ASOCIACIÓN DE EMPRESAS DE PETRÓLEO, GAS Y ENERGÍA RENOVABLE DE AMÉRICA LATINA Y EL CARIBE

Benchmarking de Madurez en Ciberseguridad Industrial en la industria petrolera y del gas para América Latina y el Caribe

Estadísticas 2021 y 2022 de las empresas socias de ARPEL

Agosto, 2023

PUBLICACIÓN ARPEL N° EJ03-2023

BENCHMARKING

ASOCIACIÓN DE EMPRESAS DE PETRÓLEO, GAS Y ENERGÍA RENOVABLE DE AMÉRICA LATINA Y EL CARIBE

"En memoria de Hernán Vázquez, creador del Grupo de Trabajo de Ciberseguridad de ARPEL, ideólogo e impulsor del proyecto Indicador de Madurez en Ciberseguridad Industrial"

Benchmarking de Madurez en Ciberseguridad Industrial en la industria petrolera y del gas para América Latina y el Caribe

Estadísticas 2021 y 2022 de las empresas socias de ARPEL

Agosto 2023

Autor

El presente informe fue preparado a solicitud de ARPEL y su Comité de Ciberseguridad Industrial, por el consultor Ing. Gerardo F. González Gionchetti (Gerardo.f@gonzalezgionchetti.ar)
Revisión
Comité de Ciberseguridad Industrial
- Ing. Javier F. Castillo (YPF)
- Ing. Ernesto Landa (TGP)
- Lic. Pablo Amoedo (ARPEL)

Derechos de autor

Los derechos de autor de este documento, ya sea en su versión impresa o digital son propiedad de la Asociación Regional de Empresas del Sector Petróleo, Gas, y Biocombustibles en Latinoamérica y el Caribe (ARPEL). Cualquier copia de este trabajo protegido deberá incluir esta nota sobre los derechos de autor.

Exoneración de responsabilidad

A pesar de haberse realizado esfuerzos para garantizar la exactitud de la información contenida en este documento, ni ARPEL, ni ninguno de sus socios, autores o revisores, ni las empresas e instituciones que ellos representan, asumen responsabilidad alguna por cualquier uso que se haga del mismo. Ninguna referencia a nombres o marcas registradas de fabricantes de equipos y/o procesos representa un endoso de parte de los autores, ARPEL o cualesquier de sus socios.

01
Tabla de contenidos

01. Prólogo **4**

02. Introducción: Comité de Ciberseguridad Industrial **5**

03. Desarrollo: El Modelo C2M2 v1.1a **8**

03.1 Arquitectura ONG-C2M2 v1.1a 10

03.2 Dominios 10

03.3 Indicadores de niveles de madurez 13

03.4 Clasificación de las prácticas 14

03.5 Visualización de resultados 16

04. Desarrollo: Metodología utilizada **19**

04.1 La experiencia 20

05. Resultados Obtenidos **21**

05.1 Resultado General de Compliance por MIL 23

05.2 Resultados de cumplimiento por Dominio 25

06. Conclusiones **29**

07. Glosario de términos y acronimos **31**

Prólogo

Madurez…

Quizás el termino madurez parezca trivial y sea un concepto que todos entendemos, pero tal vez interpretamos de manera distinta. Madurar no implica el simple hecho de crecer, es un concepto relacionado al desarrollo pleno de capacidades que pueden ser diferentes según el contexto donde se aplique.

En la actualidad, la creciente interconexión de los sistemas industriales y la adopción de tecnologías digitales mayormente utilizadas en entornos de tecnologías de la información, han brindado enormes beneficios en términos de eficiencia y productividad. Como contrapartida, han aumentado su exposición a ciber amenazas que pueden comprometer la seguridad de los procesos que controlan teniendo impacto directo sobre los cuatro receptores de riesgos: Personas, Medio Ambiente, Finanzas e Imagen Corporativa. Es entonces donde la Ciberseguridad Industrial aparece como disciplina para dar respuesta a este contexto.

Aplicar el concepto de madurez en términos de ciberseguridad industrial consiste en generar las capacidades necesarias para proteger a los procesos industriales desde su componente tecnológica. Para ello es importante la adopción de un modelo que permita las organizaciones poder medirse y compararse con sus semejantes con el fin de entender hacia donde evolucionar, en otras palabras cuales son aquellas capacidades que deben generarse o robustecerse para alcanzar un determinado nivel de madurez objetivo.

Es por ello que dentro de las acciones que desarrollamos dentro del Comité de Ciberseguridad Industrial de ARPEL y apalancados en nuestra misión dentro de la región, hemos acompañado a nuestras empresas socias en la identificación de sus capacidades en Ciberseguridad Industrial y ayudado a construir planes de acción a partir de ellas utilizando como referencia el modelo C2M2 del Departamento de Energía de los Estados Unidos de América.

Como resultado de esta actividad hemos decidido realizar esta publicación con el fin de brindar a los lectores la información necesaria para identificar las capacidades desarrolladas en la región (manteniendo la confidencialidad de la información de nuestros miembros) y poder así situarse y hacer foco sobre aquellas que necesitan acciones concretas para su evolución.

Esperamos sea de utilidad para toda la industria y el primer paso para avanzar en la búsqueda de niveles de madurez adecuados para cada segmento dentro de ella.

Ing. Javier F. Castillo
Presidente Comité de Ciberseguridad Industrial de ARPEL

02
Introducción:
ARPEL y el Comité de Ciberseguridad Industrial

La Asociación Regional de Empresas de Petróleo, Gas y Energías Renovables (ARPEL), es una asociación sin fines de lucro, creada en 1965 con el objeto de promover la integración, la cooperación y la asistencia recíproca entre empresas del sector, para contribuir de manera activa al crecimiento sostenible y a la excelencia operativa de la industria del Gas y del Petróleo en el ámbito de Latinoamérica y el Caribe.

Dentro de ARPEL, existen Comités Técnicos que desarrollan procesos que apuntan a la mejora continua, partiendo del intercambio de mejores prácticas, normas internacionales y bases de conocimiento en foros de diálogo. Con las ideas y propuestas que surgen, se elaboran y editan Guías y Manuales en los cuales las empresas socias pueden basarse para enriquecer sus modelos de negocio. Además, contribuyen a brindar acciones de concientización y capacitación, y también apoyo técnico a los socios para la implementación efectiva de estas mejores prácticas.

De estos mismos comités surge información para la realización de estudios de contraste (Benchmarking), los cuales tienen como fin medir y comparar la evolución en la performance de las empresas socias, y acompañarlas en un proceso de mejora continua.

Los Comités Técnicos funcionan con apoyo de la Secretaría Ejecutiva de ARPEL que hace posible estas acciones interdisciplinarias dentro de una comunidad enfocada en la industria del Gas, del Petróleo y de las Energías Renovables.

El Grupo de Trabajo de Ciberseguridad Industrial, hoy **Comité de Ciberseguridad Industrial**, fue creado en 2015 por iniciativa del Gerente de Informática, Ciberseguridad y Digitalización de ARPEL, Hernán Vázquez y el apoyo de una de las principales empresas socias de ARPEL: YPF de Argentina.

Hoy está conformado por expertos en la temática que trabajan en las empresas de petróleo y gas de América Latina y el Caribe, y su principal objetivo es mitigar los ciber riesgos y remediar las vulnerabilidades ante amenazas emergentes y de alto potencial.

En una industria en donde la digitalización está abarcando un espectro cada vez más amplio de los procesos operativos, el Comité de Ciberseguridad Industrial fue concebido para colaborar en el desarrollo de una estrategia de Ciberseguridad Industrial, que sea capaz de acompañar este proceso de transformación, promoviendo la sinergia entre sus miembros y dotando a la comunidad ARPEL de una mejor y mayor protección frente a Ciber Amenazas.

Con este objetivo en mente se han impulsado fuertemente distintas iniciativas de capacitación, concientización, talleres prácticos, eventos, asesoramiento y consultoría especializada, no solo de Latinoamérica sino también de América del Norte y Europa.

Este Comité es transversal a todas las unidades de negocio y operaciones de la cadena de valor de la industria de petróleo y gas, y se focaliza en la protección de las personas, el cuidado del medio ambiente y en velar por la resiliencia de los procesos productivos del sector desde su componente tecnológica en todo aquello que implique ciber riesgos, vulnerabilidades y/o amenazas que puedan explotar las mismas en los ambientes tecnológicos de IT y en especial en el mundo OT.

El Comité de Ciberseguridad Industrial mantiene encuentros trimestrales, aumentando su frecuencia ante eventos o a demanda de algunas de las empresas socias por temas específicos.

Dentro del Comité, se han definido la Misión y Visión con el fin de tener siempre presentes los objetivos del mismo, la manera de estar cerca de las necesidades de las empresas socias y sus estrategias de crecimiento y desarrollo futuro.

Misión

Contribuir a la madurez y mejora continua de la Ciberseguridad Industrial en las empresas socias, siendo un equipo colaborativo en todos los dominios y sus especialidades, promoviendo la Capacitación y Concientización, como la acción e implementación de contramedidas y mejoras, impulsando el concepto de SEGURIDAD DESDE EL DISEÑO.

Visión

Ser líderes en Ciberseguridad industrial y referentes del sector del Petróleo y el Gas, acompañando la estrategia de las empresas socias con medidas y actitud de prevención, vigilancia y resiliencia que potencien y aseguren la continuidad de su negocio, priorizando la seguridad de las personas, el medio ambiente y los procesos.

Como corolario de la Misión y Visión expuesta, se desprende:

- Promover acciones de colaboración para el desarrollo de una estrategia de Ciberseguridad Industrial, mediante el establecimiento de sinergias varias, dotando a la comunidad ARPEL de una mejor y mayor protección.
- Articular y cohesionar un entorno de colaboración mutuo que, a través de diferentes líneas de acción, generen valor agregado en la Ciberseguridad para las empresas socias de ARPEL.
- Compartir información y experiencias, en un marco de estricta confidencialidad, agregando valor a las empresas socias en sus procesos de prevención
- Diseñar y desarrollar políticas, mejores prácticas y procedimientos de Ciberseguridad Industrial que aumenten el valor agregado y la madurez de las empresas socias de ARPEL, acompañando a sus referentes en la implementación efectiva de la misma
- Buscar la “Seguridad desde el diseño” como establece la norma internacional IEC62443 que el Comité de Ciberseguridad Industrial ha adoptado como columna vertebral de la Ciberseguridad Industrial, ya que la misma es adoptada en diferentes industrias como un nuevo estándar.

Desde su creación, el comité de Ciberseguridad Industrial ha tenido una vasta actividad realizando Seminarios, Talleres y capacitación promoviendo la Ciberseguridad Industrial. Para ello ha realizado convenios y asociaciones con organismos como la OEA, el Centro de Ciberseguridad Industrial (CCI) con base en España y con el fuerte apoyo de empresas socias.

A continuación, se enumeran los principales talleres, seminarios y eventos realizados, de los cuales se puede encontrar información en la página Web de ARPEL.

- 2015 - Creación del **Grupo de Trabajo de Ciberseguridad Industrial** dentro de ARPEL
- Junio 2016 – Webinar – **La Ciberseguridad Empresarial. Conceptos y retos**
- Octubre 2016 - 1er Seminario **"La Ciberseguridad en infraestructuras críticas frente a un mundo tecnológicamente dependiente e interconectado"** en conjunto con la OEA y Cancillería Argentina, llevado a cabo en forma presencial en el Palacio San Martin, Buenos Aires, Argentina.
- Abril 2017 – En la **Reunión Anual de ARPEL** para CEOs (Pta del Este, Uruguay) se incluye en la agenda el tema de ciber industrial
- Mayo 2017 – Taller **"Herramienta de evaluación de madurez del proceso de ciberseguridad en organizaciones industriales"** organizado junto al Centro de Ciberseguridad Industrial (CCI) de España. Dictado en las instalaciones de YPF S.A., Buenos Aires, Argentina
- Agosto 2017 – 2do Seminario **"Fundamentos de la ciberseguridad industrial"**, llevado a cabo en YPF S.A., Buenos Aires, Argentina.
- Abril 2018 - Curso IC10 **"Introducción a la Ciberseguridad Industrial"** dictado por Wiseplant en Buenos Aires, Argentina.
- Julio 2018 – Curso IC33 **"Ciberseguridad en Infraestructuras Críticas, Riesgos, Oportunidades y Prioridades"**, dictado por Wiseplant en Buenos Aires, Argentina.
- Octubre 2018 - 3er Seminario **"Ciberseguridad en Infraestructuras Críticas, Riesgos, Oportunidades y Prioridades"** en conjunto con la OEA, llevado a cabo en Buenos Aires, Argentina (UCA Puerto Madero)
- Diciembre 2018 – Documento I3 **"Cautivando el interés de la junta directiva en los temas de Ciberseguridad"**
- Abril 2019 – Webinar **"Ciberseguridad en Infraestructuras Críticas, Riesgos, Oportunidades y Prioridades"**
- Septiembre 2019 – Curso **"Diseño de Escenarios en Seguridad y Ciberseguridad"** con Jeimy Cano. Dictado en las instalaciones de YPF S.A., Buenos Aires, Argentina
- Abril 2020 – Curso **"Identificación de riesgos con el ZCM"** dictado por Wiseplant, en forma virtual. Ya en contexto de pandemia mundial.
- Marzo 2021 - Proyecto **"Medición de madurez en Ciberseguridad Industrial basado en el modelo C2M2"** (Primera edición). Virtual en plataformas tecnológicas de ARPEL.
- Marzo 2022 - Proyecto **"Medición de madurez en Ciberseguridad Industrial basado en el modelo C2M2"** (Segunda edición). Virtual en plataformas tecnológicas de ARPEL.
- Agosto 2022 – 1er **Panel de intercambio y reflexión** – Safety & Security
- Septiembre 2022 – Charla de intercambio de mejores prácticas - **"La cadena de suministro industrial como eslabón débil de la ciberseguridad"** por José Valiente CCI de España.
- ***Noviembre 2022 – Se oficializa la creación del Comité de Ciberseguridad Industrial***
- Noviembre 2022 - 2do Panel de intercambio y reflexión – **Ciber riesgos Industriales**
- Marzo 2023 – 3er Panel de intercambio y reflexión – **La importancia de los Modelos de madurez**
- Abril 2023 – Curso 2151 – **"Gestión de la Ciberseguridad Industrial para Gerentes de Proyecto"** dictado por WisePlant en forma virtual.

