Ciberseguridad: ¿Cómo nos va en los rankings?

Alejandro Barros C.[1]

En el último tiempo, hemos visto la publicación de dos índices de ciberseguridad me refiero al *Global Cybersecurity Index* (GCI) elaborado por la agencia de Naciones Unidas, Unión Internacional de Telecomunicaciones ITU, y el National Cyber Security Index – NCSI.

El NCSI está desarrollado por Estonia[2], en su versión actual nuestro país aparece bastante bien posicionado, lo que ha sido profusamente destacado por nuestras autoridades en materias digitales, ya que hemos avanzando 30 posiciones desde la medición anterior desde la posición 56 a la 27[3], este avance ya es llamativo y si a eso agregamos que tanto República Dominicana (21) como Gana (25) aparecen mejor ranqueados, esto enciende otras alerta respecto de la calidad metodológica del referido índice. Sobre este último indicador, hay varias cosas que llaman la atención y al menos en su versión anterior me generaron algunas dudas metodológicas, las cuales he expresado en el pasado[4].

Pero en este espacio quiero profundizar en los resultados del índice de la ITU, el *Global Cybersecurity Index* (GCI) 2024[5], esta es ya su quinta versión, nuestro país muestra un peor desempeño que en el NCSI, y quedó en un lugar relativamente rezagado, incluso comparado con algunos países de América Latina. El indicador evalúa 5 dimensiones o pilares.

- **Medidas legales:** Evalúa la existencia y efectividad de leyes y regulaciones específicas que aborden la ciberseguridad, como aquellas relacionadas con el **ciberdelito**, la **protección de datos personales**, la **privacidad en línea**, y las **notificaciones de brechas de seguridad**.

- **Medidas técnicas**: Evalúa la **implementación de capacidades técnicas** a nivel nacional, tales como la existencia de **equipos de respuesta a incidentes de ciberseguridad** (CIRTs), sistemas de protección de infraestructuras críticas, y marcos técnicos que adopten estándares internacionales.

---

[1] Alejandro Barros C, Profesor Adjunto – Departamento de Ingeniería Industrial, Universidad de Chile. Perito Judicial de la Corte de Apelaciones de Santiago

[2] National Cyber Security Index – NCSI - https://ncsi.ega.ee/ncsi-index/?order=rank

[3] Chile escala 30 puestos en el ranking de Ciberseguridad, El Mostrador - https://ciberseguridad.gob.cl/noticias/chile-escala-30-puestos-en-ranking-mundial-de-ciberseguridad-y-queda-25-en-2024/

[4] Ciberseguridad, algunos rankings hay que tomarlos con pinzas - https://www.alejandrobarros.com/ciberseguridad-algunos-rankings-hay-que-tomarlos-con-pinzas/

[5] Global Cybersecurity Index (GCI) 2024 - https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

- **Medidas organizacionales**: Evalúa la existencia de **estrategias nacionales de ciberseguridad**, **planes de acción** y la **organización de entidades dedicadas a la ciberseguridad**, así como la claridad en roles y responsabilidades dentro del gobierno y el sector privado.

- **Medidas de desarrollo de capacidades**: Analiza los **esfuerzos para educar y entrenar** tanto a profesionales en ciberseguridad como a la población en general. Esto incluye la existencia de programas de formación, concienciación y el desarrollo de capacidades a largo plazo a nivel nacional.

- **Medidas de cooperación**: Mide el grado de **colaboración y cooperación** entre entidades nacionales e internacionales, así como las asociaciones público-privadas. Esto incluye la participación en acuerdos internacionales, la colaboración interinstitucional y la implementación de marcos cooperativos para el intercambio de información.

