coordinador / SEC / Ministerio de Energía / Coordinados	LP
45	Acercamiento y acuerdos con empresas fabricantes nacionales e internacionales en ciberseguridad industrial para fomentar la inversión en la industria como polo de desarrollo económico y capital humano.	Ministerio de Energía / Ministerio de Economía	LP

CONCLUSIONES 11

La información contenida en este documento representa el trabajo de un grupo de especialistas reunidos en una mesa de trabajo de CIGRE Chile que se decidió a analizar las amenazas y riesgos de ciberseguridad dada la relevancia que representa este tema en el sector eléctrico. A continuación, se presentan las principales conclusiones:

- Dado el Análisis de Brechas de Ciberseguridad en el Sector Eléctrico, se requiere de manera prioritaria colocar el acento en ciberseguridad a nivel legal, normativo técnico y de gobierno institucional que permita de manera explícita a las empresas del rubro comenzar a invertir y aumentar los presupuestos en tecnología, procesos y personas en materia de protección de activos y ciberactivos críticos ante posibles ataques cibernéticos.

- Dada la infraestructura eléctrica actual y su progresiva transformación digital, se requiere de medidas concretas que contribuyan a desarrollar una infraestructura ciber-resiliente orientada a la gestión de riesgos y de la continuidad del negocio, de manera tal que se minimicen los impactos y se mitiguen rápidamente los riesgos ante amenazas del ciberespacio.

- Conociendo que el eslabón más débil de la cadena en materia de seguridad de la información son las personas, se requiere desarrollar una cultura de ciberseguridad en el sector eléctrico a nivel de empleados, ejecutivos, stakeholders y proveedores (terceros) que contribuya de manera proactiva a cuidar la información crítica de la infraestructura a través de campañas de sensibilización, programas de concienciación y cursos de capacitación en materia de ciberseguridad industrial.

- A nivel mundial los ataques cibernéticos a infraestructuras críticas han ido en aumento, se requiere comenzar un plan para contar con un CSIRT Eléctrico en el mediano plazo para la gestión y respuesta ante incidentes de seguridad, permitiendo conectarse con otros CSIRT de Gobierno, banca y defensa para la rápida cooperación y compartición de información que minimice el impacto ante cualquier sabotaje, fraude o robo de información a nivel país.

- Las alianzas de colaboración tanto nacionales como internacionales son fundamentales para aumentar la base de conocimiento. En este contexto, son primordiales los actuales tratados que se han firmado en materia de ciberseguridad con distintos países y el relacionamiento con expertos de centros de investigación, empresas fabricantes y universidades, entre otros, para conocer los últimos avances en materia de ciberseguridad industrial.

- Los ciberejercicios son una medida efectiva y práctica de preparación de la infraestructura eléctrica ante ciberataques ya que permiten simular y crear situaciones de riesgo ante un ataque a través de las redes de comunicación y control y ver que tan preparados se encuentra los sistemas y cuáles serían las mejoras que se deberían hacer. Los ciberejercicios realizados de manera periódica representan una buena práctica para contribuir a la ciber-resiliencia y a la gestión de riesgos y de continuidad del negocio en el tiempo.

- Es de suma relevancia medir el nivel de madurez en ciberseguridad tanto del

11 CONCLUSIONES

sector eléctrico como de las principales empresas y organizaciones que lo conforman. Se propone hacer esta práctica anualmente para que el sector eléctrico transite desde niveles inferiores de ciberseguridad a un nivel avanzado en un periodo de 3 años. El Plan Director propuesto plantea medidas concretas en el corto, mediano y largo plazo, asumiendo que la gradualidad ayudará a conseguir el objetivo de madurez deseado en esta materia.