03
Desarrollo:
El Modelo C2M2 v1.1a

Como continuidad de los eventos y otras acciones realizadas por el Comité de Ciberseguirdad Industrial, se decidió armar un proyecto con acciones que sean efectivas y sirvan a las empresas socias para mejorar, o directamente diseñar un Plan de Acción y/o Programa de Ciberseguridad. El mismo debía basarse en las mejores prácticas y normas internacionales que desde ARPEL se estaban ya fomentando y concientizando a partir de la creación del Comité de Ciberseguridad Industrial.

Habiendo realizado entre 2016 y 2019 varios seminarios, talleres y capacitaciones especificas en asociación con organismos de la talla de CCI (Centro de Ciberseguridad Industrial), OEA (Organización de Estados Americanos), Ministerio de Modernización y Cancillería Argentina, entre otros; fue que, en 2020, desde la Gerencia de Tecnología de ARPEL, se confeccionó el siguiente proyecto de diagnóstico y evaluación de la madurez en ciberseguridad industrial.

El objetivo de este es brindar a las empresas miembro el primer paso para una medición rápida y efectiva del Nivel de madurez en Ciberseguridad Industrial. Entregarles como resultado un diagnóstico y un plan de acción sugerido, concreto, con acciones particulares de corto plazo y eficaces para cada empresa participante.

Además, ARPEL se propuso consolidar los resultados y crear un índice (propio de ARPEL) con el fin de definir una línea base o patrón de referencia de madurez para la industria del Petróleo y el Gas, dado que no existen antecedentes en la región.

De esta manera, dentro de la industria del Petróleo y del Gas podremos conocer el estado de situación real actual, bajo un criterio unificado por ARPEL, que nos permitirá actuar en consecuencia para implementar las contramedidas necesarias que permitan evolucionar en la madurez de Ciberseguridad Industrial de cada empresa con el objeto de tener mayores y mejores herramientas para gestionar el Ciber Riesgo.

El Comité de Ciberseguridad Industrial concibe la Ciberseguridad como la Gestión de los Ciber Riesgos asociados a los activos (físicos y virtuales) y procesos de producción, por lo que este primer diagnóstico es el paso fundamental para dar comienzo a una Gestión de Ciber riesgos ordenada y sólida. De esta manera se reduce la exposición a amenazas en las instalaciones industriales en plena era de la digitalización e hiper conectividad, así como también nos permitirá estar un paso adelante para futuras exigencias legales y comerciales que son inminentes en todo Latinoamérica, lo que redundrá de forma directa en la reducción de costos, como por ejemplo en el caso de las pólizas de ciber riesgos.

Los valores diferenciales de ARPEL, como ser la mutua cooperación y confidencialidad para con las empresas socias, hace que sea el entorno y contexto ideal para establecer una metodología y proceso para la obtención de medidas estándares de la industria en el campo de ciber riesgos y Ciberseguridad Industrial.

En consecuencia, se definió que las empresas socias que deseasen participar de forma libre y gratuita de dicha medición, recibieran un informe de análisis global de la madurez y además uno segmentado por dominio (y por objetivos dentro de los mismos) identificando fortalezas, debilidades y acciones de mejora en el corto y mediano plazo.

Gracias a la participación de las empresas socias es que ARPEL puede confeccionar hoy este informe y mostrar el primer resultado de Indicador de Madurez en Ciberseguridad Industrial (IMCI) .

El 20 de abril de 2021 lanzó oficialmente al proyecto en el marco de una reunión trimestral del Comité de Ciberseguridad. Allí se presentó el modelo a utilizar para la medición de madurez, así como la metodología y los entregables que recibiría cada empresa socia participante del proyecto.

Ciclo de evolución de Madurez cibernética

La idea y objetivo principal de este proyecto es la de realizar una evaluación del **"estado actual de la salud cibernética"** de cada empresa y realizar un análisis de las brechas encontradas, dejando en manos de cada empresa la priorización de estas, su planificación de remediación y ejecución.

El modelo elegido fue el desarrollado por el Departamento de Energía (DoE) del Homeland Security (DHS) de EE. UU, que ha desarrollado dos modelos, uno para el subsector de Energía (ES-C2M2) y el otro para Petróleo y Gas (ONG-C2M2).

Dada la industria principal de las empresas socias de ARPEL es que se adoptó este último modelo.

Siguiendo el ciclo de evolución de la madurez en ciberseguridad industrial propuesto y descrito anteriormente, a continuación, se expresan más en detalle las entradas, actividades y salidas de cada una de estas etapas, siendo las dos últimas las que quedan particularmente en manos de cada una de las empresas socias que hayan realizado la evaluación para su desarrollo y ejecución.

	INPUTS	ACTIVIDADES	OUTPUTS
Evaluación de desemeño	1. Evaluación C2M2 2. Políticas y procedimientos 3. Comprensión de programa de ciberseguridad	1. Ejecución de la evaluación C2M2	Informe final de resutados C2M2
Análisis de GAPs identificados	1. Informe final de resultados C2M2 2. Objetivos de la organización 3. Impacto para IICC	1. Analizar los GAPs en el contexto de la organización 2. Evaluar las potenciales consecuencias 3. Determinar los GAPs prioritarios	Listado de GAPs y principales consecuencias
Priorizar y Planificar	1. Listado de GAPs y principales consecuencias 2. Restricciones organizacionales	1. Identificar acciones para el manejo de GAPs 2. Análisis de costo beneficio de las acciones 3. Priorizar acciones 4. Planificación ejecución de acciones	Plan de implementación priorizado
Implementación del Plan	1. Plan de implementación priorizado	1. Seguimiento de ejecución del Plan 2. Re evaluación periódica en base a cambios	Datos de seguimiento del plan

ARPEL, a través de este proyecto, ha realizado la ejecución de las primeras dos etapas, entregando un informe detallado de la ejecución del ONG-C2M2 v1.1a conteniendo un análisis de brechas por cada dominio y sugiriendo una priorización de estas.

A continuación, se describen las características básicas de este modelo, denominado ONG-C2M2 (Oil and Natural Gas - Cibersecurity Capability Maturity Model) v1.1a, para luego pasar a los resultados obtenidos, su interpretación y conclusiones.

03.1

Arquitectura ONG-C2M2 v1.1a

El modelo ONG-C2M2 surge de una combinación de estándares, marcos de ciberseguridad, mejores prácticas, programas e iniciativas de seguridad cibernética ya existentes. ONG-C2M2 proporciona una guía flexible para ayudar a las organizaciones ordenar, diseñar, desarrollar y mejorar sus capacidades en Ciberseguridad. Como resultado, las prácticas que componen el modelo ONG-C2M2 están desarrolladas en un alto nivel de abstracción, que pueden interpretarse para organizaciones de diferentes estructuras y tamaños, lo cual da mayor versatilidad a este modelo.

El modelo ONG-C2M2 está organizado en 10 dominios. Cada dominio es una agrupación lógica de mejores y habituales prácticas de Ciberseguridad. Las prácticas dentro de un dominio están, a la vez, agrupadas por objetivos dentro de cada dominio. Luego, dentro de cada objetivo, las prácticas están ordenadas por MIL (Maturity Indicator Levels), es decir, por nivel de madurez al cual pertenecen.

En los próximos puntos veremos el detalle de esta arquitectura para comprenderla mejor y poder entender sus resultados.

03.2

Dominios

Cada uno de los 10 dominios de ONG-C2M2 v1.1a contiene un conjunto estructurado de mejores prácticas de Ciberseguridad. Cada conjunto de mejores prácticas representa las actividades que una organización puede realizar para establecer y desarrollar capacidades dentro de dicho dominio.

Por ejemplo, el dominio de Gestión de Riesgos es un grupo de mejores prácticas que una organización puede realizar para establecer y evolucionar la capacidad de administración de riesgos de ciberseguridad.

Para cada dominio, ONG-C2M2 proporciona una declaración de propósito, que no es más que un resumen de alto nivel de la intención de dicho dominio. La declaración de propósito ofrece un contexto para interpretar las mejores prácticas en el dominio.

Estas prácticas dentro de cada dominio están organizadas en objetivos, que representan logros que contribuyen a la madurez dentro del dominio.

Por ejemplo, el dominio de Gestión de Riesgos comprende tres objetivos:

1. Establecer una estrategia de gestión de riesgos de ciberseguridad
2. Gestionar el riesgo de ciberseguridad
3. Prácticas de la Gestión

Cada uno de los objetivos en un dominio comprende un conjunto de mejores prácticas, que están ordenadas por nivel de madurez (MIL)

La figura siguiente muestra la arquitectura definida del ONG-C2M2.

Arquitectura del modelo

A continuación, se describe cada uno de los 10 dominios, en el orden en que aparecen en el modelo ONG-C2M2 v1.1a e identificados con su sigla en inglés. En el futuro nos referiremos a cada dominio a través de su sigla de identificación.

Gestión de riesgos (RM)

Establecer, operar y mantener un programa empresa de gestión de riesgos de ciberseguridad para identificar, analizar y mitigar los riesgos de ciberseguridad para la organización, incluyendo a sus unidades de negocio, empresas subsidiarias, infraestructura interconectada relacionada y partes interesadas.

Gestión de activos, cambios y configuración (ACM)

Gestionar los activos de tecnología de la operación (OT) y de tecnología de la información (TI) de la organización, incluyendo tanto hardware como software, acorde con el riesgo para la infraestructura crítica y los objetivos de la organización.

Gestión de Identidad y Acceso (IAM)

Crear y administrar las identidades para todas las entidades a las que se les puede conceder acceso, ya sea lógico o físico, a los activos de la organización. Controlar el acceso a dichos activos acorde con el riesgo para la infraestructura crítica y los objetivos de la organización.

Gestión de amenazas y vulnerabilidad (TVM)

Establecer y mantener planes, procedimientos y tecnologías para detectar, identificar, analizar, gestionar y responder a las amenazas y vulnerabilidades de la ciberseguridad, de acuerdo con el riesgo para la infraestructura de la organización (p. ej., crítica, TI, operativa) y los objetivos de la organización.

Concientización de la situación (SA)

Establecer y mantener actividades y tecnologías para recopilar, analizar, alertar, presentar y utilizar información operativa y de ciberseguridad, incluyendo información de estado y resumen de los otros dominios de ONG-C2M2, para formar una imagen operativa común (COP).

Intercambio de información y comunicaciones (ISC)

Establecer y mantener relaciones con entidades internas y externas para recopilar y proporcionar información sobre ciberseguridad, incluidas amenazas y vulnerabilidades, a fin de reducir los riesgos y aumentar la capacidad de recuperación operativa, en consonancia con el riesgo para la infraestructura crítica y los objetivos de la organización.

Respuesta a Eventos e Incidentes, Continuidad de Operaciones (IR)

Establecer y mantener planes, procedimientos y tecnologías para detectar, analizar y responder a los eventos de ciberseguridad y mantener las operaciones a lo largo de un evento de ciberseguridad, de acuerdo con el riesgo para la infraestructura crítica y los objetivos de la organización.

Gestión de la cadena de suministro y de dependencias externas (EDM)

Establecer y mantener controles para gestionar los riesgos de ciberseguridad asociados a los servicios y activos que dependen de entidades externas, en consonancia con el riesgo para la infraestructura crítica y los objetivos de la organización.

Gestión del personal (WM)

Establecer y mantener planes, procedimientos, tecnologías y controles para crear una cultura de ciberseguridad y garantizar la idoneidad y competencia permanente del personal, en consonancia con el riesgo para la infraestructura crítica y los objetivos de la organización.

Gestión de programas de ciberseguridad (CPM)

Establecer y mantener un programa de ciberseguridad Empresarial que ofrezca gobernanza, planificación estratégica y patrocinio para las actividades de ciberseguridad de la organización de manera que alinee los objetivos de ciberseguridad con los objetivos estratégicos de la organización y el riesgo para la infraestructura crítica.

