MODELO DE EVALUACIÓN DE LA CIBERSEGURIDAD EN INSTITUCIONES PÚBLICAS. IMPLEMENTACIÓN Y PROPUESTAS DE MEDIDAS EN SERVICIOS PÚBLICOS

MARCELO ROJO ARAYA

Magíster en Gerencia y Políticas Públicas, Universidad de Santiago de Chile.

Administrador Público, Universidad de Santiago de Chile.

marcelo.rojo.a@gmail.com

ID-ORCID: 0009-0003-3690-4327.

Resumen

Este artículo presenta el diseño y aplicación de un modelo para evaluar el nivel de madurez de la ciberseguridad en el ámbito público: el Modelo de Evaluación de la Ciberseguridad en Instituciones Públicas. Para su diseño, se analizaron y extrajeron elementos de dos modelos: uno por la Agencia Europea de Ciberseguridad y otro por la Organización de Estados Americanos con el Banco Interamericano de Desarrollo. A su vez, se siguieron los lineamientos de la Política Nacional de Ciberseguridad de Chile y los distintos instrumentos vigentes. Para su ejecución, se implementó exploratoriamente en la Superintendencia de Insolvencia y Reemprendimiento y la Fiscalía Nacional Económica. Se evidenció que este Modelo permite identificar avances y debilidades en la materia y, a partir de estas últimas, generar propuestas de mitigación y mejora.

Palabras clave: ciberseguridad, CSIRT, modelo de evaluación, prevención, protección.

Abstract

Cybersecurity Evaluation Model in Public Institutions.

Implementation and Actions Proposal in Public Services

This article presents the design and application of a model for assessment with respect to the maturity level of cybersecurity in the public domain: the Cybersecurity in Public Institutions Evaluation Model. For its design, it analyzed and extracted elements of two models:

one by the European Union Agency for Cybersecurity and the other by the Organization of American States together with Inter-American Development Bank. In turn, it followed the guidelines of National Cybersecurity Policy in Chile and the distinct current resources. For its execution, it exploratorily implemented in the Superintendency of Insolvency and Resumption/Re-entrepreneurship and the Office of National Economic Prosecutor. It evinced that this Model allows for identifying advances and weaknesses in the matter and, from the last ones, generating mitigation and improvement proposals.

Keywords: cybersecurity, CSIRT, evaluation model, prevention, protection.

Durante los últimos años, las sociedades han sido testigos del avance de las tecnologías de la información y comunicación (TIC) en casi todos los ámbitos sociales e individuales. Se procesa un conjunto de información digital sobre lo que se hace o deja de hacer: geolocalizaciones, con quiénes se establecen comunicaciones, sobre qué temas, por cuánto tiempo y más. Sólo en términos de telefonía móvil, según GSMA (2022), la cantidad de líneas ha crecido un 5% entre 2021 y 2022), abarcando al 67% de la población mundial; y, para 2025, van a existir 5,7 billones de líneas de telefonía móvil, cubriendo el 70% de los habitantes del planeta.

De esta manera, la situación de abundancia de información digital y comunicación en línea viene creciendo año tras año. No obstante, esta nueva realidad no se limita al mundo privado de las personas, sino que, por el contrario, abarca las distintas esferas de lo social. El ámbito público está afectado por las nuevas tecnologías de la información y la comunicación. En cada interacción digital quedan rastros o huellas que son utilizados para campañas de venta de productos, diseño de nuevas aplicaciones o elaboración de nuevas políticas por parte de los Estados. Los datos generados constantemente por la población son la nueva materia prima desde la cual se está repensando nuestro quehacer, desde nuestra esfera privada a nuestra interacción pública. Estos datos, generados y almacenados en servidores, analizados por algoritmos, utilizados para la creación de nuevas acciones que inciden en nuestro comportamiento, se transforman en un elemento fundamental del orden social contemporáneo.

En definitiva, el espacio digital o ciberespacio ya es una parte central de nuestro día a día. Siendo los datos un elemento de vital importancia para las organizaciones, en general, su almacenamiento y uso requieren de nuevas medidas de protección y resguardo. En este contexto es que la ciberseguridad entra en escena. El actual flujo de datos e información requiere que se lleven adelante tareas de seguridad de la información ya que no sólo para proteger la intimidad y privacidad de las personas, sino también porque su eventual manipulación puede tener grandes consecuencias a nivel social en términos económicos, políticos, además del resguardo de los derechos de privacidad personal. La información se ha transformado en un elemento de valor que requiere ser protegido como un bien, tanto de las personas como de las instituciones, empresas u otras organizaciones.

Con lo anterior, se manifiesta el crecimiento de intereses en la recopilación, manejo y explotación de información. Tecnologías como *Big Data* o los recursos de Inteligencia Artificial son algunas de las técnicas con las cuales se extrae valor de la información. Ello ha llevado una manipulación de este bien tanto para fines lícitos, como segmentación de ventas o efectividad en la implementación de programas públicos, tal como para fines ilícitos, a saber: filtraciones, robo de datos personales, espionaje corporativo o estatal, por ilustrar. Esto compela a las organizaciones de fines privados y públicos al desarrollo de mecanismos de seguridad y vigilancia informática. Así, bajo el paraguas de la ciberseguridad, en tanto disciplina en crecimiento, se han propuesto e implementado medidas, normativas y protocolos para la prevención o combate del acceso o uso indebido de datos. De aquí que, para Panetta (2021), en 2023, alrededor del 75% de la información personal de la población mundial se regirá bajo leyes de privacidad.

Así, en América Latina, en los últimos años se ha visto la implementación de normativas para establecer procesos y protocolos de ciberseguridad. Sin embargo, la infraestructura informática propia de esta región dista bastante de la presente en las denominadas *big-tech* (grandes compañías de servicios digitales como Google, Amazon, Microsoft, Facebook o Apple). Los Estados corren con el doble desafío de actualizarse a la vez que tienen que combatir las posibles amenazas a sus sistemas, infraestructura e información: «no sólo afectan a particulares o empresas de forma individual, sino que también se consideran una amenaza para

los Estados, las sociedades y las economías» (Fonfría y Duch-Brown, 2020, p. 2). De aquí que las administraciones públicas, en general, y sus políticas públicas, en particular, hayan debido empezar a relacionarse con la ciberseguridad. Si se considera, además, que mucha de la información en manos de tales administraciones corresponde a datos sensibles, hay un imperativo, bajo el principio de transparencia y ética pública, el resguardo y protección ante potenciales amenazas.

En buena medida, organismos como el Banco Interamericano de Desarrollo (BID) o la Organización de Estados Americanos (OEA) han elaborado estándares en ciberseguridad. En Chile, a partir de 2011, se han llevado a cabo medidas con el fin de proteger la información de potenciales usos ilícitos[1]. En 2017, de hecho, se estableció la Política Nacional de Ciberseguridad (2017-2022), durante el segundo gobierno de Michelle Bachelet. Justamente, en el marco de esta Política Nacional, se toman los modelos internacionales para observar su adaptación al caso de la administración pública chilena para diseñar una propuesta de herramienta específica, su implementación y sus primeros resultados como experiencia piloto. A su vez, esta experiencia se contrastará conforme a los marcos determinados por los estándares de seguridad internacionales. Se espera, a su vez, que esta herramienta pueda superar las fronteras del país, *mutatis mutandis*, para la adopción en otros casos.