- Dado que la ciberseguridad industrial es un campo reciente de estudio y desarrollo en el país, se propone el acercamiento a universidades, institutos y empresas fabricantes, entre otros, para fomentar la investigación, el desarrollo e innovación y carreras y diplomados que permitan resolver los problemas nacionales en materia de ciberseguridad en el sector eléctrico, a través del acceso a fondos de inversión que contribuyan al desarrollo de un polo económico potente en el tiempo aumentando el capital humano y nuevos puestos de trabajo.

- Finalmente, cabe decir que este trabajo del Grupo de Ciberseguridad de CIGRE Chile tiene la esperanza y el afán de poder seguir contribuyendo con este tema a nivel nacional en una futura Política o Ley de Infraestructuras Críticas, de suma relevancia para el país, y esperamos que los lineamientos, medidas, recomendaciones y conclusiones plasmadas en este estudio puedan ser de gran utilidad para el sector eléctrico y también para otros sectores industriales de igual criticidad, de tal manera de priorizar acciones e inversiones que vayan en esta línea.

ANEXO A: RESUMEN DEL MODELO ES-C2M2 12

"A continuación, se detalla el Modelo ES-C2M2 usado y aplicado en el sector eléctrico de Estados Unidos que permitió llevar a cabo una muestra del nivel de madurez en ciberseguridad del sector eléctrico en Chile. Como grupo de trabajo de CIGRE Chile damos un especial agradecimiento al DOE (Departamento de Energía) de USA por haber accedido a nuestra petición de uso y envío del toolkit de autoevaluación y las guías para su uso de su versión 1.1".

El modelo de madurez de capacidad en ciberseguridad del subsector de electricidad (ES-C2M2) puede ayudar a las organizaciones y empresas eléctricas a evaluar y realizar mejoras en sus programas de ciberseguridad.

El ES-C2M2 es parte del Programa del Modelo de Madurez de Capacidad de Ciberseguridad (C2M2) del DOE (Departamento de Energía de USA) y fue desarrollado para abordar las características únicas del subsector de electricidad. El programa respalda el desarrollo continuo y la medición de las capacidades de ciberseguridad en el subsector de electricidad y puede usarse para:

- Fortalecer las capacidades de ciberseguridad en el sector eléctrico.

- Habilitar a las utilities para evaluar y comparar de manera efectiva y consistente las capacidades de ciberseguridad.

- Compartir conocimientos, mejores prácticas y referencias relevantes dentro del sector como un medio para mejorar las capacidades de ciberseguridad.

- Permitir a los servicios públicos priorizar acciones e inversiones para mejorar la ciberseguridad .

El ES-C2M2 está diseñado para usarse con una metodología de autoevaluación y un kit de herramientas (disponible a pedido) para que una organización mida y mejore su programa de ciberseguridad. Una autoevaluación usando el set de herramientas se puede completar en un día, pero este mismo kit podría adaptarse para un esfuerzo de evaluación más riguroso. Además, el modelo puede informar el desarrollo de un nuevo programa de ciberseguridad.

El ES-C2M2 proporciona orientación descriptiva en lugar de preceptiva y centrada en la industria. El contenido del modelo se presenta en un alto nivel de abstracción para que pueda ser interpretado por organizaciones de subsectores de varios tipos, estructuras y tamaños. Se espera que el uso masivo del modelo respalde la evaluación comparativa de las capacidades de seguridad cibernética del subsector. Estos atributos también hacen del ES-C2M2 una herramienta fácilmente escalable para la implementación en el subsector del Framework (marco de referencia) de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST).

El modelo surge de una combinación de estándares, marcos, programas e iniciativas de ciberseguridad existentes y proporciona una guía flexible para ayudar a las organizaciones a desarrollar y mejorar sus capacidades de ciberseguridad. Como resultado, las prácticas del modelo tienden a estar en un alto nivel de abstracción y pueden interpretarse para organizaciones de diversas estructuras y tamaños.