Dominios del modelo C2M2

RM Gestión de riesgos	**ACM** Gestión de activos, cambios y configuración	**IAM** Gestión de Identidad y Acceso	**TVM** Gestión de amenazas y vulnerabilidad
SA Concientización de la situación	**ISC** Intercambio de información y comunicaciones	**IR** Respuesta a Eventos e Incidentes, Continuidad de Operaciones	**EDM** Gestión de la cadena de suministro y de dependencias externas
WM Gestión de personal	**CPM** Gestión de programas de ciberseguridad	- Los dominios son agrupaciones lógicas de las prácticas de ciberseguridad - Cada dominio tiene un acrónimo que hacer referencia a la planilla de evaluación	

03.3

Indicadores de niveles de madurez

El modelo ONG-C2M2 v1.1a define cuatro niveles de madurez (MIL=Madurity Indicators Level), MIL0 a MIL3, que se aplican independientemente a cada dominio en la ONG-C2M2.

Cuatro aspectos de los MIL (Madurity Indicators Level) son importantes para comprender y aplicar el modelo ONG-C2M2 v1.1a:

1. Los niveles de **indicador de madurez se aplican independientemente a cada dominio.** Como resultado, una organización que utiliza el modelo ONG-C2M2 puede estar operando en 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 **MIL 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 predecesores. Por ejemplo, una organización debe realizar todas las prácticas de dominio en MIL1 y MIL2 para lograr MIL2 en el dominio. De manera similar, la organización tendría que realizar todas las prácticas en MIL1, MIL2 y MIL3 para lograr MIL3.

3. **Establecer una MIL objetivo** para cada dominio es una estrategia efectiva para usar la ONG-C2M2 con el fin de guiar la mejora del Programa de Ciberseguridad. Las organizaciones deben familiarizarse con las prácticas del modelo ONG-C2M2 antes de determinar los MILs objetivos. Las actividades de análisis de brechas y los esfuerzos de mejora deben centrarse en alcanzar esos niveles objetivo.

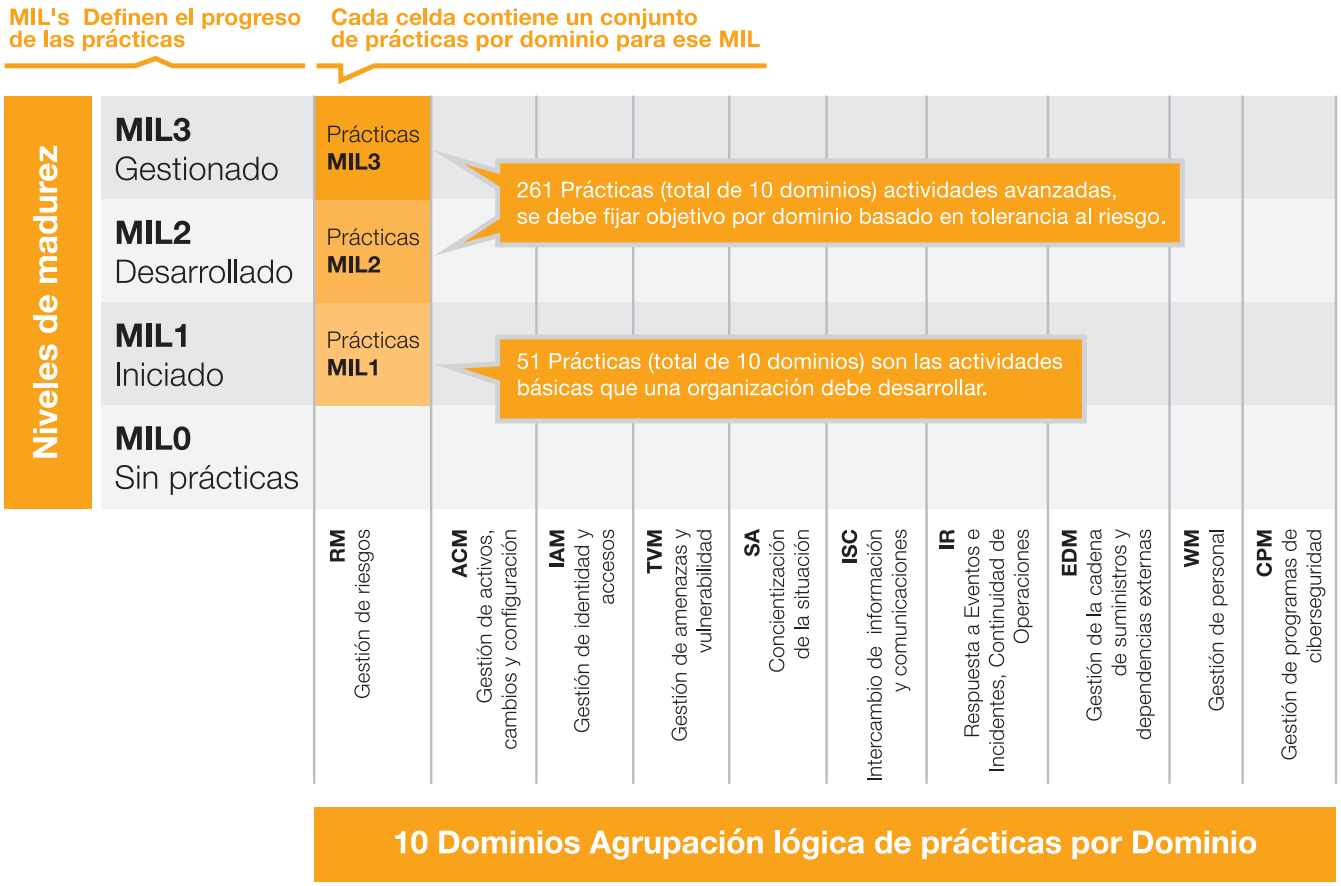
4. El desempeño de la práctica y el **logro de MIL deben alinearse con los objetivos comerciales y la estrategia de ciberseguridad de la organización.** El esfuerzo por lograr el MIL más alto en todos los dominios puede no ser óptimo. Las empresas deben evaluar los costos de lograr un MIL específico frente a los beneficios potenciales (análisis costo/beneficio).

El modelo ONG-C2M2 se desarrolló para que todas las empresas, independientemente de su tamaño, puedan alcanzar el MIL1 en todos los dominios.

En la tabla a continuación se provee una descripción de estos niveles de madurez (MIL):

Nivel	Caracteristicas
MIL0	* Prácticas no desarrolladas ni conocidas
MIL1	* Prácticas iniciadas, aunque sea de manera Ad Hoc
MIL2	* Prácticas documentadas * Stakeholders identificados e involucrados * Se proveen recursos adecuados para soportar los procesos * Existen estándares o guías para la implantación de prácticas
MIL3	* Las actividades son reguladas por políticas, normas y gobernanza * Se incluyen requerimientos de cumplimiento para normas y procedimientos * Se revisan periódicamente las actividades acordes a las políticas y normas * La responsabilidad y autoridad de las prácticas se asignan al personal * El personal desarrolla las prácticas de forma adecuada, con el conocimiento y los skills necesarios

Así, para cada dominio existen una serie de prácticas agrupadas en cada MIL, las que constituyen la base para la interpretación de los resultados de la evaluación de madurez.



03.4

Clasificación de las prácticas

Dentro de cada celda, compuesta por un MIL y un dominio, hay un grupo de prácticas que establecen las actividades a cumplir para alcanzar ese MIL en ese dominio.
Cada una de estas prácticas puede ser respondida como:

- **Full Implemented (FI):** Completada
- **Largely Implemented (LI):** Completada con oportunidades de mejora
- **Partially Implemented (PI):** Incompleta con muchas oportunidades de mejora
- **Not Implemented (NI):** Ausente, Práctica no presente en la organización

Así, respondiendo estas **prácticas**, agrupadas por **objetivos**, dentro de un **dominio**, es que se va conformando el resultado final de esta evaluación.

Una práctica estará completa (FI) cuando se cumpla tal como se presenta en el modelo. Estará con oportunidades de mejora (LI) cuando se cumpla sustancialmente como se describe en el modelo, reconociendo oportunidades de mejora en uno o mas aspectos de la misma para poder cumplir los objetivos organizacionales, de gestión y operativos de cada dominio. Luego, estará parcialmente completa (PI) cuando dichas oportunidades de mejora sean muchas en todos los objetivos de cada dominio. Finalmente, cuando una practica no es conocida o ni siquiera desarrollada ad hoc en la organización, es cuando la misma será calificada como ausente (NI).

Aquí es donde cabe destacar que, dentro del contexto de este modelo, **el término o expresión "ad hoc"** se refiere a realizar una práctica o actividad de una manera tal que depende, en gran medida, de la iniciativa y experiencia de un individuo o de un equipo (con claro liderazgo), sin formalización dentro de la Organización. Los métodos, herramientas y técnicas

utilizadas, la prioridad dada en una instancia o situación en particular y la calidad del resultado pueden variar significativamente dependiendo de quién realiza la práctica. Con personal experimentado y debidamente capacitado, se pueden lograr resultados de alta calidad, aunque las prácticas sean ad hoc.

Sin embargo, debido a que las **lecciones aprendidas** no son asimiladas y documentadas a nivel organizacional, los enfoques y resultados son difíciles de repetir y planificar mejoras en las prácticas de los distintos dominios dentro de la organización. Además, se **pierde conocimiento genuino** de la Organización (pérdida de know how) por no transmitirse el mismo entre las personas y se pierden oportunidades claras de mejora por no compartir y documentarlos. Esto **trae aparejado grandes riesgos "invisibles"** a la Organización que son lamentados y "descubiertos" cuando alguna persona de mucha experiencia deja la compañía (cualquiera sea el motivo) y ya es tarde para mitigarlos.

Como ejemplo, a continuación, se muestra un **grupo de prácticas**, ya respondidas, correspondientes al **Dominio ACM, agrupadas por objetivo** y dentro de ellos **por MIL.**

1. Gestionar inventario de activos		
MIL1	a. Hay un inventario de activos OT y de TI que son importantes para la entrega de la función; la gestión del inventario puede ser ad hoc.	LI
	b. Hay un inventario de activos de información que son importantes para la entrega de la función (por ejemplo, puntos de ajuste SCADA, información del cliente, datos financieros); la gestión del inventario puede ser ad hoc.	LI
MIL2	c. Los atributos del inventario incluyen información para respaldar la estrategia de ciberseguridad (por ejemplo, ubicación, propietario del activo, requisitos de seguridad aplicables, dependencias del servicio, acuerdos de nivel de servicio y conformidad de los activos con los estándares relevantes de la industria)	PI
	d. Los activos inventariados se priorizan según su importancia para la entrega de información.	PI
MIL3	e. Existe un inventario de todos los activos de TI y OT relacionados con la entrega de la función.	PI
	f. El inventario de activos es actual (como define la organización)	LI
2. Gestionar la configuración de activos		
MIL1	a. Las líneas de base de configuración se establecen al menos de manera ad hoc, para los activos inventariados en los que es conveniente garantizar que los activos múltiples se configuren de manera similar.	PI
	b. Las líneas base de configuración se utilizan, al menos de manera ad hoc, para configurar los activos en despliegue.	PI
MIL2	c. El diseño de líneas de base de configuración incluye objetivos de ciberseguridad	NI
MIL3	d. La configuración de los activos se monitorea para mantener la coherencia con las líneas de base a lo largo del ciclo de vida de los activos	PI
	e. Las líneas de base de configuración se revisan y actualizan con una frecuencia definida por la organización.	PI
3. Gestionar cambios en los activos		
MIL1	a. Los cambios en los activos inventariados se evalúan al menos de manera ad hoc, antes de ser implementados	LI
	b. Los cambios de los activos inventariados se registran al menos de manera ad hoc.	LI
MIL2	c. Los cambios de los activos se prueban antes de ser implementados, siempre que sea posible.	PI

03.5

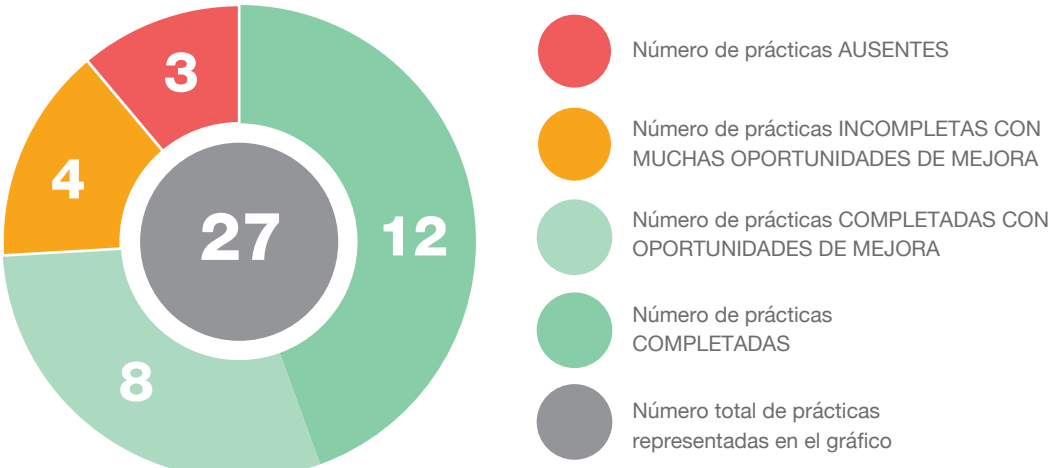
Visualización de resultados

Finalmente llegamos al punto de comprender los resultados obtenidos para esa “foto” de la salud en madurez cibernética de cada empresa.