Marco Conceptual

A partir de la concepción del Estado y la administración weberiana (Weber, 1969), la dominación racional-legal implica una «institucionalización» de la burocracia en tanto administración del poder y, por tanto, las decisiones. Esta, pues, muta la atomización política señorial proveniente del periodo medioevo y, a su vez, de la tradición principesca o el ejercicio caudillista, centrando así el ejercicio de la violencia legítima en una única autoridad. De aquí que el Estado conlleve «burocracias» con funciones asignadas formalmente, esté determinado por un conjunto de reglas que ordenan las relaciones sociales y, con todo lo

[1] Se ha denominado crimen digital al acceso y/o uso ilícito en la literatura especializada (Fonfría y Duch-Brown, 2020).

anterior, se asiente en un territorio que pretende también ser un foco de identidad colectiva (Medina, 2010).

Conforme lo anterior, tanto la condición de esta concepción de Estado como su propio desarrollo se vinculan con la noción de política pública como de tratamiento de información. Por una parte, entendiendo la política pública como todo aquello que los gobiernos deciden hacer o dejar de hacer (Dye, 2008), esta es la acción del Estado, en última instancia, sobre determinada sociedad; por tanto, una «burocracia» o administración del Estado es la estructura organizacional para el funcionamiento de políticas públicas. Por otra, sin perjuicio de las implicancias entre una y otra, las políticas como las administraciones públicas generan, recolectan, miden, monitorean, documentan, evalúan y almacenan datos. Es decir, están en el meollo de los sistemas de información. Por tanto, en los tiempos actuales, se sitúa así la noción de ciberseguridad.

Por tanto, se define ciberseguridad como sigue: «la capacidad de resistir, con un nivel determinado de fiabilidad, a toda acción que comprometa la disponibilidad, autenticidad, integridad, o confidencialidad de los datos almacenados o transmitidos, o de los servicios ofrecidos» (Ballestero, 2020, p. 40). Por «disponibilidad» se entiende que la información y los recursos puedan ser accesibles para aquellos actores autorizados. Por «autenticidad» se entiende que la información sea aquella que ha sido operada por los agentes autorizados y no modificada por terceros, extendiéndose la idea de que sean datos que albergan el verdadero sentido por el que fueron recolectados. Por «integridad» se remite a la cualidad de la información para ser correcta y no haber sido modificada. Por último, la «confidencialidad» implica que la información no sea divulgada sin autorización y, pues, sólo pueden acceder aquellos entes autorizados. Estas definiciones no buscan terminar el debate teorético ni son ecuánimes: diversos autores sostienen o acentúan distintas particularidades[2]. Se trata, en este caso, de adecuarlas dentro de la administración del Estado, es decir, como nociones útiles para la administración pública chilena.

[2] Por ilustrar, Arreola García (2019) menciona también «los productos y servicios ilegales en internet, la pornografía infantil, el grooming, el ciberespionaje» (p. 28), de manera que su definición contiene estas actividades.

La ciberseguridad, en tanto concepto como visión, se opone a la amenaza, en tanto «circunstancia o evento que puede explotar, intencionadamente o no, una vulnerabilidad específica de un sistema u organización» (Ballestero, 2020, p. 40). Así, una vulnerabilidad, entendida como debilidad, desprotección o descontrol por el cual una amenaza podría generarse, puede conllevar situaciones no intencionadas como incendios, cortes de electricidad o errores no forzados, así como comportamientos intencionados como robo de información, suplantación de titularidades de cuenta, bloqueos de páginas web, etc.

Respecto de las amenazas, su clasificación ha respondido a distintas concepciones dentro de la disciplina de la ciberseguridad. Teóricamente, siguiendo a Lizardo Galvá (2018), se puede establecer la siguiente clasificación de amenaza por:

- Usuario. Remite al uso indebido, impericia o descuido. En este caso, un usuario no se atiene al procedimiento de seguridad de la información. Por ejemplo, la compartición de claves;
- Programa malicioso. Remite a malwares, troyanos, gusanos informáticos, virus, spyware, entre otros. Son desarrollo o programaciones capaces de explotar las vulnerabilidades, aprovechando de utilizar la amenaza en impactos concretos del activo;
- Error de programación. Remite a códigos que encierran vulnerabilidades o brechas susceptibles de explotarse por programas maliciosos o terceras personas;
- Intruso. Remite a «todo aquel que logra entrar a un sistema o acceder a información sin estar autorizado para ello» (Galvá, 2018, p. 65). Es la amenaza conocida por hacker, cracker, en tanto todo personal no autorizado;
- Siniestro. Remite a todo evento que, siendo amenaza, no es intencional. Se incluyen desde catástrofes naturales hasta vulnerabilidad no forzada;
- Personal técnico interno. Remite a todo usuario interno que, intencional o descuidadamente, modifica, roba o filtra información. Por ejemplo, espionaje, comercialización ilícita de datos;
- Fallas electrónicas del sistema. Remite a toda caída de sistema. Esta puede deberse a problemas en el suministro eléctrico, por ejemplo.

Así, quien perpetra la amenaza ha recibido distintas clasificaciones también. Ahora bien, ello escapa en cierta manera del enfoque a esta propuesta, aun cuando la literatura especializada de a poco ha profundizado de manera notoria su estudio (Ballestero, 2020). En buena medida, la persona perpetradora contiene una motivación, además del conocimiento requerido. Por tanto, es por el lado de la motivación por la cual se determina su tipología (por ejemplo, el cibercrimen frente al ciberactivismo).

Contexto Normativo y de Agenda

En Chile, la actual política de ciberseguridad «es el resultado del trabajo iniciado en el año 2015» (Álvarez-Valenzuela, 2018, p. 2). En abril de 2017, en el segundo gobierno de Michelle Bachelet, se presentó la Política Nacional de Ciberseguridad (PNCS) 2017-2022, estableciendo un conjunto de puntos e instrumentos. Sus propósitos a largo plazo se señalaron como (1) resguardar la seguridad de las personas en el ciberespacio, (2) proteger la seguridad del país, (3) promover la colaboración y coordinación entre instituciones y (4) gestionar los riesgos en el ciberespacio (Gobierno de Chile, 2017). Sus objetivos se plantearon así (Gobierno de Chile, 2017):

- «Contar con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos» (p. 16). Introduce la noción clave de infraestructura crítica y, a partir de este, refiere a la creación de *Computer Security Incident Response Team* (CSIRT, en castellano, Equipos de Respuesta a Incidentes de Seguridad Informática).
- Velar por los derechos de las personas en el ciberespacio, contemplando «la prevención, la disuasión y la sanción de ilícitos» (p. 18). Afirmando la realidad del ciberespacio como un contexto transversal y no sectorial, se acentúa el respeto y promoción de la información y la protección de datos, la transparencia y la libertad de expresión como derechos fundamentales.
- Desarrollar una cultura de ciberseguridad. Se busca, a través de políticas de fomento, sensibilización y formación, la adopción individual, organizacional, institucional y

empresarial de «buenas prácticas y responsabilidad en el manejo de tecnologías digitales» (p. 21).