12 ANEXO A: RESUMEN DEL MODELO ES-C2M2

El modelo está organizado en 10 dominios. Cada dominio es una agrupación lógica de prácticas de ciberseguridad. Las prácticas dentro de un dominio se agrupan por objetivos. Dentro de cada objetivo, las prácticas son ordenadas por un indicador de nivel de madurez o Maturity Indicator Level (MIL).

Cada uno de los 10 dominios del modelo contiene un conjunto estructurado de prácticas de ciberseguridad. Cada conjunto de prácticas representa las actividades que una organización puede realizar para establecer y madurar una determinada capacidad en el dominio. Por ejemplo, el dominio de Gestión de Riesgos es un grupo de prácticas que una organización puede realizar para establecer y madurar la capacidad de gestión de riesgos de ciberseguridad. Para cada dominio, el modelo proporciona una declaración de propósito, que es un resumen de alto nivel de la intención del dominio, seguido de notas introductorias que dan contexto al dominio e introducen sus prácticas.

Fuente: ES-C2M2, https://www.energy.gov/sites

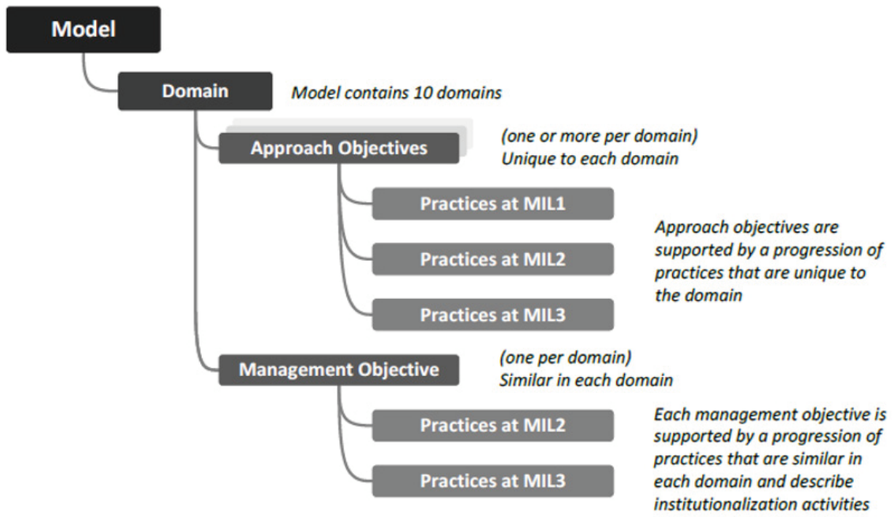


Figure 4: Model and Domain Elements

/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

ANEXO A: RESUMEN DEL MODELO ES-C2M2 12

A continuación, se presenta una breÅr el riesgo de ciberseguridad para la organización, incluidas las unidades de negocio, subsidiarias, infraestructura interconectada relacionada y partes interesadas.

Gestión de activos, cambios y configuraciones Administrar los activos de OT y TI de la organización, incluidos el hardware y el software, en proporción con el riesgo para la infraestructura crítica y los objetivos de la organización.

Gestión de identidad y acceso. Crear y administrar identidades para organismos a los que se les puede otorgar acceso lógico o físico a los activos de la organización. Controlar el acceso a los activos de la organización de acuerdo con el riesgo para la infraestructura crítica y los objetivos de la organización.

Gestión de amenazas y vulnerabilidades Establecer y mantener planes, procedimientos y tecnologías para detectar, identificar, analizar, administrar y responder a las amenazas y vulnerabilidades de ciberseguridad, proporcionales al riesgo para la infraestructura de la organización (ejemplo: crítica, TI, operativa) y objetivos organizacionales.

Conciencia situacional Establecer y mantener actividades y tecnologías para recopilar, analizar, alarmar, presentar y usar información operativa y de seguridad cibernética, incluyendo información de estatus y resúmenes de los otros dominios del modelo para formar una imagen operativa común.