Teniendo en cuenta los puntos anteriores, vemos que hay varios cortes o vistas para analizar los resultados y eso es lo que mas enriquece este modelo ya que nos permite encontrar Quick Wins, es decir, acciones rápidas de mejora.

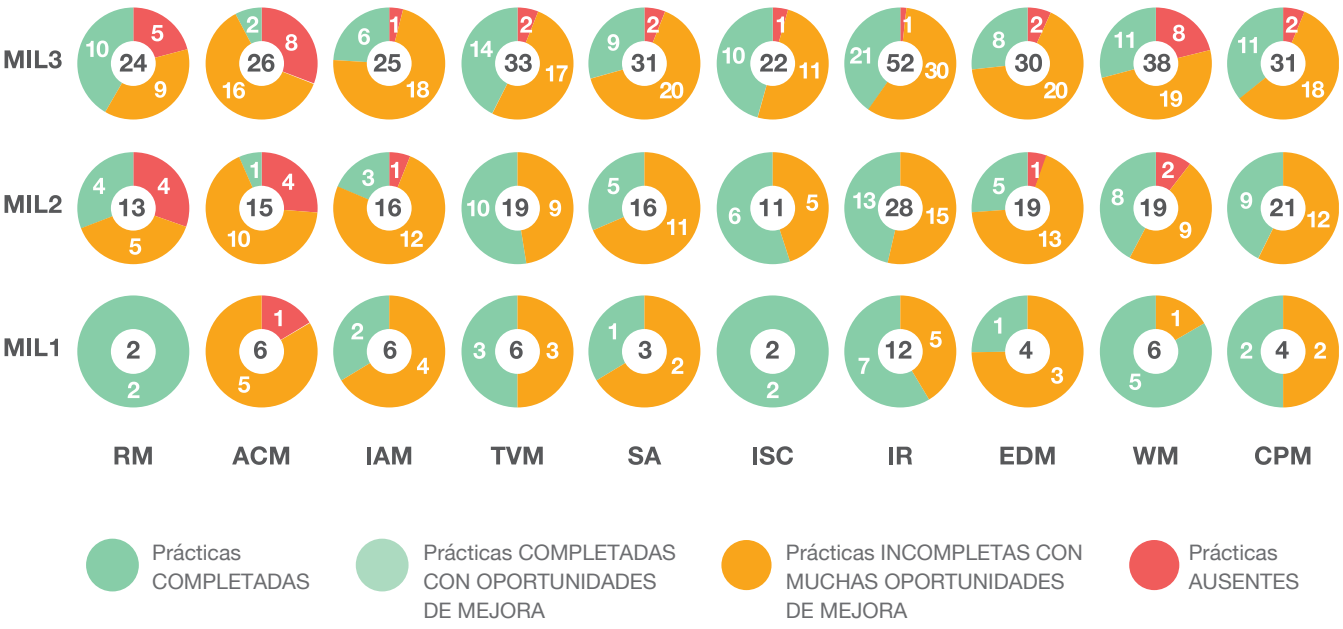
Ahora veremos ejemplos de diversas formas de interpretar los resultados y luego, en el próximo apartado, veremos los resultados generales asociados al Indicador de Madurez en Ciberseguridad Industrial (IMCI) .

Una vez respondidas todas las prácticas de los 10 dominios, obtenemos un resultado final visual constituido por “donas” (donuts) de la siguiente manera



En la misma se identifican las 4 posibles calificaciones para cada práctica (en los colores verde oscuro, verde claro, naranja y rojo oscuro) y la cantidad de prácticas en dicha calificación. En el centro de la misma se observa el total de prácticas para ese dominio en ese MIL.

De esta manera es fácil ver el nivel de cumplimiento en cada dominio y MIL y a la vez en forma general. Si llevamos estas donas a una matriz constituida por los dominios y los MIL, observamos en términos generales el resultado de la evaluación, como vemos a continuación:



Aquí vemos una matriz compuesta por los 10 dominios (identificados por su sigla) en las abscisas y los MIL en las ordenadas. Cada celda esta representada por una de las donas descritas. Tener en cuenta que los niveles MIL2 y MIL3 son acumulativos, por lo que el total de prácticas dentro de esas respectivas donas incluye a las practicas del nivel anterior.

Vemos en el gráfico que para el MIL1 tenemos completados los dominios RM, ACM e ISC. Mientras que, para el MIL2, solo el ACM y ninguno para MIL3.

Resumimos en la siguiente tabla los puntos salientes de la estructura del modelo descrito.

Dominio		Descripción del dominio
RM	**Gestión de riesgos**	Establecer, operar y mantener un programa de gestión de riesgos de ciberseguridad empresarial para identificar, analizar y mitigar el riesgo de ciberseguridad para la organización, incluidas sus unidades comerciales, subsidiarias, infraestructura interconectada relacionada y partes interesadas.
ACM	**Gestión de activos, cambios y configuración**	Gestionar los activos de tecnología de operaciones (OT) y tecnología de la información (TI) de la organización, incluido el hardware y el software, de acuerdo con el riesgo para la infraestructura crítica y los objetivos de la organización.
IAM	**Gestión de Identidad y Acceso**	Crear y administrar identidades para entidades a las 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.
TVM	**Gestión de amenazas y vulnerabilidad**	Establecer y mantener planes, procedimientos y tecnologías para detectar, identificar, analizar, gestionar y responder a las amenazas y vulnerabilidades de ciberseguridad, de acuerdo con el riesgo para la infraestructura de la organización (p. ej., crítica, de TI, operativa) y los objetivos de la organización.
SA	**Concientización de la situación**	Establecer y mantener actividades y tecnologías para recopilar, analizar, generar alarmas, presentar y utilizar información operativa y de ciberseguridad, incluido el estado y la información resumida de los otros dominios del modelo, para formar una imagen operativa común (COP).
ISC	**Intercambio de información y comunicaciones**	Establecer y mantener relaciones con entidades internas y externas para recopilar y proporcionar información sobre ciberseguridad, incluidas amenazas y vulnerabilidades, para reducir los riesgos y aumentar la resiliencia operativa, de acuerdo con el riesgo para la infraestructura crítica y los objetivos de la organización.
IR	**Respuesta a Eventos e Incidentes, Continuidad de Operaciones**	Establecer y mantener planes, procedimientos y tecnologías para detectar, analizar y responder a eventos de cibeseguridad y para mantener las operaciones durante un evento de ciberseguridad, de acuerdo con el riesgo para la infraestructura crítica y los objetivos de la organización.
EDM	**Gestión de la cadena de suministro y de dependencias externas**	Establecer y mantener controles para gestionar los riesgos de ciberseguridad asociados con los servicios y activos que dependen de entidades externas, de acuerdo con el riesgo para la infraestructura crítica y los objetivos de la organización.
WM	**Gestión de personal**	Establecer y mantener planes, procedimientos, tecnologías y controles para crear una cultura de ciberseguridad y garantizar la idoneidad y competencia continuas del personal, acorde con el riesgo para la infraestructura crítica y los objetivos de la organización.
CPM	**Gestión de programas de ciberseguridad**	Establecer y mantener un programa de ciberseguridad empresarial que proporcione gobernanza, planificación estratégica y patrocinio para 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.

Definiciones del indicador de nivel de madurez

MIL 1: Iniciado	1.Se realizan prácticas iniciales pero pueden ser ad hoc	
MIL 2: Implementado	1. Prácticas son documentadas	3. Se proporcionan recursos adecuados para apoyar el proceso (personas, financiación y herramientas)
	2. Se identifican e involucran a las partes interesadas de la práctica	4. Se han identificado estándares y/o lineamientos para guiar la implementación de las prácticas.
MIL 3: Gestionado	1. Las actividades están guiadas por políticas (u otras directivas organizacionales) y gobernanza	4. La responsabilidad y la autoridad para realizar las prácticas se asignan al personal.
	2. Las políticas incluyen requisitos de cumplimiento para normas y/o directrices específicas	5. El personal que realiza la práctica tiene las habilidades y conocimientos adecuados.
	3.Las actividades se revisan periódicamente para garantizar que se ajusten a la política.	

Escala de respuesta del instrumento de evaluación

Cada respuesta describe el desempeño de una práctica modelo por parte de la organización

Completamente Implementado	Extensamente implementado	Parcialmente implementado	No implementado
Completo	Completo pero con oportunidades de mejora identificadas	Incompleto con múltiples oportunidades de mejora	Ausente, la práctica no ha sido implementada

No vamos a entrar en mayor nivel de detalle en lo que respecta a las prácticas en sí mismas y la división por objetivos dentro de cada dominio, ya que ese análisis hace mucho a cada empresa en particular y no aporta más información para el índice que estamos buscando generar en ARPEL.

Por tanto, con esta información ya podemos pasar a ver los resultados obtenidos durante 2021 y 2022 con la ejecución de este modelo en varias empresas socias.

04
Desarrollo:
Metodología utilizada

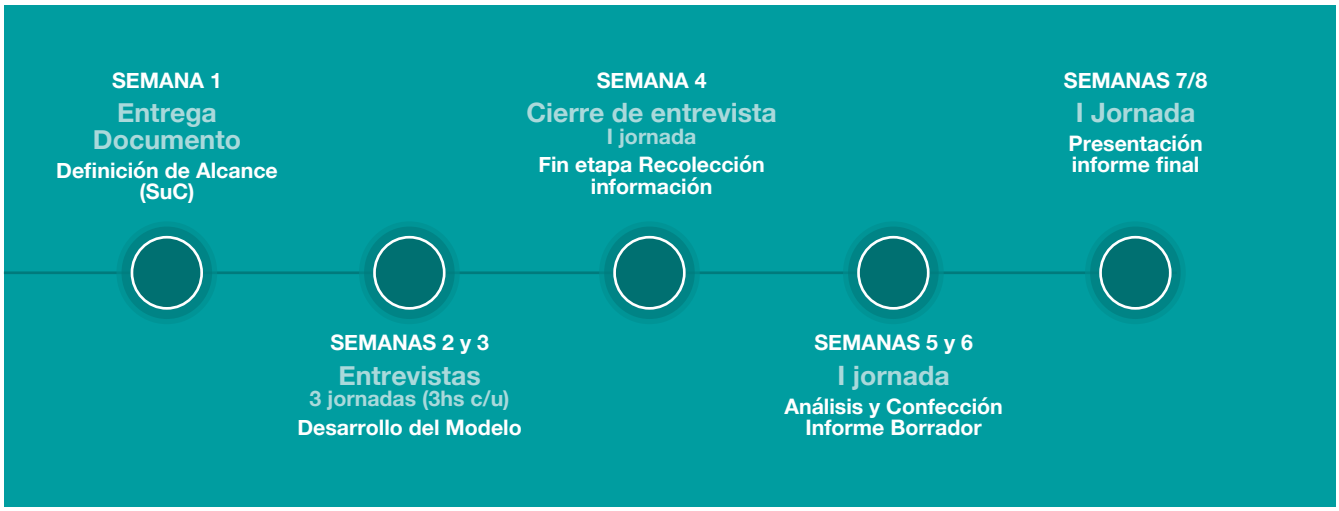
El desarrollo de este modelo se basa en entrevistas moderadas por ARPEL junto a un Consultor especializado, generando un diálogo ameno y confidencial con la empresa socia. La confidencialidad es uno de los factores principales que ARPEL ha conservado y esmerado en mantener durante todo el proceso, incluyendo la entrega de informes borradores y finales.

En las entrevistas se ha seguido el orden establecido por el modelo de los diversos dominios. De esta manera el consultor obtiene una "foto" del estado de salud o grado de madurez en OT de la organización. Esta herramienta es muy efectiva tanto para empresas que recién empiezan a ver el tema y necesitan un punto de partida sencillo y efectivo como para las más maduras que desean seguir mejorando y optimizando sus procesos.

Se lleva a cabo una primera sesión (de una o dos horas de duración), donde se presenta el tema y se hace énfasis en los perfiles necesarios de las personas ejecutar el modelo. Luego, estos assessment se realizan en no más de 3 o 4 sesiones de 3 horas reloj cada una, siempre y cuando las personas sean las indicadas para responder las preguntas. Cabe destacar que durante las entrevistas NO se solicita evidencia alguna, ya que todo se basa en la confianza y en la premisa de que este ejercicio debe arrojar un verdadero estado de salud para poder detectar y corregir aquellas capacidades que requieren un nivel superior. Una buena analogía es la de las personas al ir al médico. Ir a mentirle no tiene sentido alguno ya que nos iremos con un diagnóstico erróneo y no tendremos posibilidad de mejoras o de prevenir una situación no deseada. Recordemos que al no pedir evidencia es que no hay análisis o estudios o auditorías involucradas en este proceso.

El **entregable** recibido por cada empresa no solo tiene la evaluación de las más de 300 prácticas del modelo, sino que **incluye como valor agregado** un detalle de brechas, o **principales hallazgos, por cada dominio y un diagnóstico general de alto nivel** indicando posibles Quick Wins o puntos de apalancamiento principales a desarrollar en el mediano y corto plazo.