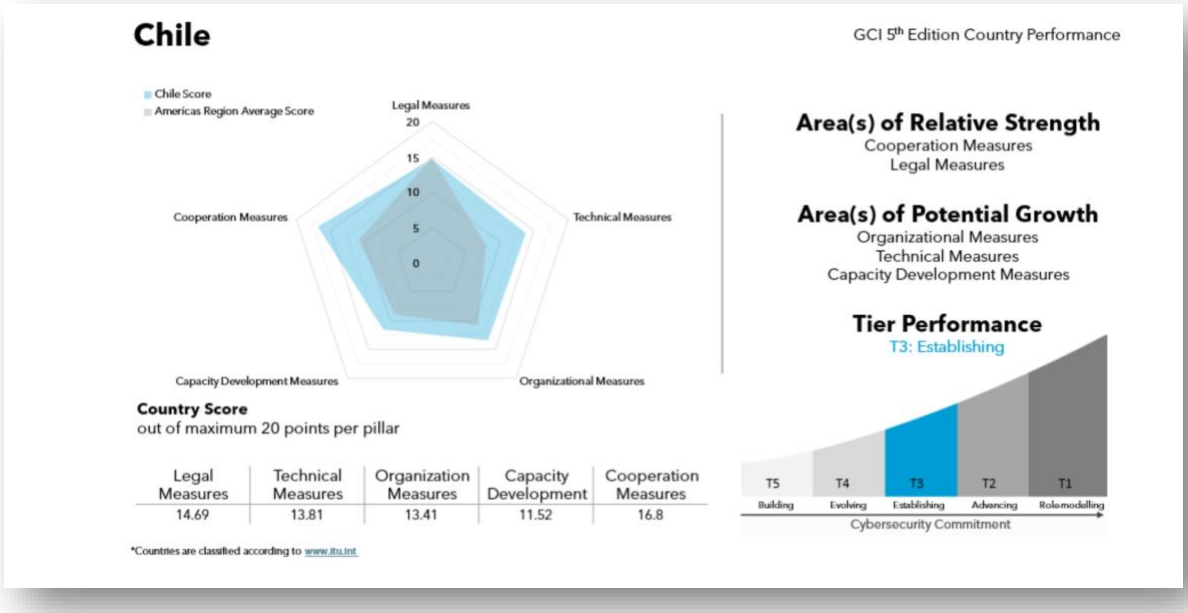
Estos cinco pilares ofrecen una visión completa del **nivel de madurez** de un país en términos de su preparación y capacidad para hacer frente a los retos y amenazas de ciberseguridad.

El *Global Cybersecurity Index* (GCI) clasifica a los países en **cinco niveles (tiers)** según su compromiso con la ciberseguridad. Estos niveles ayudan a identificar el progreso de los países en cinco pilares.

Nivel	***Descripción***	***Características***
Tier 1: Role-modelling (Ejemplar)	Este es el nivel más alto del ranking. Los países en este nivel son **líderes mundiales en ciberseguridad** y sirven como modelo a seguir para otros. Tienen implementados marcos de ciberseguridad robustos y efectivos en todas las áreas clave.	Poseen legislaciones avanzadas, agencias de ciberseguridad bien desarrolladas, capacidades técnicas sólidas y una fuerte cooperación tanto a nivel nacional como internacional. Además, están comprometidos con el desarrollo continuo de talento y tecnologías de ciberseguridad
Tier 2: Advancing (Avanzando)	Estos países están avanzando rápidamente en la implementación de medidas de ciberseguridad, pero aún no alcanzan el nivel de los líderes mundiales.	Han implementado **buenas prácticas** en varias áreas, aunque aún pueden mejorar en ciertos aspectos, como el desarrollo de capacidades o la coordinación interinstitucional. Los marcos legales y técnicos están en progreso o parcialmente implementados.
Tier 3: Establishing (Estableciendo)	Los países en este nivel están en proceso de **desarrollar e**	Tienen medidas básicas en algunas áreas, pero **carecen de**

	implementar sus estrategias y capacidades de ciberseguridad	**integraciones completas** o de políticas totalmente desarrolladas en otras. A menudo, enfrentan desafíos en la implementación técnica y en la formación de talento, y la cooperación internacional es más limitada
Tier 4: Evolving (Evolucionando)	Estos países están en una fase temprana de desarrollo en términos de ciberseguridad. Han comenzado a implementar algunas medidas, pero les falta **madurez en muchas áreas clave**.	Suelen tener limitaciones significativas en la implementación técnica, en la protección de infraestructuras críticas y en la concienciación pública. Aunque han adoptado algunas normativas, aún no tienen una estrategia clara y bien implementada.
Tier 5: Building (Construyendo)	Es el nivel más bajo del ranking. Estos países están **en las primeras etapas** de desarrollar su infraestructura y capacidad en ciberseguridad	Carecen de marcos legales, técnicos y organizativos sólidos, y están comenzando a trabajar en el desarrollo de capacidades. En muchos casos, estos países enfrentan limitaciones severas de recursos y carecen de la infraestructura necesaria para gestionar eficazmente las amenazas cibernéticas

Nuestro país se encuentra clasificado en el nivel *Tier 3 - Estableciendo*, lo que significa que, ***aunque ha avanzado en el desarrollo de sus capacidades de ciberseguridad, pero todavía tiene áreas por mejorar para alcanzar niveles más altos de compromiso con la ciberseguridad***. Al revisar la versión anterior (2020) del ranking si bien no son del todo comparables, ya que hubo cambio del marco metodológico, nuestro país no avanzó demasiado (ver análisis de las mediciones anteriores en).