Intercambio de información y comunicaciones Establecer y mantener relaciones con entidades internas y externas para recopilar y proporcionar información de seguridad cibernética, incluidas amenazas y vulnerabilidades, para reducir riesgos y aumentar la capacidad de recuperación operativa, acorde con el peligro para la infraestructura crítica y los objetivos de la organización.

Respuesta a eventos e incidentes, continuidad de operaciones Establecer y mantener planes, procedimientos y tecnologías para detectar, analizar y responder a eventos de seguridad cibernética y proteger las operaciones durante un evento de seguridad cibernética, acorde con el riesgo para la infraestructura crítica y los objetivos organizacionales.

Cadena de suministro y gestión de dependencias externas Establecer y mantener controles para gestionar los riesgos de ciberseguridad asociados con los servicios y activos que dependen de entidades externas, proporcionales al riesgo para la infraestructura crítica y los objetivos de la organización.

Administración de personal Establecer y mantener planes, procedimientos, tecnologías y controles para crear una cultura de ciberseguridad y para garantizar la idoneidad y competencias continuas del personal, acorde con el riesgo para la infraestructura crítica y los objetivos organizacionales.

Gestión del programa de ciberseguridad Establecer y mantener un programa de ciberseguridad empresarial que prometa gobernanza, planificación estratégica y ampare las actividades de ciberseguridad de la organización de una manera que alinee los objetivos de ciberseguridad con los objetivos estratégicos de la organización y el riesgo para la infraestructura crítica.

El modelo define cuatro niveles de indicadores de madurez, MIL0 a MIL3, que se aplican

independientemente a cada dominio del modelo. Los MILs definen una progresión doble de madurez (enfoque e institucionalización) que se explican en las siguientes secciones.

Hay cuatro aspectos de los MILs que son importantes para comprender y aplicar el modelo:

1. Los niveles del indicador de madurez se aplican independientemente a cada dominio. Como resultado, una organización que usa el modelo puede estar operando con diferentes clasificaciones MIL para diferentes dominios. Por ejemplo, una organización podría estar operando en MIL1 en un dominio, MIL2 en otro dominio y MIL3 en un tercer dominio.

2. Los MILs son acumulativos dentro de cada dominio. Para obtener un MIL en un dominio determinado, una organización debe realizar todas las prácticas en ese nivel y sus niveles anteriores. Por ejemplo, una organización debe realizar todas las prácticas del dominio en MIL1 y MIL2 para lograr un MIL2 en el dominio. Del mismo modo, la organización tendría que realizar todas las prácticas en MIL1, MIL2 y MIL3 para lograr un MIL3. 3. Establecer un MIL objetivo para cada dominio es una estrategia efectiva para usar el modelo para guiar la mejora del programa de seguridad cibernética. Las organizaciones deben familiarizarse con las prácticas en el modelo antes de determinar el MIL objetivo. Las actividades de análisis de brechas y los esfuerzos de mejora deberían centrarse en alcanzar esos niveles objetivos. 4. Tanto el desempeño de la práctica como alcanzar un MIL deben alinearse con los objetivos comerciales y la estrategia de ciberseguridad de la organización. Esforzarse por alcanzar el MIL más alto en todos los dominios puede no ser óptimo. Las empresas deben evaluar los costos de lograr un MIL específico frente a los beneficios potenciales. Sin embargo, el modelo se desarrolló para que todas las empresas, independientemente de su tamaño, puedan alcanzar un MIL1 en todos los dominios.

Table 1: Example of Approach Progression in the Cyber Program Management Domain

MIL0		
MIL1	a.	The organization has a cybersecurity program strategy
MIL2	b.	The cybersecurity program strategy defines objectives for the organization's cybersecurity activities
	c.	The cybersecurity program strategy and priorities are documented and aligned with the organization's strategic objectives and risk to critical infrastructure
	d.	The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities
	e.	The cybersecurity program strategy defines the structure and organization of the cybersecurity program
	f.	The cybersecurity program strategy is approved by senior management
MIL3	g.	The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile (TVM-1d)

Fuente: ES-C2M2, https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

A continuación, se describen las prácticas de gestión de cada MIL:

Maturity Indicator Level 0 (MIL0)
El modelo no contiene prácticas para el MIL0. El rendimiento en MIL0 simplemente significa que el MIL1 en un dominio dado, no se ha logrado.