- Coordinar la política internacional de ciberseguridad con otras agencias gubernamentales e incentivar la relación con otros Estados en ciberseguridad. Se busca la colaboración desde y hacia Chile, «el intercambio de información y experiencias, la implementación y profundización de mecanismos de diálogo político en la materia y el empuje de medidas de transparencia y construcción de confianza en el ciberespacio» (p. 22).
- Promover la industria de la ciberseguridad. En este punto, se resalta tanto la innovación de la iniciativa en ciberseguridad como la generación de oferta y demanda de productos de ciberseguridad tanto en el sector privado como público.

Con este marco de objetivos, bajo el gobierno de Sebastián Piñera, se emitió el Instructivo Presidencial N°8/2018, con las órdenes urgentes «en materia de ciberseguridad para la protección de redes, plataformas y sistemas informáticos de los órganos de la administración del Estado». Unido al marco anterior de la PNCS, el instructivo mandata al conjunto de las organizaciones públicas tanto la revisión y actualización de las políticas internas en infraestructuras críticas, la asignación al Centro de Coordinación de Entidades de Gobierno del rol de aseguramiento del funcionamiento de redes y plataformas, como la obligatoriedad de las jefaturas de servicio a diagnosticar y actuar en materia de ciberseguridad.

Con lo anterior, dos años después de la PNCS y uno desde el Instructivo, se estableció el CSIRT a través de la Resolución Exenta N°5.006/2019. El CSIRT se incorporó a la Unidad de Coordinación de Ciberseguridad dependiente del Ministerio del Interior y Seguridad Pública. Además de coordinar con diversos actores públicos y privados, se mandató a la Unidad y el CSIRT «promover planes de capacitación, difusión, educación y el desarrollo de la industria en el marco de los objetivos planteados en la Política Nacional de Ciberseguridad». Se define como un organismo encargado del fortalecimiento y la promoción de buenas prácticas, políticas, leyes, reglamentos, protocolos y estándares en materia de ciberseguridad al interior de la administración. De acuerdo con el RFC 2.350/2021 del CSIRT, la misión es

«reducir los riesgos cibernéticos en las redes del Gobierno de Chile, asesorando a las diferentes organizaciones que lo componen, actuar como socio estratégico en la defensa de las amenazas y colaborar para brindar mayor seguridad y robustez a las infraestructuras del Estado». Ahora bien, este RFC también amplía su ámbito explícitamente: además de las instituciones del Instructivo Presidencial N°8/2018, se incluye a «las instituciones privadas estratégicas, universidades y ONG vinculadas vía convenios de colaboración al CSIRT». Por último, el RFC define el conjunto de servicios que ofrece el CSIRT:

- Gestión y análisis de incidentes o eventos en seguridad informática;
- Mitigación y recuperación-restauración de sistemas informáticos;
- Coordinación de acciones ante incidentes;
- Colaboración en gestión de crisis;
- Gestión de vulnerabilidades;
- Indagación, análisis, coordinación, respuesta y divulgación de nuevas vulnerabilidades;
- Transferencia de conocimientos;
- Concienciación, formación, educación y sensibilización en ciberseguridad; y, finalmente,
- Asesoramiento técnico, político y normativo.

Por último, dentro del encuadre institucional del CSIRT, se encuentra el marco referencial de ciberincidentes: Guía de Notificación de Incidentes para Organismos de la Administración Pública (2021a). En este, se detallan niveles de peligrosidad de la realización de un incidente potencial (Crítico, Muy Alto, Alto, Medio y Bajo), de impacto de ciberincidente (mismos niveles), los contenidos de los reportes, etapas de estos (inicial, intermedio y final), canales de comunicación, tratamiento de reportes y resolución del ciberincidente.

Estas líneas, en general, se han mantenido hacia 2022-2023. El gobierno de Gabriel Boric, en sus lineamientos programáticos, ha acentuado más la arista de los derechos digitales y protección de datos que asuntos vinculados a vigilancia y control de datos.

Marco de Referencia

Actualmente, en la literatura especializada, el abordaje de la ciberseguridad, en tanto política pública dentro de la administración del Estado, implica dos modelos base con sus diferencias y alcances: el modelo de la Unión Europea (UE), a través de la Agencia de la UE para la Ciberseguridad (ENISA, por su sigla en inglés), y el modelo BID-OEA. Se tomarán de estos modelos de referencia elementos para la conformación de uno al caso chileno.

Modelo UE

A partir de un escenario de ciberseguridad en las agendas europeas, ENISA ha desarrollado una herramienta para la evaluación de la ciberseguridad a nivel nacional: el Marco de Evaluación de Capacidades Nacionales (MECN). Su objetivo es proveer a los Estados miembros de la UE de esta herramienta como autoevaluación para establecer niveles de madurez en materia de ciberseguridad. El MECN cuenta con cuatro categorías integradas por distintos objetivos (ENISA, 2020):

- Gobernabilidad y Normas de Ciberseguridad. Esta categoría «mide la capacidad de los Estados miembros para que establezcan la gobernanza, las normas y las buenas prácticas apropiadas en el ámbito de la ciberseguridad» (ENISA, 2020, p. 22).
- Creación de Capacidad y Concientización. En esta, se busca evaluar la capacidad de cada Estado miembro tanto para desarrollo una cultura sobre riesgos y amenazas en ciberseguridad como también los niveles de conocimientos y aptitudes, el desarrollo del mercado de ciberseguridad y los avances en investigación y desarrollo.
- Jurídica y Normativa. En esta, se mide la capacidad para crear marcos jurídicos, es decir, el conjunto de reglas en ciberseguridad para protección de la ciudadanía y empresas.
- Cooperación. En esta categoría, se mide el intercambio de informaciones y la atención a los actores dentro y fuera de cada Estado en el marco europeo.

A partir de estas cuatro categorías y sus objetivos subyacentes, el MECN ha establecido una escala de madurez de capacidades nacionales en ciberseguridad. Dicha escala está conformada en cinco niveles:

- Nivel 1 – Inicial/*Ad-hoc*. Establece que un Estado no cuenta con un planteamiento en ciberseguridad. Ahora bien, se acepta que contenga algunos lineamientos genéricos desde los cuales se pueda avanzar en esta materia.
- Nivel 2 – Definición Temprana. Plantea que un Estado considera planteamientos para mejorar las capacidades, sin embargo, hay acciones y procesos en sus etapas iniciales, aun cuando se hayan asignado responsabilidades y tareas.
- Nivel 3 – Establecimiento. Denota que un Estado cuenta con definiciones claras y asignaciones correspondientes en ciberseguridad y respaldo de interesados. Se observan prácticas unificadas a nivel país, con actividades documentadas, recursos asignados y con plazos prestablecidos, por tanto, bajo una gestión delimitada.
- Nivel 4 – Optimización. Señala que un Estado ha obtenido resultados suficientes para evaluar su plan de acción, de manera que se observan espacios de mejora para rediseñar o adecuar las prácticas.
- Nivel 5 – Adaptabilidad. Implica que un Estado cuenta con una estrategia de ciberseguridad dinámica, retroalimentada y con un marco suficiente para enfrentar nuevos retos y decisiones incluso rápidas ante imprevistos.

Por último, el MECN no evalúa sólo la madurez a través de los niveles antes mencionados, sino que mide también la tasa de cobertura. A través de los indicadores, donde bajo la forma de cuestionario se puntúa tanto cada objetivo, categoría y, finalmente, el país, «la tasa de cobertura se calcula como la proporción entre el número total de preguntas dentro del objetivo y el número de preguntas para las que la respuesta es positiva» (ENISA, 2020, p. 24).