Los hitos principales en la ejecución son los que vemos en la siguiente imagen:



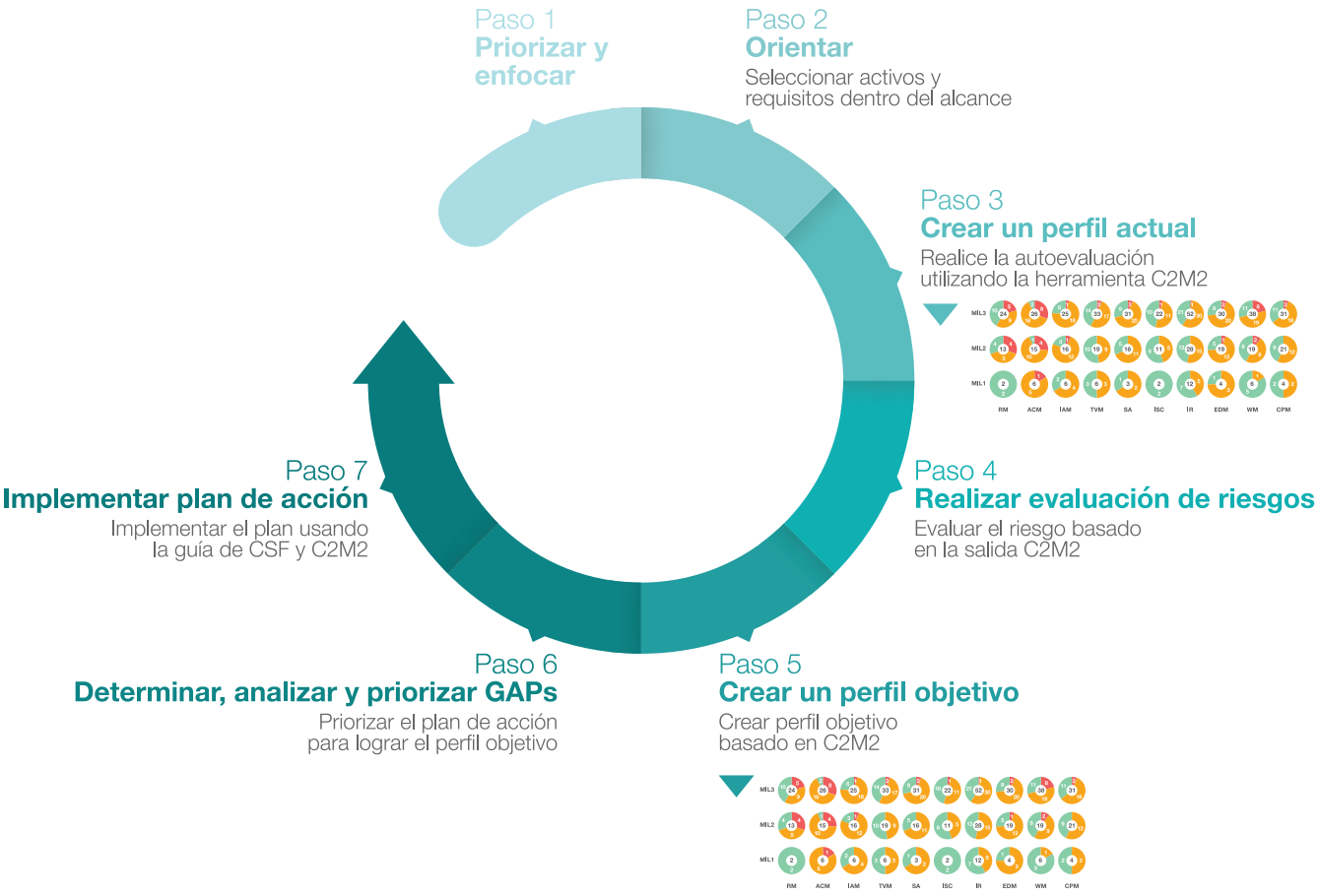
Esta línea de tiempos está situada en el máximo tiempo que pueda emplearse, y en la gran mayoría de los casos se llevó a cabo en la mitad de tiempo, es decir en el término de 4 a 5 semanas.

Las empresas participantes que alimentan este indicador de ARPEL son:

04.1

La experiencia

En el gráfico a continuación se puede observar el ciclo propuesto para la mejora continua y la toma de oportunidades de mejora por parte de las empresas socias de ARPEL luego de realizar la evaluación de madurez C2M2 v1.1a.



05
Resultados Obtenidos

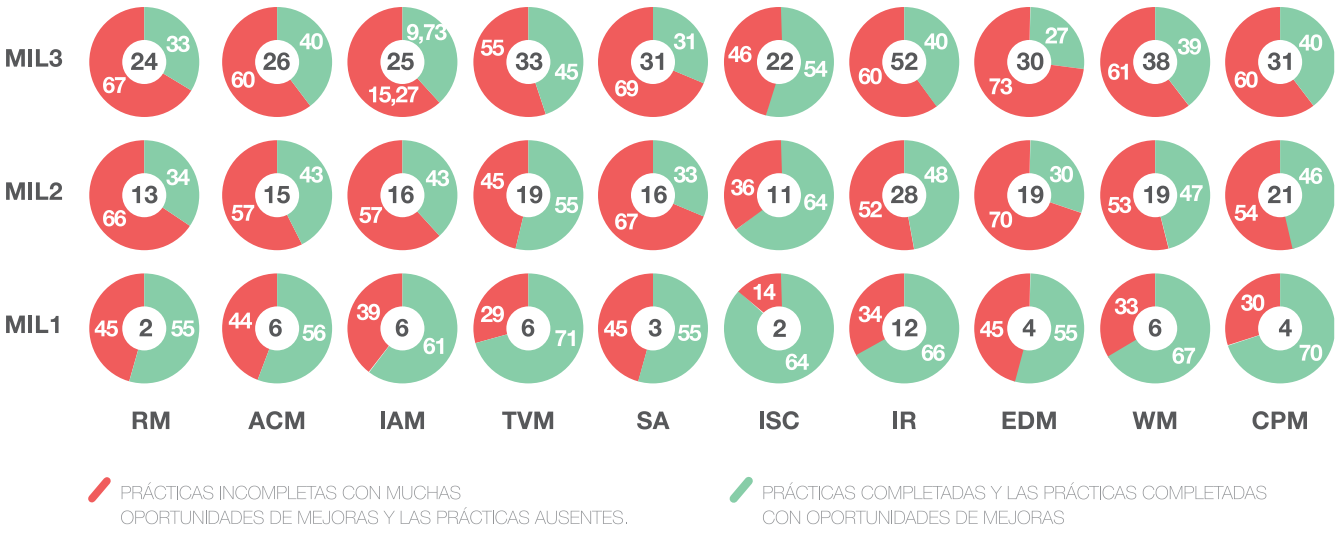
Se han realizado 12 evaluaciones entre mayo 2021 y agosto 2022. Con la debida autorización de las empresas socias, y manteniendo la absoluta confidencialidad y anonimato de los resultados, ARPEL elaboró la primera edición de su Indicador de Madurez en Ciberseguridad Industrial (IMCI) .

A continuación, se muestran diversas vistas de este y sus respectivas explicaciones, interpretaciones y conclusiones.

Es importante aquí destacar que no es objetivo de este modelo de madurez el cumplimentar al 100% cada dominio en cada MIL, ya que eso dependerá de cultura y tolerancia al riesgo de cada organización. Algunas prácticas no tienen sentido para una organización en función de su perfil de riesgo y es por ello por lo que pueden estar en “no implementada” o “´parcialmente implementada” eternamente sin que esto sea perjudicial para la organización. Recordemos que este modelo de madurez está compuesto por más de 300 mejores prácticas a lo largo de 10 dominios, por lo que cumplir al 100% el modelo es casi una utopía. Esta es una excelente guía de referencia poniendo la vara lo más alta posible para medirnos. Esto a la vez ratifica la recomendación de realizar este ejercicio en forma bi-anual mínimamente, con el objeto de medirnos contra nosotros mismos, ya que ese es el verdadero grado de crecimiento que debemos tenemos que mirando.

Como primer indicador, y manteniendo la forma gráfica de donas propuesta por el modelo C2M2, hemos agrupado las prácticas de cada nivel en el rango de “alcanzadas” (verdes) y “no alcanzadas” (coloradas).

Obteniendo un promedio simple de los resultados obtenidos en los desarrollos realizados al momento, y realizando la agrupación mencionada, obtenemos el siguiente:



Observamos los 10 dominios y los 3 MIL con la cantidad de prácticas en el centro de cada dona y el porcentaje de cumplimiento de dichas prácticas en cada dominio y nivel de madurez.

En este gráfico podemos rápidamente observar cual es el porcentaje medio de prácticas cumplimentadas en cada nivel y para cada dominio. Por como está conformado el modelo es natural ver que el porcentaje cumplimentado disminuye en cada dominio al subir de nivel de madurez.

Este gráfico nos muestra visualmente el IMCI de una forma precisa, rápida y fácilmente comparable con el resultado propio de cada empresa cliente con el fin de que pueda ver su situación respecto de la media de la industria medida por ARPEL.

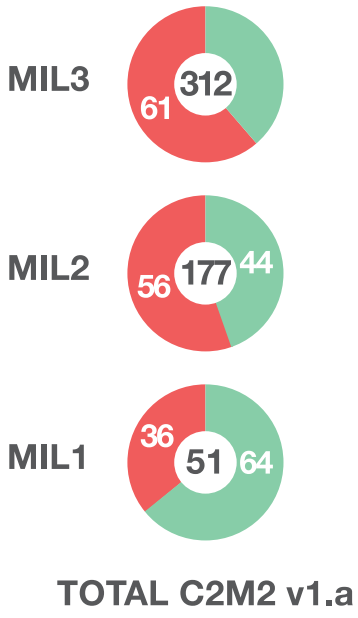
Si bien sabemos que los diversos dominios del modelo no poseen todos el mismo peso específico para la obtención de un índice general de madurez, y que para cada empresa será muy particular y subjetiva la valoración de cada uno, y que, por supuesto, esto estará íntimamente ligado a su tolerancia al riesgo y donde ponga mayor énfasis para la mitigación de los mismos, creemos que la diferencia porcentual de importancia entre ellos es muy baja, por lo que podemos darle a todos la misma importancia y obtener un nuevo indicador sobre el total del modelo y sus 312 prácticas.

Así es como hemos obtenido el siguiente indicador, donde podemos ver integradas todas las prácticas por nivel de madurez (MIL).

Notamos un alto porcentaje de cumplimiento en todos los niveles, ya que en el MIL1 estamos en general por encima del 60% (en 4 dominios se está apenas por debajo de este piso), y para el nivel MIL2 y MIL3 estamos en el orden del 40%. Observamos que existe un nivel de concientización alto en las Organizaciones de esta industria y que el mismo es llevado a la práctica para poder alcanzar estos porcentajes.

Cabe resaltar que a pesar de haber sido el primer ejercicio realizado entre las empresas socias, el resultado obtenido es más que satisfactorio y se nota el trabajo de años anteriores realizado por el Comité de Ciberseguridad de ARPEL.

Si partimos a la inversa, es decir, desde el análisis de este indicador general hacia el análisis pormenorizado por dominio, observamos que los dominios referidos al análisis de riesgos (RM) y a la gestión de activos (ACM) son los dos que se encuentran más por debajo de este promedio. Esto nos indica que son los que tienen mayor oportunidad y necesidad de mejora, por lo tanto, ya sabemos por dónde empezar a incrementar nuestra madurez general. No es casual que justo estos dominios sean los primeros en el modelo C2M2 v1.1a, ya que la gestión de los riesgos y la gestión de activos son piedras fundamentales en la Ciberseguridad ya que no podemos proteger lo que desconocemos que tenemos y tampoco podemos protegerlos si desconocemos que riesgo estamos dispuestos a tolerar. En este punto es muy importante destacar que se está midiendo la ciberseguridad industrial, y que si bien el mundo de la Operación (OT) es muy maduro en análisis de riesgo, este modelo C2M2 v1.1a representa la ausencia de los incidentes cibernéticos en estos. Dicha ausencia es muy habitual en el mundo de hoy, dado que esta especialidad es incipiente, y recién se empieza a tomar conciencia de analizar los incidentes cibernéticos a la misma altura de los diversos escenarios y causas a las que el mundo OT ya está familiarizada.



El mismo análisis puede realizarse para los MIL2 y MIL3 y así obtener los puntos principales de enfoque para lograr aumentar la madurez en estos niveles.

Hasta aquí hemos seguido estrictamente el modelo y su forma gráfica de representación a través de las donas. Veamos ahora otra forma de visualizar lo mismo en los clásicos gráficos de líneas a los que estamos más acostumbrados e incluso en los gráficos de araña que nos permiten tener una imagen global dada por el área que encierra la figura conformada.

Esto lo veremos en detalle en la próxima sección.