Maturity Indicator Level 1 (MIL1)
En cada dominio, el MIL1 contiene un conjunto de prácticas iniciales. Para lograr un MIL1, estas actividades iniciales pueden realizarse de manera ad hoc, pero deben realizarse. Si una organización comenzara sin capacidad para gestionar la ciberseguridad, debería centrarse inicialmente en implementar las prácticas del MIL1.

El MIL1 se caracteriza por una práctica de gestión única:
1. Las prácticas iniciales se realizan, pero pueden ser ad hoc. En el contexto de este modelo, ad hoc (es decir, una práctica ad hoc) se refiere a realizar una práctica que depende en gran medida de la iniciativa y experiencia de un individuo o equipo (liderazgo de equipo), sin mucha orientación organizativa a través de un plan verbal o escrito, política o capacitación. La calidad del resultado puede variar significativamente dependiendo de quién realiza la práctica, cuándo se realiza, el contexto del problema que se aborda, los métodos, herramientas y técnicas utilizadas y la prioridad dada a una instancia particular de la práctica. Con personal experimentado y talentoso, se pueden lograr resultados de alta calidad incluso si las prácticas son ad hoc. Sin embargo, en este MIL, las lecciones aprendidas generalmente no se capturan a nivel organizacional, por lo que los enfoques y resultados son difíciles de repetir o mejorar en toda la organización.

Maturity Indicator Level 2 (MIL2)
Cuatro prácticas de gestión están presentes en el MIL2, que representan un nivel inicial de institucionalización de las actividades dentro de un dominio:

1. Las prácticas están documentadas y se realizan de acuerdo con un plan. El enfoque aquí debe estar en la planificación para garantizar que las prácticas se diseñen (o seleccionen) intencionalmente para servir a la organización.

2. Las partes interesadas de la práctica están identificadas e involucradas en su desempeño. Esto podría incluir a las partes interesadas dentro de la función, de toda la organización o de fuera de la organización, dependiendo de cómo la organización implementó la práctica.

3. Se proporcionan recursos adecuados en forma de personas, financiamiento y herramientas para garantizar que las prácticas se puedan realizar según lo previsto. El desempeño de esta práctica se puede evaluar determinando si las prácticas deseadas no se han implementado debido a la escasez de recursos. Si todas las prácticas deseadas se han implementado según lo previsto por la organización, se han proporcionado los recursos adecuados.
4. La organización identificó algunos estándares y/o pautas para informar la implementación de las prácticas en el dominio. Éstas pueden ser simplemente las fuentes de referencia que la organización consultó al desarrollar el plan para realizar las prácticas.

En general, las prácticas en el MIL2 son más completas que en el MIL1 y no se realizan de manera irregular o no son ad hoc en su implementación. Como resultado, el desempeño de las prácticas en la organización es más estable y se mantendrá en el tiempo.

Maturity Indicator Level 3 (MIL3)
En el MIL3, las actividades en un dominio se han institucionalizado y se gestionan. Cinco

12 ANEXO A: RESUMEN DEL MODELO ES-C2M2

prácticas de gestión respaldan esta progresión:

1. Las actividades están guiadas por políticas (u otras directrices organizacionales) y gobernanza. Las actividades administradas en un dominio reciben orientación de la organización en forma de dirección organizativa, como en políticas y gobierno. Las políticas son una extensión de las actividades de planificación que existen en el MIL2.
2. Las políticas incluyen requisitos de cumplimiento de normas y/o pautas específicas.
3. Las actividades se revisan periódicamente para garantizar que se ajustan a la política.
4. La responsabilidad y la autoridad para realizar las prácticas se asignan al personal.
5. El personal asignado tiene habilidades y conocimientos adecuados específicos del dominio para realizar sus tareas.