Fuente: Global Cybersecurity Index (GCI) 2024

Desde un punto de vista legal se ha avanzado en actualizar el marco normativo, recordemos que antes de la última actualización de nuestro marco legal de delito informático, la ley tenía 30 años, era de 1993. De hecho, producto de los últimos cambios, es la dimensión en la cual nuestro país se encuentra en una mejor posición respecto de sus pares en América Latina.

Hoy se cuenta con un marco regulatorio bastante más actualizado, pero con un desafío considerable, esto es, el proceso de la implementación de los cambio, ya que en algunos ámbitos involucran la implementación de institucionalidad asociada, incluyendo la puesta en marcha de la Agencia Nacional de Ciberseguridad, institucionalidad fundamental de la nueva ley marco de ciberseguridad.

En el ámbito de las capacidades técnicas, una de las dimensiones más bajas (junto a medidas de colaboración) si bien ha establecido capacidades técnicas como la creación de Equipos de Respuesta a Incidentes Informáticos (CSIRT), el país puede mejorar en la integración y optimización de estas capacidades a nivel sectorial y nacional.

En los últimos años, Chile ha visto un significativo incremento en los ataques dirigidos a instituciones gubernamentales. Con algunos casos bastante notorios, tales como: Banco Estado en 2020[6], Estado Mayor

[6] https://www.elmostrador.cl/destacado/2020/09/07/el-lunes-negro-de-banco-estado-gobierno-admite-ataque-cibernetico-muy-profundo-y-la-fiscalia-inicia-investigaciones-con-la-pdi/

Conjunto en 2022[7] y Chilecompra en 2023[8] y el prestador de servicios tecnológicos GTD[9] que según informaciones de prensa le daba servicios a cerca de 3.000 clientes, por mencionar algunos casos en los últimos años.

Otro desafío relevante es la **Baja madurez en la ciberseguridad de las PYMEs**. En nuestro país, más del 90% de las empresas son **pequeñas y medianas empresas (PYMEs)**, y la gran mayoría no cuenta con políticas de ciberseguridad robustas. Muchas de ellas, no cuentan con presupuesto ni acceso a tecnologías avanzadas para proteger sus datos y sistemas, lo que las deja expuestas a ciberataques.

Chile cuenta con una vasta infraestructura crítica en sectores clave como la **minería**, **energía y telecomunicaciones**, que son fundamentales para la economía del país. El desafío en el ámbito de la ciberseguridad, radica en que muchas de estas industrias aún no cuentan con los niveles de protección adecuados frente a amenazas cibernéticas.

Otro elemento fundamental es la **Escasez de profesionales especializados en ciberseguridad, a**l igual que en otros países, Chile enfrenta una **escasez de talento en esta área**. A pesar del crecimiento de carreras técnicas y especializaciones, la demanda de profesionales especializados excede con creces la oferta disponible. Esto pone en desventaja tanto al sector público como privado, que no cuenta con los recursos humanos adecuados para gestionar y mitigar riesgos cibernéticos.

Finalmente, el nivel de conciencia limitada en la ciudadanía, aunque la digitalización ha avanzado rápidamente en Chile, especialmente con la expansión de la banca digital, la telemedicina y el comercio electrónico, la **conciencia ciudadana sobre los riesgos cibernéticos** sigue siendo relativamente baja. Muchas personas desconocen los peligros del robo de identidad, los fraudes electrónicos y cómo proteger sus dispositivos.

Si bien todos estos indicadores (rankings) tienen algunos elementos metodológicos que llaman la atención desde una dimensión metodológica, permiten identificar los principales desafíos, más aún al analizar la serie y su evolución.

Es de esperar que las próximas versiones nuestro país pueda avanzar al siguiente nivel de madurez.

[7] https://www.ciperchile.cl/2022/09/22/hackeo-masivo-al-estado-mayor-conjunto-expuso-miles-de-documentos-de-areas-sensibles-de-la-defensa/
[8] https://www.df.cl/economia-y-politica/laboral-personas/problema-de-ciberseguridad-afecta-a-mercado-publico
[9] https://www.emol.com/noticias/Economia/2023/11/14/1112861/hackeo-gtd-empresas-publicas.html