





# REVISTA DE ASUNTOS INTERNACIONALES, DEFENSA Y SEGURIDAD

---

**NUEVOS DESAFÍOS  
DE LA SEGURIDAD  
GLOBAL**

---



**Revista de Asuntos Internacionales,  
Defensa y Seguridad**

Pontificia Universidad Católica de Valparaíso



PONTIFICIA  
UNIVERSIDAD  
CATÓLICA DE  
VALPARAÍSO



Centro de  
Estudios y  
Asistencia  
Legislativa

Pontificia  
Universidad  
Católica de  
Valparaíso Chile

## REVISTA RAIDS PUCV

Edición N° 2, primer semestre del año 2024

### DIRECTOR

GIANNI RIVERA FOO

### CONSEJO EDITORIAL

ALAN BRONFMAN VARGAS

CATALINA SCHERPING BÓRQUEZ

CARLOS VERGARA EHRENBURG

ESTEBAN VERGARA POBLETE

### COLABORADORES

GILBERTO ARANDA

GABRIELLA THOMAZY

MARÍA JOSÉ ESCOBAR

ALBERTO GUERRERO

KENNETH PUGH

SERGIO MUÑOZ

CATALINA SCHERPING

### EDICIÓN

ANDREA HÖLZEL VÁSQUEZ

### DISEÑO

MAURICIO GUERRA POBLETE

Publicación editada por el Centro de Estudios y Asistencia Legislativa (CEAL) de la Pontificia Universidad Católica de Chile (PUCV) e impreso en Impresos San José.

Todos los artículos son de responsabilidad de sus autores y no reflejan necesariamente la opinión del CEAL y la PUCV. Está autorizada su reproducción mencionando la revista y el autor.

Centro de Estudios y Asistencia Legislativa de la Pontificia Universidad Católica de Valparaíso (CEAL). Avenida Brasil 2950, Valparaíso. Teléfono (56 32) 227 3634. Comentarios y propuestas de artículos a [raids@pucv.cl](mailto:raids@pucv.cl).



**NELSON VÁSQUEZ LARA**

**Rector  
Pontificia Universidad  
Católica de Valparaíso**



**ALAN BRONFMAN  
VARGAS**

**Director Centro de  
Estudios y Asistencia  
Legislativa**

**D**esde el inicio de sus actividades académicas, la Pontificia Universidad Católica de Valparaíso ha desarrollado una ininterrumpida labor académica, de investigación y extensión, orientando su quehacer regional, nacional e internacional, al cultivo del conocimiento y a su difusión.

Avalada por la reciente acreditación máxima de siete años, la comunidad PUCV se proyecta con una visión estratégica transformadora, que permee el quehacer institucional y se haga cargo de temas emergentes.

En esta línea, el segundo número de la Revista de Asuntos Internacionales, Defensa y Seguridad de nuestro Centro de Estudios y Asistencia Legislativa (CEAL) se compromete con este anhelo a través una edición dedicada a la seguridad y sus nuevos desafíos en una sociedad globalizada y altamente tecnologizada.

Los invito a leer la nueva entrega de nuestra revista, que de seguro los hará reflexionar.

**E**l Centro de Estudios y Asistencia Legislativa (CEAL) de la Pontificia Universidad Católica de Valparaíso posee dos líneas de trabajo claramente definidas: la asesoría y los estudios, que se encuentran en interacción e influencia constante, contribuyendo no sólo a la formación de directivos públicos y agentes internacionales, sino, además, posicionando a nuestro centro como un nexo concreto y efectivo entre el mundo universitario y el actuar público y privado.

Nuestra revista de Asuntos Internacionales, Defensa y Seguridad es una extensión de nuestro trabajo y por tanto su contenido, en especial este número dedicado a la seguridad, busca generar información y transferir conocimientos interdisciplinarios en los más amplios aspectos que atañen a esta problemática.

En esta revista podrán revisar artículos sobre ciberdefensa, criminalidad, relaciones internacionales, desinformación y migración. ¡Esperamos que la disfruten!