En el MIL3, las prácticas en un dominio se estabilizan aún más y se guían por directrices organizacionales de alto nivel, como la política. Como resultado, la organización debe tener una confianza adicional en su capacidad para mantener el desempeño de las prácticas a lo largo del tiempo y en toda la institución.

El ES-C2M2 está destinado para ser utilizado por una organización para evaluar sus capacidades de ciberseguridad de manera consistente, para comunicar sus niveles de capacidad en términos significativos e informar la priorización de sus inversiones en ciberseguridad. La Figura 6 resume el enfoque recomendado para usar el modelo. Una organización realiza una evaluación contra el modelo, usa esa evaluación para identificar los gaps en una determinada capacidad, prioriza esos gaps y desarrolla planes para abordarlos. A medida que se implementan los planes, los objetivos comerciales cambian y el entorno de riesgo evoluciona, el proceso se repite.

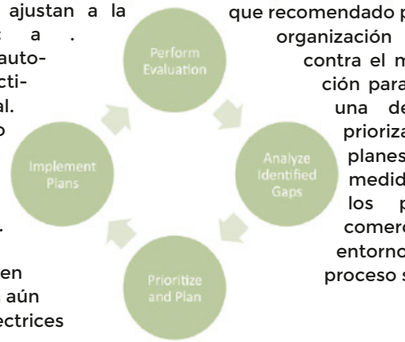


Figure 6: Recommended Approach for Using the Model

Fuente: ES-C2M2, https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

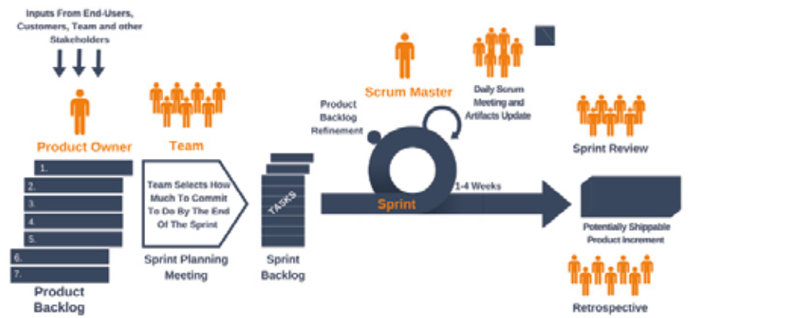
Table 4: Recommended Process for Using Evaluation Results

	Inputs	Activities	Outputs
Perform Evaluation	1. ES-C2M2 Self Evaluation 2. Policies and procedures 3. Understanding of cybersecurity program	1. Conduct ES-C2M2 Self Evaluation Workshop with appropriate attendees	ES-C2M2 Self Evaluation Report
Analyze Identified Gaps	1. ES-C2M2 Self-Evaluation Report 2. Organizational objectives 3. Impact to critical infrastructure	1. Analyze gaps in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention	List of gaps and potential consequences
Prioritize and Plan	1. List of gaps and potential consequences 2. Organizational constraints	1. Identify actions to address gaps 2 Cost-benefit analysis (CBA) on actions 3. Prioritize actions (CBA and consequences) 4. Plan to implement prioritize actions	Prioritized implementation plan
Implement Plans	1. Prioritized implementation plan	1. Track progress to plan 2. Reevaluate periodically or in response to major change	Project tracking data

Fuente: ES-C2M2, https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

ANEXO B: WORKING GROUP CIBERSEGURIDAD CIGRE CHILE 13

El trabajo colaborativo fue realizado en modalidad presencial según la planificación inspirada en la Metodología Agile distribuyendo el trabajo en tres células, legal, normativa técnica y Gobierno (tecnología-procesos-personas). Estos grupos tuvieron como objetivo generar entregables de avance en tres sprint previamente definidos en pro de la obtención del documento final de recomendaciones y plan director. Dentro de la metodología, se consideró la invitación de especialistas del sector eléctrico, gubernamental u otros que proporcionaran una visión más amplia. De este modo, se destacan las reuniones con el senador Kenneth Pugh y con Mario Farren del Ministerio del Interior, que aportaron valor al análisis y a la calidad del documento final.