Modelo BID-OEA

En 2020, BID-OEA publicaron un reporte denominado *Ciberseguridad — Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe*. Además de dar un estado de la cuestión, propone un Modelo de Madurez de la Capacidad de Ciberseguridad para evaluar a cada país, «asignándole una etapa específica que corresponde a su grado de logro en materia de ciberseguridad» (BID y OEA, 2020, p. 42). En este caso, plantea cinco etapas de madurez:

- Inicial. Refiere a la inexistencia o fase embrionaria en materia de ciberseguridad. Aun cuando haya algunas aproximaciones y cierta discusión, el país no cuenta con medidas concretas o experiencias primerizas.
- Formativa. Contempla la existencia de aspectos iniciales, en formulación y reciente implementación. Sin embargo, se considera que pueden estar mal definidos o con cierta desorganización, pese a que supone una tendencia a asentar la ciberseguridad, a diferencia de la etapa inicial.
- Consolidada. Remite a la evidencia de «indicadores instalados y funcionando» (BID y OEA, 2020, p. 42). Sin embargo, ha habido escasez de decisiones en la materia y no hay una asignación de recursos suficiente.
- Estratégica. Implica que, partiendo de indicadores operativos, se han tomado decisiones de peso para asentar en el caso del país la ciberseguridad.
- Dinámica. Afirma que hay «mecanismos claros» (BID y OEA, 2020, p. 42), asignación y reasignación de recursos, atención al entorno cambiante, celeridad decisional y tecnología sofisticada en materia de ciberseguridad.

Como se observa, en tanto etapas, supone una escala también en la atención que un Estado presta a ciberseguridad.

Así, cada etapa de madurez se divide en dimensiones «que corresponden a aspectos esenciales y específicos de la ciberseguridad» (BID y OEA, 2020, p. 43). Estas corresponden a (1) Política y Estrategia de Ciberseguridad, (2) Cultura Cibernética y Sociedad, (3) Educación, Capacitación y Habilidades en Ciberseguridad, (4) Marcos Legales y Regulatorios, y (5)

Estándares, Organizaciones y Tecnologías. A su vez, cada dimensión se subdivide en dimensiones de distinto número, dependiendo del ámbito de cada una. Sin embargo, en esto se distingue del MENC de la UE: el método BID-OEA no detalla los indicadores de cada subdimensión, limitándose a mencionarlos. Por ejemplo, en la primera dimensión, está su subdimensión Manejo de Crisis: su indicador se denomina Manejo de Crisis también y posee cinco niveles; sólo se explicita que «los datos primarios utilizados en este reporte se recopilaron mediante un instrumento en línea que se distribuyó a todos los Estados miembros» (BID y OEA, 2020, p. 44).

Por su parte, otra distinción remite a que no hay una especificación del índice que mide el grado de madurez por país. El modelo BID-OEA sólo se limita a especificar los resultados dentro de cada indicador por subdimensión en escala de uno a cinco. No se formula ni presenta un método para resultados generales por dimensión o por Estado.

Modelo de Evaluación de Ciberseguridad en Instituciones Públicas (MECIP)

De los modelos anteriormente presentados, se observa en general que consideran la ciberseguridad en un todo del Estado: es decir, que tanto su aplicación como su evaluación responden al conjunto de la administración y no a una agencia en particular. Justamente, el MECIP propuesto busca atender la implementación, con sus particularidades, en una o en un conjunto delimitado de agencias. Así, sin perjuicio de extraer de los modelos UE y BID-OEA los niveles de madurez, dimensiones, categorías, construcción de índices y medios de verificación y contraste para aplicación comparativa, se sumarán elementos propios de la administración pública chilena. En esto se cuenta el marco normativo antes señalado se toma la siguiente particularidad: este modelo está diseñado tanto para instituciones nacionales como subnacionales.

El presente MECIP propone cuatro dimensiones conformadas por 14 variables cada una. La definición de cada dimensión se fundamenta en los modelos UE y BID-OEA bajo el siguiente esquema:

- Gestión, en tanto levantamiento inicial de activos de información o diagnóstico. Se denomina DGE;

- Prevención, en tanto protección previa o de oficio de información y de activos relevantes de cada agencia. Se denomina DPR;
- Protección y respuesta, en tanto acciones en ejecución o requeridas para activos identificados. Se denomina DRE;
- Cultura y conocimiento, en tanto concienciación y actitud sensible ante la ciberseguridad. Se denomina DCO.

Dimensión Diagnóstico y Gestión DGE

En la dimensión DGE, se busca evaluar las acciones desarrolladas por los servicios en materia de gestión de activos, de riesgos. Las variables, en la forma de preguntas, se enlistan así:

1. ¿La institución cuenta con un proceso permanente para la identificación y actualización de los activos de información?
2. ¿La institución cuenta con un proceso de gestión de riesgos de los activos de información?
3. ¿La institución cuenta con un levantamiento de las formas de comunicación y el flujo de datos asociado a estas?
4. ¿La institución clasifica de forma periódica la información de acuerdo con su grado de sensibilidad?
5. ¿La institución cuenta con integración del proceso de gestión de riesgos (conforme a requisitos del Consejo de Auditoría Interna General de Gobierno CAIGG) y la gestión de riesgos vinculada a Activos de Información?
6. ¿La institución cuenta con Política de Ciberseguridad validada por la autoridad, actualizada y difundida?
7. ¿La institución cuenta con designación formal de Encargado de Ciberseguridad y Suplente Ciberseguridad?
8. ¿La institución cuenta con algún comité o instancia interna revisora de materias de ciberseguridad?

9. ¿La institución cuenta con plan para abordar materias relacionadas con la ciberseguridad?
10. ¿La institución cuenta con involucramiento por parte de la autoridad en materias de ciberseguridad?
11. ¿Los Altos Directivos Públicos (según corresponda) cuentan con actividades o indicadores asociadas a ciberseguridad (en sus convenios de Alta Dirección Pública)?
12. ¿La institución cuenta con presupuesto asignado para cubrir las necesidades en materias de ciberseguridad?
13. ¿La institución cuenta con objetivos, mediables y trazables, anuales en materia de ciberseguridad?
14. ¿La institución realiza de manera sistemática evaluaciones en materia de ciberseguridad?

Dimensión Protección y Respuesta (DRE)

En la dimensión DRE, se busca evaluar las acciones desarrolladas por los servicios en materia de protección de activos de información, protección de usuarios y respuesta ante incidentes. Las variables, en la forma de preguntas, se enlistan así:

1. ¿La institución cuenta con arquitectura tecnológica que proteja los activos críticos de información de la institución?
2. ¿La institución cuenta con procedimientos para gestión de incidentes que incluya la interacción con CSIRT?
3. ¿La institución cuenta con soluciones técnicas para el monitoreo y protección de los servicios de información expuestos a Internet?
4. ¿La institución cuenta con medidas de seguridad para el intercambio de información dentro y fuera de la institución?
5. ¿La institución cuenta con controles de seguridad que protejan la información a la que se accede de forma remota?
6. ¿La institución cuenta con controles de seguridad de firma electrónica avanzada?
7. ¿La institución cuenta con tecnologías de cifrado digital?