# Índice



# 09

---

**EDITORIAL**

Por **GIANNI RIVERA FOO**  
Director

# 12

---

**Migración Transnacional:**  
EL CASO DE CHILE Y  
LOS DESAFÍOS DE LA  
SEGURIDAD

Por **GILBERTO ARANDA** y  
**GABRIELLA THOMAZY**

# 28

---

**Seguridad y Desinformación:**  
RETOS  
CONTEMPORÁNEOS Y  
RECOMENDACIONES EN  
UNA ERA DIGITAL

Por **MARÍA JOSÉ ESCOBAR**

# 36

---

LA ARMADA DE  
CHILE EN RIMPAC Y  
SU CONTRIBUCIÓN  
A LAS RELACIONES  
INTERNACIONALES

Por **ALBERTO GUERRERO GARCÍA**

# 44

---

INNOVACIÓN EN  
CIBERDEFENSA

Por **KENNETH PUGH OLAVARRÍA**

# 58

---

LA NUEVA CRIMINALIDAD  
QUE ENFRENTAMOS

Por **EDUARDO CERNA LOZANO**

# 66

---

**Reseña de Libros**  
"LIDERAZGO" DE  
HENRY KISSINGER

Por **CATALINA SCHERPING**

# 71

---

CALENDARIO DE  
ACTIVIDADES





**GIANNI RIVERA FOO**  
Director

# editorial

**E**ste 2024, les damos la bienvenida a la segunda edición de la Revista de Asuntos Internacionales, Defensa y Seguridad (RAIDS) del Centro de Estudios y Asistencia Legislativa (CEAL) de la Pontificia Universidad Católica de Valparaíso.

Tal como lo señalamos en nuestro número inaugural, los conflictos internacionales, y con ellos la problemática de la defensa y la seguridad de las naciones y del mundo globalizado, siguen siendo más que nunca una prioridad.

A la invasión de Ucrania por Rusia, que comenzó el 24 de febrero de 2022, sumamos ahora la guerra entre Israel y Hamás, iniciada el 7 de octubre de 2023 cuando grupos armados de militantes de Hamás y la Yihad Islámica Palestina lanzaron un ataque de cohetes y comandos contra Israel desde la Franja de Gaza.

La contingencia mundial, así como los intereses nacionales y regionales, nos han impulsado a dedicar este número al complejo concepto de la seguridad, entendiéndolo en el más amplio espectro de su definición.

Con un diseño renovado, artículos más compactos y dinámicos hemos invitado a participar a los más diversos especialistas, provenientes tanto de la academia como de los ámbitos gubernamentales y legislativos.

Con un diseño renovado, artículos más compactos y dinámicos

Podríamos decir que la seguridad involucra la capacidad de dar respuesta efectiva a riesgos, amenazas o vulnerabilidades y estar preparados para prevenirlos, contenerlos y enfrentarlos. Nuestra invitación es directa, pero no por ello simple: ¿cuáles son las amenazas que enfrenta Chile?, ¿a cuáles se deben dar prioridad?, ¿cómo se deben equilibrar las medidas de seguridad de los países en concordancia con el respeto a los derechos particulares de sus habitantes? No hay respuestas únicas o definitivas, más bien un continuo debate de ideas y medidas concretas.

Los dejamos invitados a profundizar en el fenómeno de la migración y sus alcances sociales y humanitarios, así como los desafíos que plantea la discusión entre la información y la desinformación en una era digital en la cual la premura de las decisiones que se toman deben ser informadas. La nueva criminalidad presente en Chile y en la región, la ciberdefensa en un mundo interconectado y dependiente de las tecnologías, así como la participación de Chile en los ejercicios navales de intercambio en defensa y seguridad RIMPAC, serán otros de los artículos que, estamos seguros, cautivarán su interés.



# artículos

# Migración Transnacional: EL CASO DE CHILE Y LOS DESAFÍOS DE LA SEGURIDAD

Por GILBERTO ARANDA y GABRIELLA THOMAZY



**Gilberto Aranda**, es Profesor titular del Instituto de Estudios Internacionales de la Universidad de Chile, Doctor en Estudios Latinoamericanos, Profesor visitante en la Universidad Autónoma de Madrid (2022-2023), investigador del Instituto Superior de Investigación en Estudios Latinoamericanos de la Universidad de Alcalá y miembro del claustro del doctorado en Relaciones Internacionales de la Universidad de La Plata. Se especializa en Relaciones Internacionales, Política Internacional y América Latina Contemporánea. Autor de 22 artículos en revistas indexadas de Brasil, Colombia, Chile, España y México, 25 artículos en revistas no indexadas y 12 libros.