- **Scrum Muster:** Líder WG Ciberseguridad CIGRE Chile
- **Product Owner:** Líderes de cada célula
- **Team:** Especialistas y observadores

Fuente: Agile Methodology: Revolutionizing Project Management, https://medium.com/@rromanss23/agile-methedology-revolutionizing-project-management-91636775191d

13 ANEXO B: WORKING GROUP CIBERSEGURIDAD CIGRE CHILE

A continuación, se presenta el listado conformado por los participantes de las sesiones periódicas, ya sea como especialistas u observadores, del Grupo de Trabajo de Ciberseguridad de CIGRE Chile, a quienes se agradece por su importante contribución con ideas, observaciones, comentarios y objeciones, entre otras, para este proceso de análisis e investigación en torno a la ciberseguridad del sector eléctrico.

Eduardo Morales Cabello (Especialista - Líder WG Ciberseguridad) ENTEL S.A.

Alejandra Caro Troncoso (Especialista - Líder Célula Legal) EDF
Fernando Muñoz A. (Especialista - Líder Célula Normativa Técnica) Saesa
Constanza Levicán Torres (Especialista - Líder Célula Gobierno) Suncast

ESPECIALISTAS:

Jerson Reyes Sánchez (CNE)
Alvaro Acoria González (CEN)
Roxana Varela Otárola (SEC)
Oscar Álamos Guzmán (Ministerio de Energía)
Javiera Ketterer (Empresas Eléctricas AG.)
Mireya Isabel Pérez Martínez (Fluor Chile)
Christians Espinoza Roga (EEPA)
Fabián Serradell Díaz (Integración Sistemas S.A.)
Frandimar Belisario (Celeo Redes Chile)
Nicolás Ramos Giannini (Celeo Redes Chile)
Giovanni Guzmán (Saesa)
Daniel Soto Alquinta (CGE Naturgy)
Maria Cristina Sanhueza Bustamante (ENEL)
Miguel Torres N. (Transelec)
Natalio Schonhaut B. (IACEL SpA)
Paola Cortés Auger (Eléctrica Puntilla)
Rodrigo Moyano Colipe (Renea Chile SPA)
Gustavo Masman Paredes (Latin America Power S.A.)

OBSERVADORES:

Andrés Jauregui Cabrera (SEC)
Francisco Balcázar González (SEC)
Hans Rother Salazar (ENEL)
Héctor Ubal Leyton (ENEL)
Rodrigo Apablaza (ENEL)
Rodrigo Velásquez Salazar (ENEL)
Filippo Gentili (ENEL)
Doris Herrera Ferrada (Chilquinta)
Cristián Muñoz Catalán (ABB)
Daniel Andrade Mancilla (ABB)
Mauricio Moran Concha (Colbún)
Sebastián Celis Cáceres (Colbún)
Jaime Berrios Maturana (Comulsa)
Víctor Ballivián (IEC Chile)
Guillermo Parada Milanese (Cornelec)
Oscar Guarda Ríos (TEN S.A.)
Roberto Díaz M. (Prosus Corp)
Yerko Pincheira Sánchez (Prosus SPA)
Ali Lobo Uzcategui (IM3)
Carlos Jaureche (Security Advisor Chile)
Gonzalo Fuentes Rojas (Underfire S.A.)

cigre Chile

PLAN DIRECTOR de CYBER SEGURIDAD

para el Sector Eléctrico

2021 – 2023