05.1

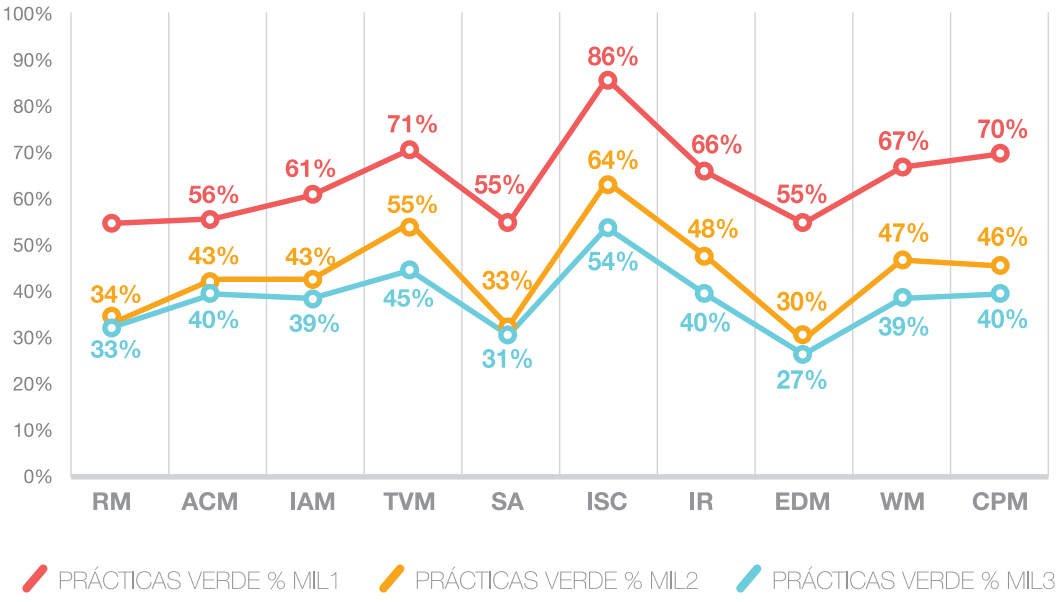
Resultado General de Compliance por MIL

En el gráfico a continuación vemos los 3 MIL juntos, y es muy esperable el resultado de tener el MIL1 con los valores más altos, luego el MIL2 y finalmente por debajo de los anteriores a la línea correspondiente al MIL3.

Observamos a primera vista que el dominio de intercambio de información y comunicaciones (ISC) es el que destaca positivamente por su nivel de cumplimiento en los 3 MIL. Esto se debe a que es el dominio más íntimamente relacionado con el mundo de la Seguridad de la Información (IT) y en consecuencia se aprecia su grado de madurez, ya que el mundo IT gestiona los ciberiesgos desde la década de los 90 en el siglo XX, mientras que el concepto de los incidentes cibernéticos y la ciberseguridad industrial data de la última década o década y media.

En contrapartida de esto, vemos que el dominio referido a la Gestión de la cadena de suministro y de dependencias externas (EDM) es el que más mejoras y atención necesita. Esto también es lógico, debido a que la ciberseguridad aplicada a las 3ras partes (contratados, contratistas, proveedores, clientes, etc.) es también algo que ha tomado mayor énfasis en los últimos años y más aún del año 2020 hacia nuestros días con el contexto vivido de pandemia a nivel mundial y la aceleración de la digitalización en las empresas en sus distintas áreas.

% compliance por MIL



Observemos el dominio Concientización de la situación (SA). Este es un dominio muy particular ya que el mismo contempla todo lo que se refiere a recopilar, analizar, alertar, mostrar y utilizar información referida a la operación y de ciberseguridad, con el fin de conformar una visualización operativa única, desde el punto de vista de la ciberseguridad. Este también es uno de los de menor porcentaje en el MIL1 y eso se debe a la integración y convergencia de los mundos IT y OT, ya que las tecnologías de monitoreo y vigilancia implementadas por el mundo IT en las redes corporativas están empezando a tomar el alcance del mundo OT y eso hace que se reduzca dicho porcentaje en la sinergia.

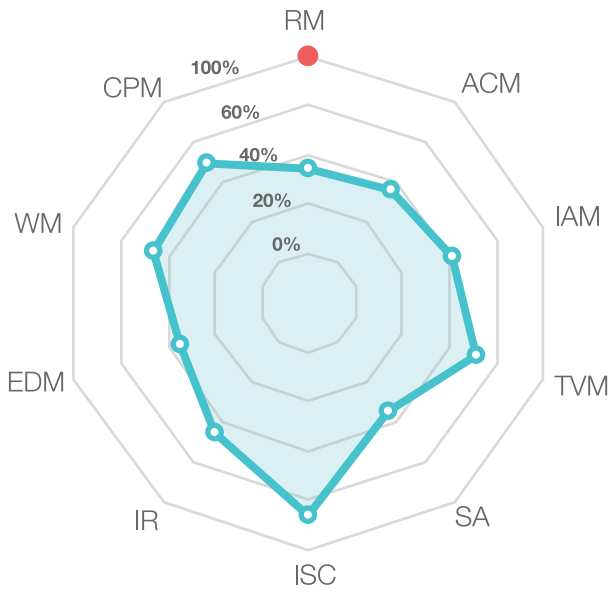
De esta manera podemos entrar en cada uno de los dominios y realizar el análisis pensando en la convergencia de los mundos IT y OT y en la ciberseguridad industrial como la competencia que este modelo evalúa. Luego, si tenemos resultados obtenidos bajo este modelo, podemos saber cómo estamos respecto de la media de la industria de Oil&Gas medida por ARPEL a través de su indicador IMCI.

Separemos ahora la medición por cada nivel de madurez y veámoslo dentro del contexto de los 10 dominios de este modelo. Utilizaremos los clásicos gráficos llamados “de araña” por su similitud a las telas que estas construyen. Este tipo de gráficos

radiales sirven para evaluar diferentes opciones en función de múltiples variables, ya que permiten mostrar una o más variables en un gráfico bidimensional donde cada radio corresponde a una variable.

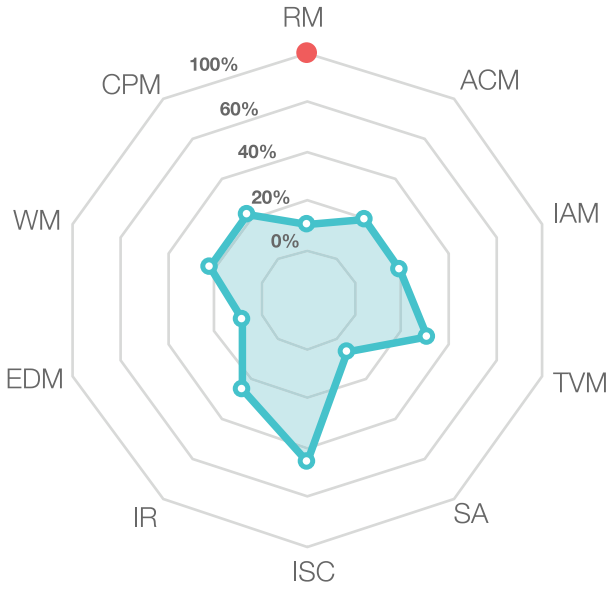
Aquí, a continuación, representamos los 3 MIL (MIL1, MIL2 y MIL3) por separado, en función de los 10 dominios del modelo.

Compliance MIL1



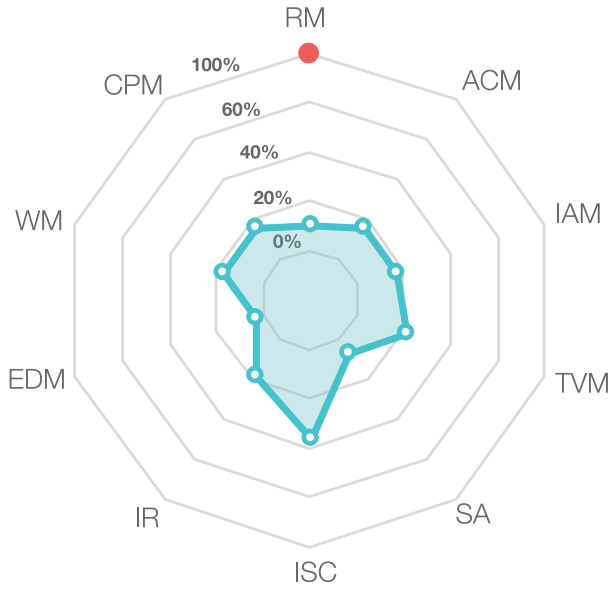
En este primer gráfico observamos el cumplimiento correspondiente al MIL1. Rápidamente, y ante el primer vistazo que damos al mismo, vemos que el área encerrada por la marcación de los diversos dominios nos da una idea general de este marco de cumplimiento general por encima del 60% (como ya mencionamos), dentro del modelo, para este nivel MIL1. No sorprende que sea el dominio ISC el de mayor cumplimiento, dado que muestra la amplia madurez en la Seguridad de la Información, muy ligado a IT, quien posee más de dos décadas abocada a la ciberseguridad, desde que las empresas se unieran a la Internet comercial a mediados de los 90.

Compliance MIL2



Siguiendo la misma idea que en el gráfico anterior, observamos el grado de cumplimiento del MIL2. Vemos que el primer impacto visual nos hace notar rápidamente una reducción del área encerrada, por lo que observamos que existe una disminución de porcentual de cumplimiento a nivel general de para este nivel MIL2 respecto de anterior MIL1.

Compliance MIL3



Finalmente, para el MIL3, observamos que el área encerrada por los puntos correspondientes a cada dominio se reduce aún un poco más que en el caso anterior del MIL2. Esto es natural y lógico por lo que venimos analizado y observando de gráficos anteriores referidos a este nivel MIL3 y porque cada dominio abarca al anterior.

Observemos que los puntos son más cercanos al centro, indicado un porcentaje más bajo de cumplimiento y es por ello por lo que el área del gráfico conformado es más reducida.

En estos últimos 3 gráficos logramos observar de una manera visual diferente los mismos puntos del análisis que veníamos realizando anteriormente, solo que separando los MIL y observándolos en todo el contexto de los 10 dominios. A esta altura ya habrán deducido que el gráfico “más deseado”, o el gráfico “perfecto”, es aquél con el área completa del polígono de 10 lados que conforma la “tela de araña”. Esto significaría un cumplimiento del 100% en cada dominio y en consecuencia obtendríamos el área más grande posible.

05.2

Resultados de cumplimiento por Dominio

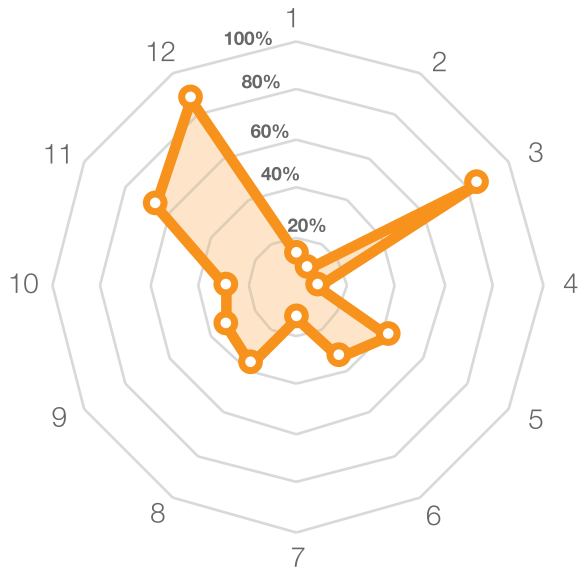
Seguiremos utilizando estos gráficos de “araña” para analizar ahora los resultados por cada dominio.

En esta sección podremos observar por separado cada uno de los dominios y los resultados obtenidos en las distintas evaluaciones realizadas. Esto nos permite visualmente tener la amplitud de los resultados, es decir, ver claramente los extremos superior e inferior y la distribución de los valores que han dado por resultado los promedios vistos en la primera parte de esta sección.

En consecuencia, esta sección nos aporta información adicional de análisis estadístico para lo que es el IMCI de ARPEL, y si lo deseamos, desarrollar un análisis más exhaustivo y particular para cada organización.

Al solo efecto de favorecer la visión de los siguientes gráficos, y de mantener la privacidad y confidencialidad de los resultados de las empresas participantes, es que se ha optado por quitar las escalas numéricas. Las líneas intermedias dan la idea de la cantidad total de las prácticas de cada dominio mientras que los vértices están asociados a la cantidad de empresas participantes (lo cual no significa que sea lineal y exista correspondencia de uno a uno).

RM



Así, en el correspondiente al primer dominio de Gestión de Riesgos (RM) observamos un extremo de alto cumplimiento muy marcado, pocas muy cercanas al centro, y luego una distribución pareja entre el resto.

Una conclusión que podríamos sacar al leer este gráfico, respecto del indicador general, es que el mismo sigue siendo representativo, pues, si sacamos los extremos que podrían sesgarnos los resultados estaríamos obteniendo aproximadamente el mismo resultado.