8. ¿La institución cuenta con protocolos HTTPS para Webmail?
9. ¿La institución cuenta con herramientas de protección para la navegación en Internet por parte de los usuarios?
10. ¿La institución cuenta con discriminación de privilegios para el acceso a la información por tipo de usuario?
11. ¿La institución ha informado respecto de los sitios o servicios expuestos a Internet que requieren de monitoreo por parte de CSIRT?
12. ¿La institución cuenta con plan de continuidad y procedimientos de recuperación ante incidentes de ciberseguridad?
13. ¿La institución realiza pruebas de restauración de manera periódica con su respectiva evaluación y análisis?
14. ¿La institución cuenta con acuerdos de niveles de servicios (SLA) con los proveedores externos?

Dimensión Prevención (DPR)

En esta dimensión, se busca evaluar las acciones desarrolladas por los servicios en materia de prevención de la ciberseguridad. Se vincula en materias como implementación de herramientas específicas, análisis externos y relación con CSIRT respecto a reportamiento. Las variables, en la forma de preguntas, se enlistan así:

1. ¿La institución cuenta con soluciones técnicas que prevengan o gestionen amenazas del tipo Ransomware, Phishing, DOS, Virus, Malware, robo de información?
2. ¿La institución cuenta con procedimientos de gestión de vulnerabilidades que incluya las reportadas por CSIRT?
3. ¿La institución realiza pruebas de intrusión tipo *ethical hacking* y su posterior análisis?
4. ¿La institución cuenta con políticas y procedimientos para el desarrollo seguro de proyecto de software?
5. ¿La institución cuenta con procedimientos de respaldo de la información actualizados?

6. ¿La institución cuenta con mecanismos de destrucción de información y medios de almacenamiento?
7. ¿La institución contrata asesorías externas para revisar vulnerabilidades?
8. ¿La institución considera, dentro de la planificación de auditorías internas, la revisión de temas relacionados con la Ciberseguridad de manera regular?
9. ¿La institución cuenta con herramientas para monitorear y prevenir la fuga o pérdida de datos?
10. ¿La institución cuenta con herramientas para realizar auditorías respecto de las acciones de los usuarios dentro de la red?
11. ¿La institución implementa acuerdos de confidencialidad con funcionarios y/o terceros con el fin de proteger su información?
12. ¿La institución cuenta con acuerdos de confidencialidad con los proveedores externos?
13. ¿La institución cuenta con procesos de auditoría externa en materia de ciberseguridad?
14. ¿La institución cuenta con procedimientos automatizados y políticas para gestión de contraseñas?

Dimensión Conocimiento y Cultura en Ciberseguridad (DCO)

En esta dimensión, se busca evaluar las acciones desarrolladas por los servicios en materia de formación, gestión de personas, capacitación y difusión. Las variables, en la forma de preguntas, se enlistan así:

1. ¿La institución cuenta con funcionarios con conocimientos en ciberseguridad?
2. ¿El personal directivo de la institución cuenta con conocimientos básicos en ciberseguridad?
3. ¿El personal directivo muestra interés en apoyar las actividades en materias de ciberseguridad?
4. ¿La institución realiza actividades de difusión o sensibilización interna en ciberseguridad?

5. ¿La institución participa en instancias de formación avanzada en ciberseguridad para el personal?
6. ¿La institución cuenta con instancias de aprendizaje sobre incidentes de ciberseguridad ya acontecidos (internos o de otros servicios)?
7. ¿La institución contempla, en el plan anual de capacitación, tópicos relativos a ciberseguridad?
8. ¿La institución cuenta con convenios con otras instituciones para la formación en ciberseguridad?
9. ¿Se realizan instancias de actualización formativa, en la institución, en nuevas herramientas en ciberseguridad?
10. ¿La institución revisa periódicamente fuentes de información externas respecto de materias de ciberseguridad?
11. ¿La institución revisar permanentemente boletines y campañas que realiza CSIRT?
12. ¿La institución realiza un proceso de inducción al personal nuevo en materias de ciberseguridad?
13. ¿La institución participa de instancias de cooperación intergubernamental en materia de ciberseguridad?
14. ¿La institución realiza procesos de innovación respecto de materias de ciberseguridad?

Niveles de Cumplimiento

Cada variable implica un nivel de cumplimiento. El MECIP establece, pues, tres niveles de cumplimiento que implica valores (0, 1, 2). De esta manera, por cada pregunta hay una respuesta cuyo valor es de (0, 1 ó 2); la sumatoria de las respuestas valora a su vez la dimensión. La sumatoria de todas las dimensiones evalúa el cumplimiento total de la institución y, de manera relativa, cada dimensión pondera su cumplimiento con respecto a este total y en comparación con las otras dimensiones. En Tabla 1 se presenta la descripción del nivel de cumplimiento.

La representación gráfica del desarrollo institucional considera un modelo de telaraña (véase Gráfico 1). La línea azul presenta el resultado obtenido finalmente por la institución con las puntas valorando cada dimensión; la línea roja es el resultado óptimo por dimensión, es decir, 28 puntos por dimensión.

Tabla 1

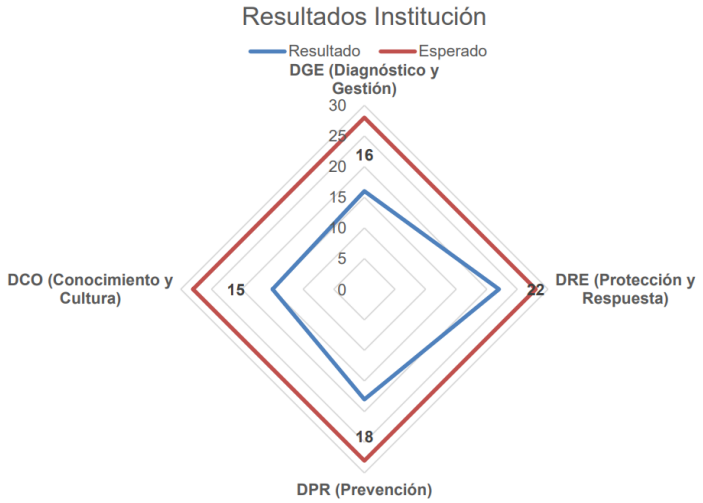
Niveles de Cumplimiento por Variable

Nivel	Descripción	Valor
No Cumple	Las acciones vinculadas a este aspecto no han sido desarrolladas por la institución. No existe evidencia razonable de una preocupación efectiva en la materia.	0
Cumple Parcialmente	Se cuenta con el desarrollo de acciones relacionadas al aspecto, pero existen elementos no completados o de consiguiente profundización para implementación. Se reconoce como ejecución en curso, implementación parcial o en proceso.	1
Cumple	Se cuenta con implementación de acciones relacionadas con el aspecto. Las acciones están establecidas como práctica permanente en la institución, se revisan con frecuencia determinada y se propone su mejora continua.	2

Nota. Fuente: elaboración propia.

Gráfico 1

Ejemplo de Representación Gráfica de Resultados



Nota. Fuente: elaboración propia.

Tipificación del Nivel de Madurez Institucional

De acuerdo con lo anterior, el MECIP propone cuatro niveles de evaluación institucional. Utilizando la terminología de los modelos anteriormente considerados, estos son niveles de madurez. En Tabla 2 se presenta de manera resumida estos niveles.

Tabla 2

Tipificación de Madurez Institucional en Ciberseguridad

Nivel de Madurez Institucional	Insuficiente	Básico	Intermedio	Avanzado
Resultados de Cumplimiento (%)	0-24%	25-49%	50-74%	75-100%
Color				

Nota. Fuente: elaboración propia.