**Gabriella Thomazy**, es candidata a Doctora en la Universidad Nacional de Servicio Público de Budapest (Escuela de Doctorado en Ciencias Militares, Estudios de Seguridad). Posee el título de Magíster en Sociología de la Universidad de Miskolc, Hungría, así como un Magíster en Gestión de Recursos Humanos de la misma universidad, Diplomada en Gestión de Bienestar en Organizaciones (Pontificia Universidad Católica, Chile). Posee varios años de experiencia laboral en Chile entre ellos como Directora de Recursos Humanos – América Latina. Actualmente radicada en su país natal, Hungría.

## RESUMEN

En las últimas décadas, la migración se ha transformado en un fenómeno de alcance mundial que si bien es un tema principalmente social y humanitario, ya existe una tendencia que menciona a la migración como un desafío para la seguridad global. Este texto analiza el fenómeno desde el punto de vista internacional y en específico el caso de Chile.

**Palabras clave:** Migración Transnacional – Seguridad – Chile

## ABSTRACT

In recent decades, migration has become a worldwide phenomenon that, although it is mainly a social and humanitarian issue, there is already a trend that mentions migration as a challenge for global security. This text analyzes the phenomenon from an international point of view and specifically the case of Chile.

**Keywords:** Transnational Migration – Security – Chile



FREEPIK

## INTRODUCCIÓN

La migración se ha convertido en un fenómeno mundial en las últimas décadas, despertando el interés de los estudios de seguridad. La migración es cada vez más considerada un tema de seguridad, argumentándose que podría amenazar tanto a la soberanía nacional como a la seguridad humana. (Wohlfeld, 2014; Tálas, 2019). Esta última atañe a la protección de las personas y de las comunidades dentro de los Estados, comprendiendo tanto los derechos humanos, como el desarrollo humano. Esta dimensión apunta a la mejora de los niveles de vida y de las capacidades personales, tiene como principio básico la ausencia de violencia física y la supervivencia (Sen, 2000). Ambos conceptos están interrelacionados: el “estar libre de necesidades” requiere para su realización encontrarse “libre de temores”, como bien ha destacado el giro emocional en las ciencias sociales (Ahmed, 2019). Una vida digna exige percepción de seguridad pública y privada. Lo anterior requiere que los conflictos sociales sean controlados por la autoridad, por lo que se necesita una gestión de crisis (Kaldor, 2010).

socio-ambientales, al verse desposeídos ante Estados ausentes o fragilizados, han decidido cruzar las fronteras asumiendo los riesgos que implica para su supervivencia la búsqueda de otra comunidad política (aunque sea temporalmente), al interior de América Latina, con la esperanza de lograr una buena vida.

La migración regional ha crecido desde la crisis económica de 2008, sumándose al cambio de la política migratoria de los Estados Unidos. Los migrantes provienen, primariamente, de América Latina. Chile, desde hace 20 años es uno de los países preferidos de los migrantes en la región, debido a los indicadores económicos, la institucionalidad, y la seguridad, además de los sueldos más altos en la región, principalmente, en puestos que requieren educación superior (Thomázy, 2020: 412).

Colombia, Ecuador y Perú a partir del año 2015, pasaron de ser países de tránsito a países de destino para los migrantes, principalmente por la masiva salida de los migrantes venezolanos (IOM, 2017), con

**Chile, desde hace 20 años es uno de los países preferidos de los migrantes en la región, debido a los indicadores económicos, la institucionalidad, y la seguridad, además de los sueldos más altos en la región, principalmente, en puestos que requieren educación superior (Thomázy, 2020: 412)**

Adicionalmente, la migración aparece en la agenda de seguridad de muchos países, no solo en Europa sino también en América del Sur. Aunque la migración sigue siendo un tema principalmente social y humanitario en los países sudamericanos, no obstante, ya existe una tendencia que menciona a la migración como un desafío para la seguridad (Flemes et al., 2012; Baeza Freer et al., 2018).