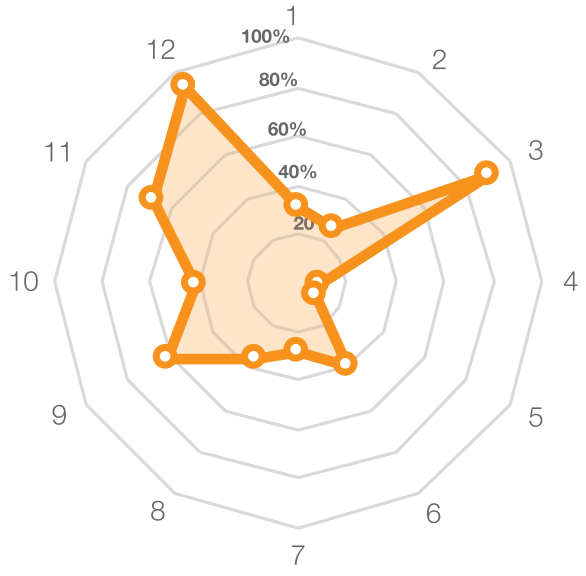
En los siguientes gráficos de los restantes 9 dominios van a poder observar las mismas características, que por supuesto fueron analizadas para validar el IMCI que hemos mostrado al inicio de esta sección.

No es nuestra intención entrar en detalles y justificaciones estadísticas de nuestro Indicador de Madurez de Ciberseguridad Industrial (IMCI). El objetivo del mismo es ser un patrón, un espejo donde poder mirarse, y una herramienta que potencie a las empresas de la Industria a superarse y alcanzar objetivos de madurez en Ciberseguridad Industrial.

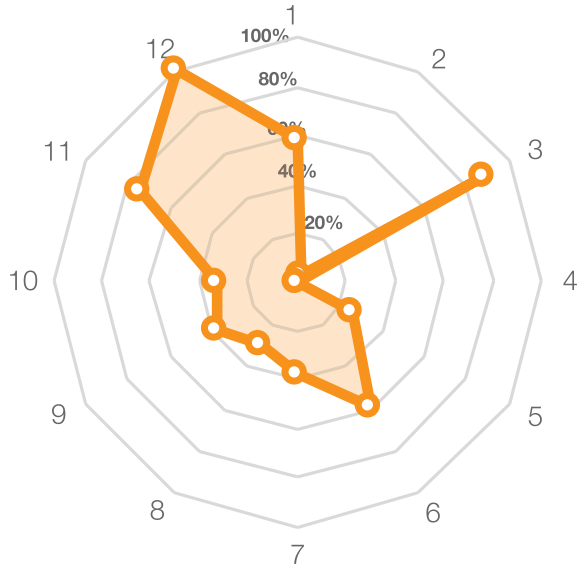
Además, cada reporte final presentado a las empresas socias cuenta con un análisis por objetivo dentro de cada dominio, lo cual presenta detalles adicionales al proporcionar un gráfico que muestra las respuestas a las prácticas por dominio y objetivos. Estos gráficos de donas por objetivos permiten un análisis más en profundidad del resultado del dominio para cada MIL.

Dicho esto, a continuación, se muestran los 9 dominios restantes con su totalidad de prácticas, por lo que estamos observando el cumplimiento a nivel MIL3 de los mismos.

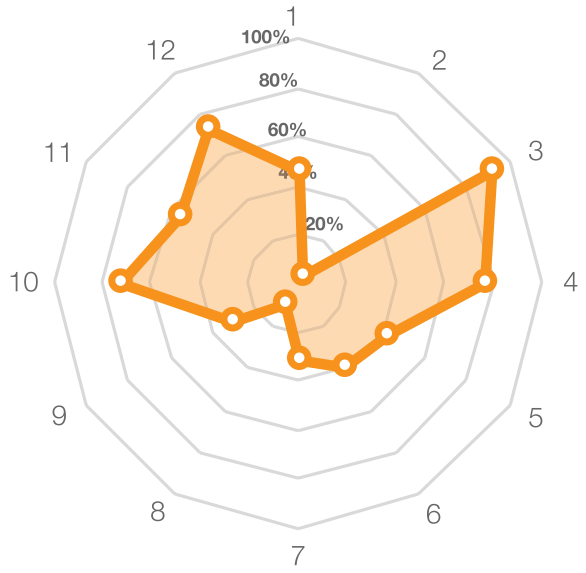
ACM



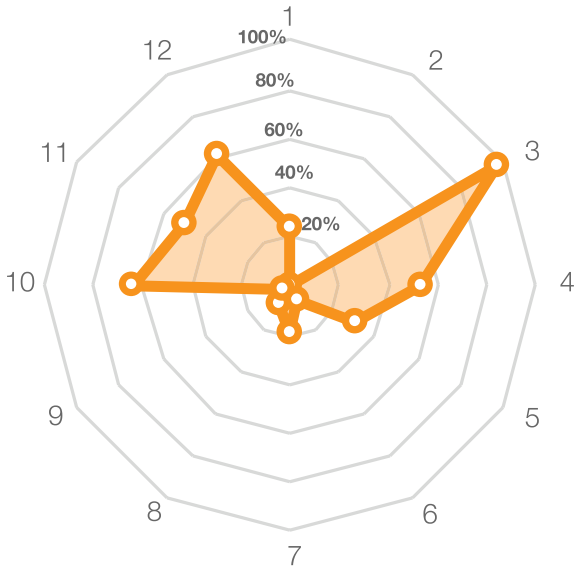
IAM



TVM

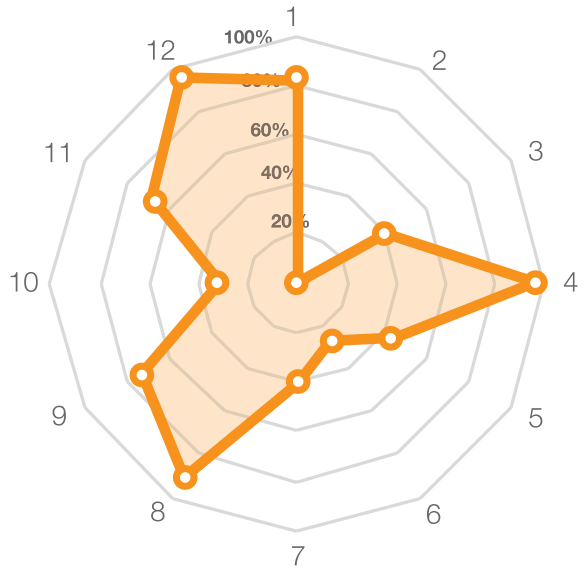


SA

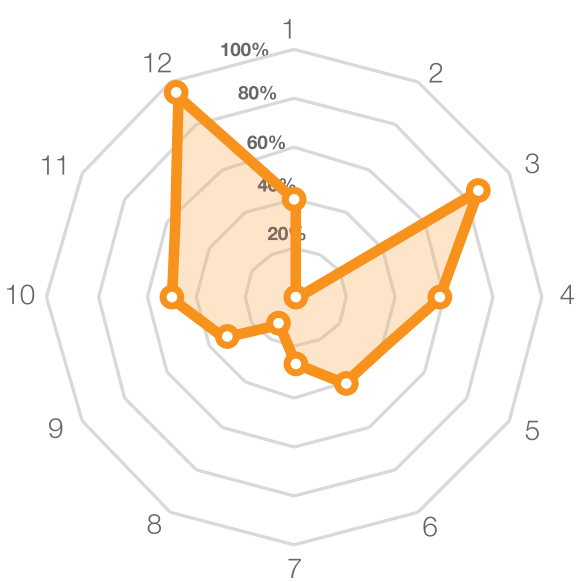


Cabe hacer una observación respecto del gráfico del dominio Concientización de la Situación (SA). Observamos que, salvo 3 mediciones que abren el gráfico hacia la parte externa, todo el resto es muy parejo ocupando un círculo concéntrico del 25 a 30% aproximadamente, el cual coincide con el resultado obtenido para el MIL3 de este dominio en el IMCI. Con esto solo queremos validar y resaltar la importancia de seguir alimentando este indicador y que cuantas más empresas podamos medir, o bien, diversos alcances dentro de una misma empresa, más sólido será este indicador IMCI