El primer nivel es «Insuficiente». De color rojo, refiere a la inexistencia de acciones o medidas en materia de ciberseguridad o cuyas actividades son escasas. En este nivel, la institución debió obtener un porcentaje de la sumatoria de las respuestas menor al 24%.

El segundo nivel es «Básico». De color amarillo, refiere a la evidencia de un grado inicial de ciberseguridad, con iniciativas; no obstante, no hay un programa, plan, estrategia o política establecida de manera permanente y sólida. En este nivel, la institución debió obtener un porcentaje de la sumatoria de las respuestas entre el 25 y 49%.

El tercer nivel es «Intermedio». De color verde claro, refiere a la evidencia de acciones y lineamientos formalizados, con pretensión de continuidad y con asignación de responsabilidades. En este nivel, la institución debió obtener un porcentaje de la sumatoria de las respuestas entre el 50 y 74%.

El cuarto nivel es «Avanzado». De color verde oscuro, refiere a la evidencia de acciones, lineamientos y estrategias permanentes, con responsabilidades asignadas y con perspectivas de retroalimentación. En este nivel, la institución debió obtener un porcentaje de la sumatoria de las respuestas superior al 75%.

La clasificación de la institución en uno de estos niveles permite establecer el resultado Meta u Objetivo para el período siguiente. Con base en la metodología PDCA o Ciclo

Deming, se circunscribe esta clasificación entre las etapas Check (verificación de herramienta) y Act (acuerdo para plan de mitigación del período siguiente).

Método de Aplicación MECIP en Instituciones

Por último, se realizará una aplicación en dos instituciones como primera aproximación a la propuesta de MECIP. Para ello, se considerará el siguiente proceso de aplicación cuyas etapas son las siguientes:

1. Contexto. Identificación de la institución, su vinculación en el organigrama de la administración del Estado y aproximación al presupuesto.
2. Coordinación. Identificación de actores relevantes para realización de entrevistas.
3. Inducción MECIP. Aproximación a la metodología MECIP para actores relevantes.
4. Levantamiento de Información. Aplicación del levantamiento de información a través de las dimensiones de MECIP y sus variables por medio de entrevistas.
5. Análisis de Datos. Análisis de las entrevistas y sus respuestas para asignación de valores a las variables.
6. Representación de Resultados. Ordenamiento de las variables con sus respectivos valores e ilustración de resultados por dimensión y comparación con línea óptima.
7. Tipificación de Nivel de Madurez. Entrega de resultados a nivel institucional de acuerdo con nivel de madurez.
8. Proposición de Plan de Acción. Como parte de una retroalimentación y agregación de valor, se presenta un insumo propositivo de Plan de Acción a partir del Nivel de Madurez.

En esta ocasión, el MECIP realizó su aplicación en la Superintendencia de Insolvencia y Reemprendimiento (SUPERIR) y la Fiscalía Nacional Económica (FNE). Ambas se vinculan con el Ministerio de Economía, Fomento y Turismo de Chile.

Aplicación del MECIP en SUPERIR y FNE

Aplicación en Superintendencia de Insolvencia y Reemprendimiento (SUPERIR)

La Ley N°20.720[3] publicada en 2014, en su capítulo IX, establece la creación de la Superintendencia de Insolvencia y Reemprendimiento de naturaleza descentralizada. En su art. 332, se definen sus funciones como:

> Supervigilar y fiscalizar las actuaciones de los Veedores, Liquidadores, Martilleros Concursales, administradores de la continuación de las actividades económicas del deudor, asesores económicos de insolvencia y, en general, de toda persona que por ley quede sujeta a su supervigilancia y fiscalización.

Vía correo electrónico, se logró contacto con el encargado de ciberseguridad Pablo Valladares, jefe de gabinete del superintendente. A partir de este contacto, se derivó a dos profesionales encargadas de seguridad de información (Ximena Guzmán) y del área de control de gestión (Ana Hernández, quien fuera suplente de ciberseguridad durante 2022). Las entrevistas se realizaron vía Google Meet en enero de 2023.

En la dimensión DGE, la SUPERIR obtiene un resultado intermedio, con un 57% del todo (16 sobre 28 puntos). En las variables vinculadas a materia presupuestaria (pregunta 12) y definición de objetivos (pregunta 13), SUPERIR no cumple. En cuatro preguntas cumple cabalmente, a saber, números 4, 7, 8 y 10. En las restantes, sólo cumple parcialmente.

En la dimensión DRE, se observa que la SUPERIR cumple con un nivel avanzado, a saber, en torno a un 79% (22 puntos sobre 28). Registra un único No Cumple: sobre pruebas de restauración (pregunta 13). A su vez, en sólo 4 variables la SUPERIR cumple de manera parcial: en las preguntas 2, 3, 5 y 12. En lo demás, cumple cabalmente.

En la dimensión DPR, la SUPERIR obtiene en torno al 64% con 18 sobre 28 puntos. La institución no cumple en las variables sobre *ethical hacking* (pregunta 3), herramientas para

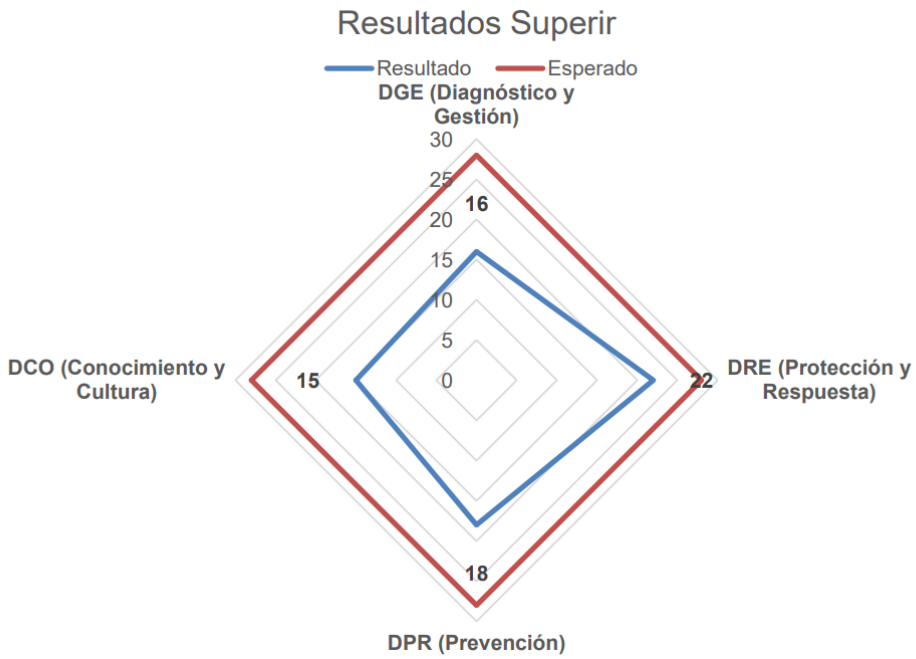
[3] Titulada como: Sustituye el Régimen Concursal Vigente por una Ley de Reorganización y Liquidación de Empresas y Personas, y Perfecciona el Rol de la Superintendencia del Ramo.

la prevención de fuga de información (pregunta 9) y sobre procesos de auditoría externa (pregunta 13). De manera parcial, sólo alcanza a cumplir las variables 7, 8, 10 y 12. En las restantes, cumple de manera cabal. Cabe señalar, en esta dimensión, que el ámbito de auditoría externa es sensible: por un lado, la institución sí contempla la contratación de asesorías externas, en tanto cumple de manera parcial esto (pregunta 7); no obstante, por otro, no cuenta con la realización de estos procesos (pregunta 13).