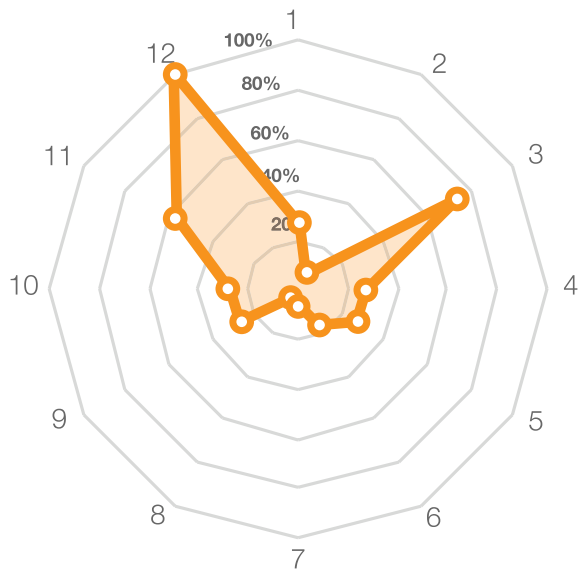
ISC



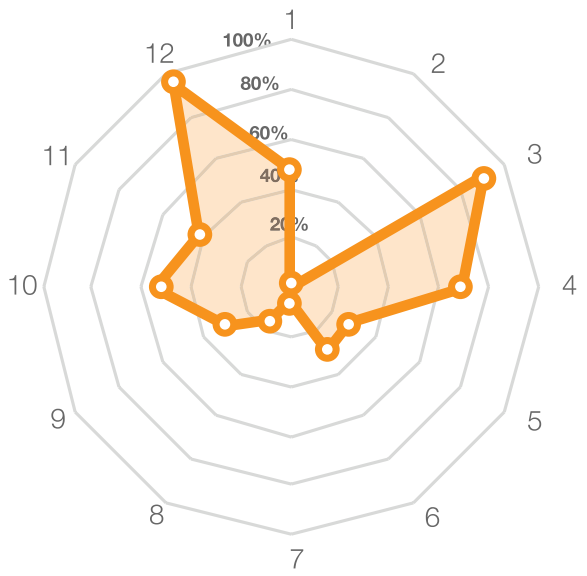
IR



EDM

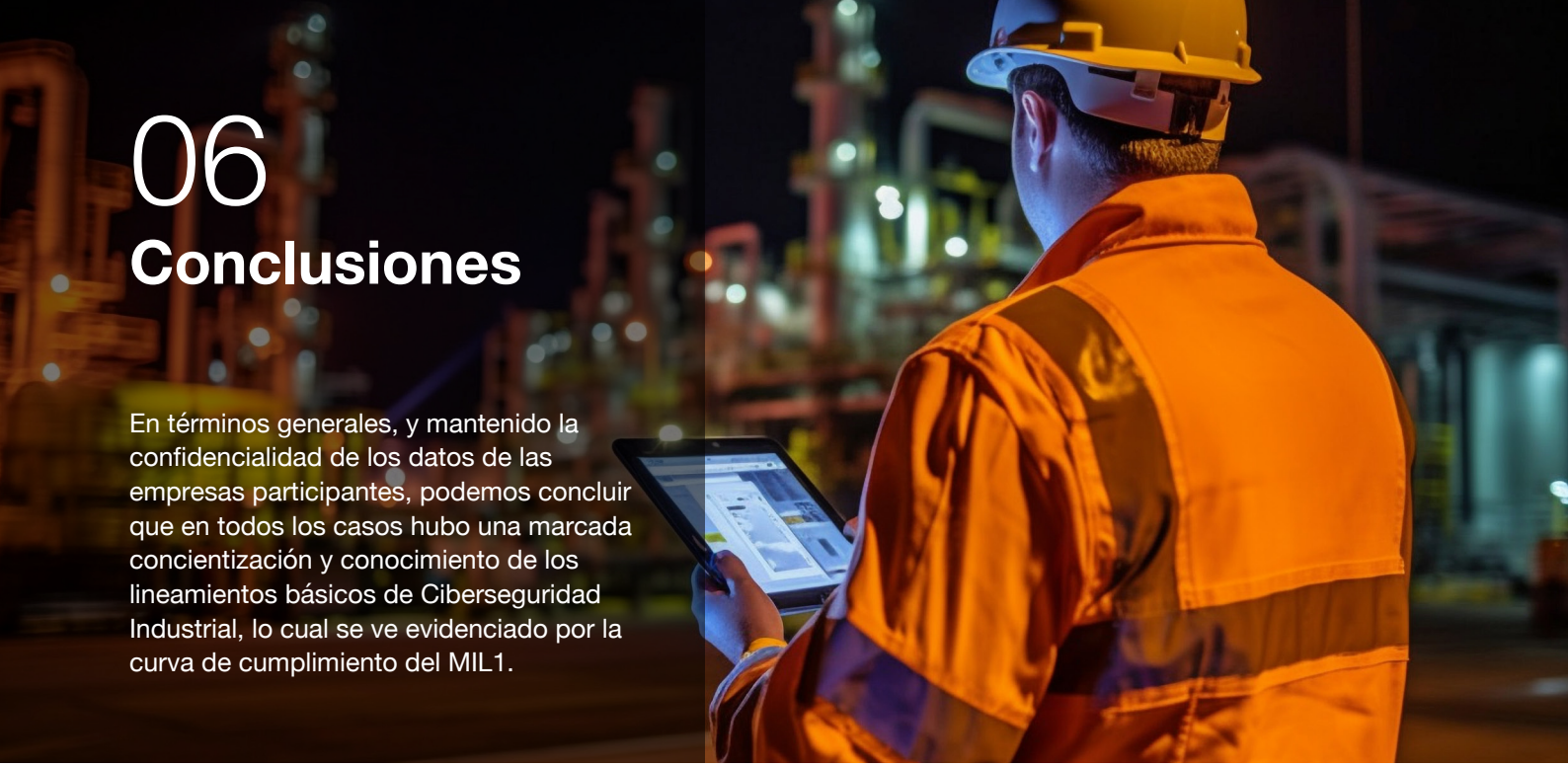


WM



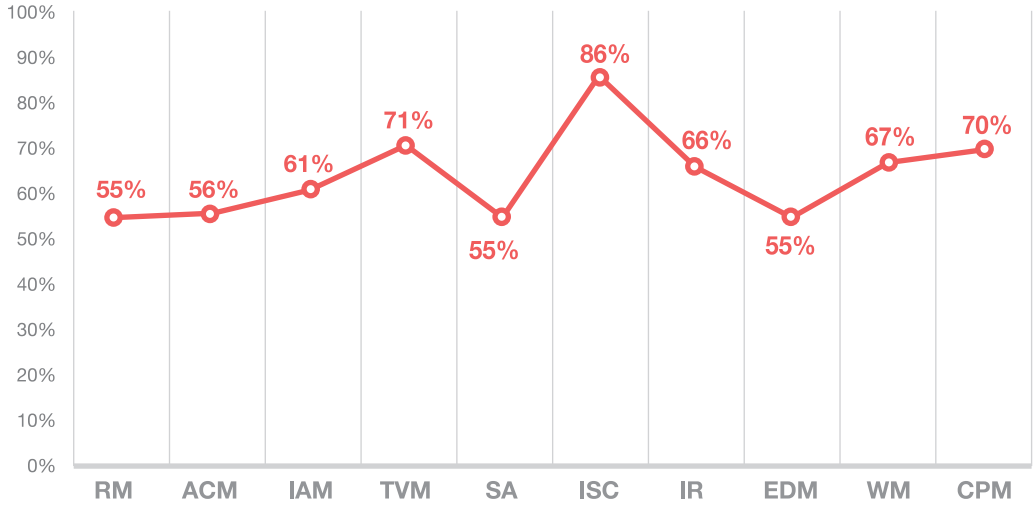
Finalmente, vemos aquí el último dominio, que representa un poco la conjunción de todos los anteriores, pues, es la Gestión de programas de ciberseguridad (CPM). Observamos que tenemos tres (3) mediciones de alto grado de cumplimiento, mientras todo el resto se encuentra en el orden del 30%. Esto último puede darnos una pequeña corrección respecto del indicador general que nos estaba indicando un grado de 37% de cumplimiento total.

Ratificamos entonces la validez de estos puntos de vista adicionales, o complementarios, con el fin de tener una visión más cercana a la realidad que cada empresa puede encarar en un plan de acción propio para incrementar su madurez en Ciberseguridad industrial.



06
Conclusiones

En términos generales, y mantenido la confidencialidad de los datos de las empresas participantes, podemos concluir que en todos los casos hubo una marcada concientización y conocimiento de los lineamientos básicos de Ciberseguridad Industrial, lo cual se ve evidenciado por la curva de cumplimiento del MIL1.

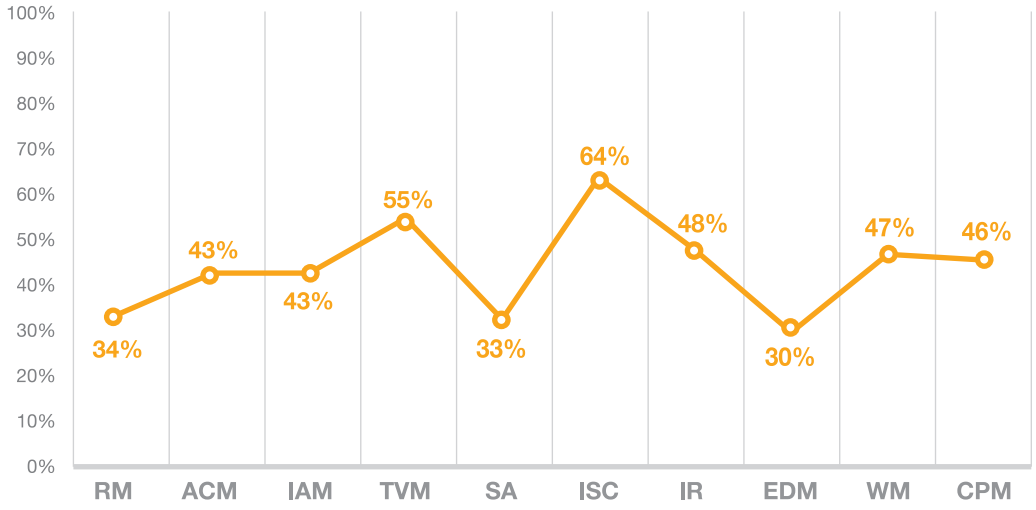


Observamos aquí que, excepto 4 dominios (RM, ACM, SA y EDM), todos los demás están por encima del 60% de cumplimiento. De cualquier manera, es muy cercano a dicho **piso de 60%** el caso de RM, ACM y EDM. La razón por la que estos dominios se encuentran más bajos responde a que son los más notorios en un inicio hacia la convergencia IT/OT. Esto se debe a que el **análisis de riesgos funcional** debe empezar a contemplar las ciber amenazas, **los inventarios** deben consolidarse entre IT y OT y tener ciertos atributos importantes a nivel de hard y soft para hacer posible su protección ante vulnerabilidades, los cuales en el mundo OT no son comunes de incluir.

Finalmente, el dominio EDM (Gestión de la Cadena de Suministro y Dependencias Externas) es el referido a **riesgos de ciberseguridad asociados a los servicios y activos que dependen de entidades externas,** y las oportunidades de mejora en el mismo están dadas por ejercer un mayor control en el ámbito de OT con proveedores, contratistas y terceras partes en general.

Antes de pasar al MIL2, es importante aquí volver a destacar que **no es objetivo de este modelo de madurez el cumplimentar al 100% cada dominio en cada MIL,** ya que eso dependerá de cultura y tolerancia al riesgo de cada organización. Algunas prácticas no tienen sentido para una organización en función de su perfil de riesgo y es por ello que pueden estar en “no implementada” o “´parcialmente implementada” eternamente sin que esto sea perjudicial para la organización. Recordemos que el modelo de madurez está compuesto por más de 300 mejores prácticas, por lo que cumplir el modelo al 100% es casi utópico, y por ello es una excelente guía de referencia poniendo la vara lo más alta posible para medirnos por nosotros mismos.

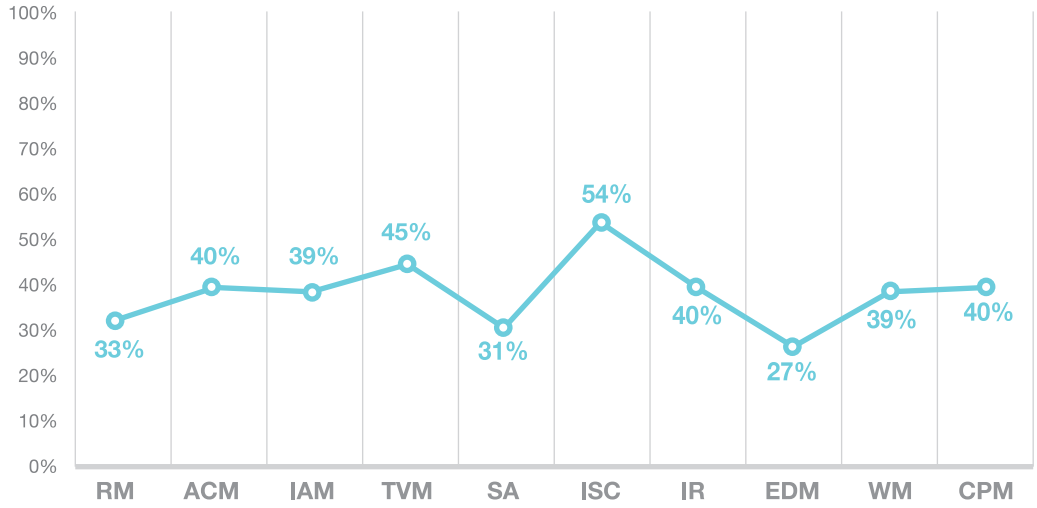
Dicho esto, pasemos al MIL2.



Observamos aquí que, excepto 3 dominios, **el piso ahora lo tenemos en el 43%** en lugar del 60% del MIL1. Los 3 dominios que nos quedan con un porcentaje inferior son RM, SA y EDM.

RM y EDM se mantienen bajo esa línea piso, tanto en el MIL1 como en MIL2, y aplican las mismas razones mencionadas para el MIL1. El caso de SA baja a partir de este nivel por las oportunidades de mejora detectadas a nivel de monitoreo y vigilancia de las redes y dispositivos OT, lo cual es también consecuencia de lo indicado en el MIL1 respecto de la convergencia en gestión de activos de IT y OT.

Finalmente pasemos a ver el MIL3



En este caso observamos que, excepto 3 dominios, **el piso ahora es de 39%**. Los 3 dominios que nos quedan con un porcentaje inferior son RM, SA y EDM. Los mismos que en MIL2. Aplican aquí las mismas consideraciones que en los MIL anteriores para estos 3 dominios. Recordemos que el modelo es acumulativo con los MIL, es decir, cada MIL superior contiene a los anteriores, lo cual justifica y da lógica a los resultados y análisis que estamos llevando a cabo.

En resumen, en **los 3 MIL** hemos observado **pisos de 60%, 43% y 39%,** lo cual también es lógico que el piso baje al aumentar en exigencia de grado de madurez. Cabe destacar que las mayores oportunidades de mejora observadas en las empresas han sido referidas a la **Gestión de Riesgos (RM),** a la **Gestión de Activos y también de Identidades (ACM e IAM),** y en **Gestión de personal (WM),** sobre todo por la importancia de los puestos y cargos dedicados a Ciberseguridad que deberían formalizarse. Por supuesto el dominio de **Concientización de la situación (SA),** ha tenido observaciones, pero las mismas son más de evolución y dependientes de otros dominios a madurar previamente, como el de ACM e IAM que ya mencionamos.

Como cierre final podemos decir que todas las empresas que participaron de este ejercicio ya tenían una conciencia de la importancia de la ciberseguridad industrial ya que son parte del ecosistema de ARPEL y participan activamente del Comité de Ciberseguridad Industrial. Han aprovechado el mismo para poder mejorar sus planes de Ciberseguridad y sobre todo para integrar al personal de IT y de OT, y así poder trabajar de forma más cercana en equipos multidisciplinarios, que es la piedra fundamental para el éxito de un Plan de Ciberseguridad Integrado dentro de una empresa de Oil&Gas.

07
Glosario de términos y acronimos

C2M2: (Cybersecurity Capability Maturity Model) – Modelo de capacidad en la madurez de ciberseguridad
DHS: (Department of Homeland Security) – Departamento de seguridad de USA
DoE: (Deparment of Energy) – Departamento de Energia de DHS de USA.
ICS: (Industrial Control System) – Sistemas de Control Industrial
IEC: (International Electrotechnical Commision) – Comisión Internacional Electrotécnica
IMCI: (Indicador de Madurez en Ciberseguridad Industrial)
IT: (Information Technology) – Tecnología de la información
IoT: Internet of Things – Internet de las Cosas
IIoT: Industrial Internet of Things – Internet Industrial de las Cosas
ISO: (International Organization for Standarization) – Organización Internacional de Normalización
MIL: (Maturity Indicator Level) – Indicador de nivel de madurez
NIST: (National Institute of Standards and Technology) – Instituto Nacional de estándares y tecnología de USA
ONG-C2M2 v1.1a: Oil and Natural Gas - Modelo de capacidad en la madurez de ciberseguridad
OT: Operational Technology – Tecnología operacional

BENCHMARKING

Benchmarking de Madurez en Ciberseguridad Industrial en la industria petrolera y del gas para América Latina y el Caribe

Estadísticas 2021 y 2022 de
las empresas socias de ARPEL

ASOCIACIÓN DE EMPRESAS DE
PETRÓLEO, GAS Y ENERGÍA RENOVABLE
DE AMÉRICA LATINA Y EL CARIBE

ARPEL es una asociación sin fines de lucro que nuclea a empresas e instituciones del sector petróleo, gas y energía renovable en América Latina y el Caribe. Fue fundada en 1965 como un vehículo de cooperación y asistencia recíproca entre empresas del sector, con el propósito principal de contribuir activamente a la integración y crecimiento competitivo de la industria y al desarrollo energético sostenible en la región.

Actualmente sus socios operan en más de 30 países de América Latina y el Caribe e incluyen a empresas operadoras nacionales e internacionales, proveedoras de tecnología, bienes y servicios para la cadena de valor, y a instituciones nacionales e internacionales del sector.

Sede Regional:
Av. Luis A. de Herrera 1248. WTC. Torre 2. Piso 7. Of. 717.
CP 11300. Montevideo, Uruguay
Tel: (+598) 2623-6993 • info@arpel.org.uy

www.arpel.org