En la dimensión DCO, la SUPERIR alcanza sólo un 54% (15 sobre 28 puntos), siendo la dimensión más baja de las cuatro. Hay cuatro preguntas cuyas respuestas manifiestan que la SUPERIR no está cumpliendo (5, 8, 9 y 14); otras cinco son de carácter parcial en su eficacia, vinculadas a las preguntas 1, 3, 6, 10 y 13; y, finalmente, otras cinco son de cumplimiento cabal, en las preguntas 2, 4, 7, 11 y 12.

Gráfico 2

Resultados de Aplicación MECIP a SUPERIR



Nota. Fuente: elaboración propia.

Evaluación General

De acuerdo con el Gráfico 2 y las Tablas 3 y 4, la SUPERIR contiene un nivel de madurez en ciberseguridad de carácter intermedio de un 63%.

Las dimensiones más bajas responden al Conocimiento y Cultura, por un lado, y al Diagnóstico y Gestión, por otro. La prevención está más cerca que las antedichas dimensiones en alcanzar un nivel avanzado. A su vez, la dimensión de protección y respuesta se encuentra en un nivel avanzado, aun cuando caben espacios de mejora.

Tabla 2

Resumen de Resultados por Dimensión SUPERIR

Dimensión	Puntuación Efectuada	Puntuación Esperada	Evaluación [%]
DGE – Diagnóstico y Gestión	16	28	**57**
DRE – Protección y Respuesta	22	28	**79**
DPR – Prevención	18	28	**64**
DCO – Conocimiento y Cultura	15	28	**54**
Resultado General			**63%**

Nota. Fuente: elaboración propia.

Tabla 3

Nivel de Madurez SUPERIR

Nivel de Madurez Institucional	Insuficiente	Básico	Intermedio	Avanzado
Resultados de Cumplimiento (%)	0-24%	25-49%	50-74%	75-100%
Color				

Nota. Fuente: elaboración propia.

Aplicación en Fiscalía Nacional Económica (FNE)

A partir del Decreto-Ley DL N°211 de diciembre de 1973[4], fija en su artículo 1° que su objetivo es «promover y defender la libre competencia en los mercados». Para ello, el artículo 2° determina la asignación de responsabilidades al Tribunal de Defensa de la Libre Competencia y a la FNE. Así, en su título III, la FNE se define como servicio público descentralizado también bajo supervigilancia a través del Ministerio de Economía. En su artículo

[4] Cuyo título es: «Fija Normas para la Defensa de la Libre Competencia».

39 se delimitan sus atribuciones, entre otras, la instrucción de las investigaciones procedentes para comprobar las infracciones a la ley de libre de competencia y la representación del interés general en el orden económico ante dicho Tribunal y los tribunales de justicia.

A través de la jefa de división de Administración y Gestión, se logró el contacto y la venia para la entrevista con Cristian Mella, suplente de ciberseguridad. Durante el mes de diciembre, se realizó la entrevista de manera presencial en dependencias de FNE.

En la dimensión DGE, FNE obtuvo un 64%, es decir, un nivel intermedio de 18 sobre 28 puntos. Sólo posee un no-cumplido: la variable vinculada a levantamiento de flujos de información y comunicación (pregunta 3). De allí, cinco preguntas manifiestan una realidad cuyo cumplimiento es pleno: preguntas 5, 6, 7, 8 y 10. Las restantes variables poseen un cumplimiento parcial.

En la dimensión DRE, FNE refleja un nivel de 75%, de 21 sobre 28 puntos. Con sólo una variable no-cumplida, vinculada a pruebas de restauración, posee seis de cumplimiento parcial (preguntas 3, 4, 5, 12, 13 y 14) y las restantes siete de cumplimiento pleno.

En la dimensión DPR, el resultado fue de 85% (24 sobre 28 puntos). Sólo registra una única variable no cumplida: sobre aplicación de procedimiento para destrucción de información y medios de almacenamiento (pregunta 6). A su vez, sólo dos variables contemplan un cumplimiento parcial, correspondiente a las preguntas 1 (sobre soluciones de amenazas como Ransomware, phishing, entre otros) y 8 (sobre la consideración de asuntos sobre ciberseguridad en las auditorías internas). En todas las demás variables, FNE cumple cabalmente.

En la dimensión DCO, FNE obtiene un 71%, vale decir, 20 sobre un total de 28 puntos posibles. Hay tres variables que no se cumplen: convenios con otras instituciones de formación en ciberseguridad (pregunta 8), instancias de actualización formativa en nuevas herramientas (pregunta 9) y realización de procesos de innovación (pregunta 14). Sólo se registran dos preguntas cuyos resultados son parciales: pregunta 6 sobre instancias de aprendizaje a partir de incidentes y pregunta 10 sobre revisión periódica de fuentes de información externas en ciberseguridad. En lo demás, FNE cumple cabalmente.

Evaluación General

Aun cuando se observa, en Tabla 4, que dos de las cuatro dimensiones posee sobre el 75%, el promedio de las cuatro dimensiones llega al 74%, es decir, al límite del nivel intermedio previo al nivel avanzado.

Asimismo, el Gráfico 3 ilustra de mejor manera la cercanía más por dimensión que en general de la FNE al modelo óptimo propuesto por MECIP. Destaca el DPR, muy cercano en cuatro puntos a su realización cabal. A su vez, en el lado opuesto, también se manifiesta la brecha, entendida a su vez como espacio de mejora, en la dimensión DGE.

Tabla 4

Resumen de Resultados por Dimensión FNE

Dimensión	Puntuación Efectuada	Puntuación Esperada	Evaluación [%]
DGE – Diagnóstico y Gestión	18	28	**64**
DRE – Protección y Respuesta	21	28	**75**
DPR – Prevención	24	28	**86**
DCO – Conocimiento y Cultura	20	28	**71**
Resultado General			**74%**

Nota. Fuente: elaboración propia.

Tabla 5

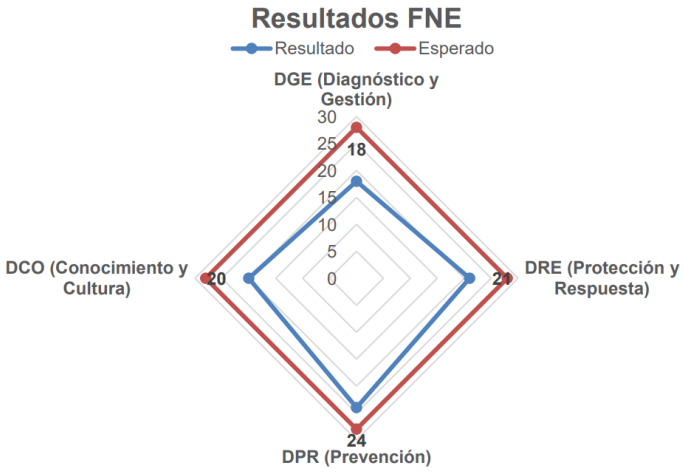
Nivel de Madurez FNE

Nivel de Madurez Institucional	Insuficiente	Básico	Intermedio	Avanzado
Resultados de Cumplimiento (%)	0-24%	25-49%	50-74%	75-100%
Color				

Nota. Fuente: elaboración propia.

Gráfico 3

Resultados de Aplicación MECIP a FNE



Nota. Fuente: elaboración propia.

Consideraciones Finales

A través del Modelo de Evaluación de Ciberseguridad en Instituciones Públicas (MECIP), el cual recoge elementos tanto de la Política Nacional de Ciberseguridad de Chile como de los modelos de la Agencia de la Unión Europea para la Ciberseguridad y de la Organización de Estados Americanos con el Banco Americano de Desarrollo, se diseñó y aplicó de manera exploratoria un modelo aplicable a cada institución de la administración pública chilena, sea de carácter nacional o subnacional. Se ha buscado, pues, recoger buenas prácticas internacionales como los ámbitos de implementación en el marco chileno.

Para el diseño del MECIP, se consideró un conjunto de cuatro dimensiones con catorce variables cada una. El valor de cada variable es 0, 1 y 2 manifestando respectivamente «no cumplimiento», «cumplimiento parcial» y «cumplimiento». Así, cada variable posee un máximo de 28 puntos sobre los cuales hay niveles de progresión: insuficiente, básico, intermedio o avanzado. Asimismo, estos niveles de maduración se aplican a la institución completa. Las dimensiones corresponden a Diagnóstico y Gestión, Prevención, Protección y Respuesta, y Conocimiento y Cultura. Todo este conjunto se deriva de las aproximaciones realizadas a los modelos antedichos.

Este modelo está diseñado para una implementación simple cuya perspectiva no desincentive su uso por una terminología tecnificada. Como se observa, la evaluación no está pensada sólo para profesiones vinculadas a la materia de ciberseguridad: directivos, auditores, administradores, controladores pueden aplicarla. De manera eficaz y celera, se puede ejecutar y dar tanto con el panorama institucional como con los espacios de mejora.

La aplicación del MECIP se realizó a dos instituciones: Superintendencia de Insolvencia y Reemprendimiento y Fiscalía Nacional Económica, ambas vinculadas bajo supervigilancia al Ministerio de Economía, Fomento y Turismo. Ambas instituciones obtuvieron resultados de nivel intermedio de maduración, aun cuando hay matices: mientras la primera llega sólo al 63% sobre el total óptimo, la segunda está próxima al nivel avanzado, a un punto de este. En cualquier caso, son resultados positivos. Sin perjuicio de esto, no obstante, hay oportunidades de mejora: de esto dependerá los procesos decisorios que cada proceso estratégico tome.

Perspectivas Futuras

El sector público chileno ha generado, de manera dispersa quizás, aproximaciones a la ciberseguridad. Por ilustrar, las instituciones antedichas han mantenido la implementación del Sistema de Seguridad de la Información cuyo origen se remonta a la aplicación de las Medidas de Eficiencia Institucional (MEI). Esto ha generado una mejor perfilación para enfrentar los desafíos en esta materia.

Con todo, desde distintas aristas, quedan asuntos pendientes. En primer lugar, se encuentra en discusión en las agendas legislativas la creación o el rediseño de una institucionalidad dedicada a ciberseguridad. El CSIRT ha representado, en este sentido, una aproximación que, según se puede apreciar, ha cumplido con un desempeño positivo.

Referencias

Abal Medina, J. M. (2010). *Manual de Ciencia Política*. Eudeba.

Aguilar Antonio, J. M. (2021). Retos y Oportunidades en Materia de Ciberseguridad de América Latina frente al Contexto

Global de Ciberamenazas a la Seguridad Nacional y Política Exterior. *Estudios Internacionales*, 53 (198), 169-197. https://doi.org/10.5354/0719-3769.2021.57067

Álvarez-Valenzuela, D. (2018). Ciberseguridad en América Latina y Ciberdefensa en Chile. *Revista Chilena de Derecho y Tecnología*, 7 (1), 1-2. https://doi.org/10.5354/0719-2584.2018.50416

Arreola García, A. (2019). Desafíos a las Estrategias de Ciberseguridad en América. *Revista del Centro de Estudios Superiores Navales*, 40 (4), 25-49. http://repositorio.uninav.edu.mx/xmlui/handle/123456789/1042

BID-OEA. (2020). *Ciberseguridad. Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe.* Servicio de Publicaciones del Banco Interamericano de Desarrollo y Organización de Estados Americanos. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Boric, Gabriel. (2021). Programa de Gobierno. https://boricpresidente.cl/propuestas/derechos-sociales/

Ballestero, F. (2020). La Ciberseguridad en Tiempos Difíciles. *Boletín Económico de ICE*, (3122), 39-48. https://doi.org/10.32796/bice.2020.3122.6993

CSIRT. (2021). *Guía de Notificación de Incidentes para Organismos de la Administración Pública*. Ministerio del Interior y Seguridad Pública. https://www.csirt.gob.cl/media/2021/10/Guia-de-notificacion-ciberincidentes.pdf

CSIRT. (2021). *RFC 2350 del CSIRT de Gobierno. Equipo de Respuesta ante Incidentes de Seguridad Informática*. Ministerio del Interior y Seguridad Pública. https://www.csirt.gob.cl/media/2021/10/RFC2350-final.pdf

Dye, T. R. (2008). *Understanding Public Policies*. Pearson Prentice Hall.

ENISA. (2020). *Marco de Evaluación de las Capacidades Nacionales*. Agencia de la Unión Europea para la Ciberseguridad (ENISA). https://www.enisa.europa.eu/publications/report-files/ncaf-

translations/national-capabilities-assessment-framework-es.pdf

Fonfría, A. y Duch-Brown, N. (10 de noviembre, 2020). Elementos para una Política de Ciberseguridad Efectiva. *Real Instituto Elcano*. https://www.realinstitutoelcano.org/analisis/elementos-para-una-politica-de-ciberseguridad-efectiva/

Gobierno de Chile. (2017). *Política Nacional de Ciberseguridad 2017-2022*. Servicio de Publicaciones Comité Interministerial sobre Ciberseguridad. http://163.247.42.118/transparencia/POL/PNCS.pdf

GSMA (2022). *The Mobile Economy 2022*. GSMA Intelligence. https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf

Lizardo Galvá, R. (2018). La Seguridad de la Información: desde la Antigüedad hasta el Internet de las Cosas. *Revista Seguridad, Ciencia & Defensa*, 4 (4), 60-69. https://doi.org/10.59794/rscd.2018.v4i4.47

Panetta, K. (October 20th, 2021). The Top 8 Cybersecurity Predictions for 2021-2022. *Gartner* https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022

Sorokin, P., Sotomayor Saavedra, M. A., Bórquez Polloni, B., Martí, M., Duro, A., Quiroz Malca, E.,… Vergès, C. (2020). Datos en Tiempos de Pandemia: la Urgencia de un Nuevo Pacto. Reflexiones desde América Latina y el Caribe. *Revista de Bioética y Derecho*, (50), 221-237. http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872020000300014&lng=es&tlng=es

Weber, M. (1969). *Economía y Sociedad. Esbozo de Sociología Comprensiva*. Fondo de Cultura Económica.