La migración transnacional (Basch, Glick y Szanton, 1994) ha devenido en un tema relevante en el debate público y la agenda política. Los migrantes, por distintas circunstancias económicas, políticas y/o

una direccionalidad hacia países con escasa experiencia histórica de receptividad masiva de migrantes, desviándose de los tradicionales receptores del Norte (Stefoni y Stang, 2017). Desde mediados de la década pasada, la triple crisis política, económica y social venezolana había orientado a ciudadanos(as) de dicho país a dejar su país para radicarse en Estados Unidos, España, Colombia y Chile, a los que se sumó a partir de 2018 Brasil, Perú y Ecuador, ante las restricciones al ingreso en algunos de los primeros Estados receptores (Aranda y Bórquez, 2020). En esa época arrancaron las primeras iniciativas de regularización de nuevos inmigrantes, pero

la magnitud de la migración venezolana ya exigía políticas de regularización que no fueran meros paliativos temporales. También se hicieron ciertos esfuerzos políticos para concretar acciones cooperativas que respondieran a la migración venezolana, respetando los derechos y habilitando el acceso a los mecanismos de regularización. Así, fue suscrita la “Declaración de Quito sobre movilidad humana de ciudadanos venezolanos en la región” del 4 de septiembre de 2018, signada por Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, México, Panamá, Paraguay, Perú y Uruguay. En dicho documento, se expresó la voluntad regional a colaborar para “la provisión de asistencia humanitaria; acceso a mecanismos de permanencia regular, incluyendo la consideración de procesos de regularización migratoria; combate a la trata de personas y al tráfico ilícito de migrantes; lucha contra la violencia sexual y de género; protección infantil; rechazo a la discriminación y la xenofobia; acceso a los procedimientos para la determinación de la condición de refugiado; y, en general, continuar trabajando en la implementación de políticas públicas destinadas a proteger los derechos humanos de todos los migrantes”.

Sin embargo, la dimensión de la crisis humanitaria compleja estaba recién escalando. Hasta el 2022 más de 6 millones de venezolanos habían huido de su país, constituyéndose Colombia en el principal receptor, Perú en segundo lugar, y Ecuador tercero, luego de lo cual aparece Chile en el cuarto puesto como receptor de migración venezolana (Thomázy, 2022: 22).

De hecho, con el Régimen Internacional de Derechos Humanos, de carácter extraterritorial, algunos Estados fueron incorporando lentamente valores y normas internacionales en sus ordenamientos domésticos, generándose una tensión entre derecho internacional y nacional (Álvarez 2012; Hollifield, 2012). En América Latina estas cuestiones fueron abordadas por la Relatoría para los Trabajadores Migratorios en 1966. Hacia 2003, la Corte Interamericana de Derechos Humanos determinó en su Opinión Consultiva N.º 18, que aun cuando un Estado puede hacer diferencias entre personas migrantes en situación regular o irregular, y entre nacionales y extranjeros, siempre y en cualquier caso las polí-

ticas migratorias debían respetar los derechos humanos ya fuera en su objetivos o ejecución (García 2016: 113). A partir de dicha normativa, los Estados comienzan a implementar diversas políticas respecto de los inmigrantes (Bello 2005, 86) con registros que observan la implementación de instrumentos *ad hoc* para regularizar -o limitar- el ingreso y estadía de inmigrantes, tales como los visados adicionales, además de certificados de residencia temporal con vigencia abreviada. La selectividad a discreción se erigió en norma respuesta a la demanda laboral o de experticia.

Después de la tésitura pandémica del Covid-19, Chile, Colombia y Perú comenzaron a debatir entre intensificar su seguridad, mediante enfoques penales favorecidos por una población sensibilizada por las noticias de la masividad migratoria, y el papel de las perspectivas internacionales de derechos humanos patrocinadas por Naciones Unidas y sus agencias especializadas en una migración que comprendería a toda persona en movimiento a través de una frontera internacional (OIM 2018). Es así como desde la agencia internacional para las migraciones (OIM), en cambio, lo definitorio de la condición de migrante no radica en el estatus legal de la persona, o los motivos del desplazamiento, la duración de la estadía o del carácter voluntario o forzado de la misma (OIM 2018). Así no sólo los desastres naturales, conflictos armados, inseguridad ciudadana, violencia delictual o el genocidio pueden gatillar las migraciones, sino que también una decisión voluntaria en virtud de profesión o interés en habitar una sociedad distinta a la de nacimiento.

Lo anterior no es óbice para que la migración forzada sea la más urgente al referirse a quien no tiene otra alternativa que moverse, asilados y refugiados. La condición de asilo incluye a las personas vinculadas a delitos políticos, correspondiendo al Estado receptor la decisión de otorgarse. América Latina presenta una trayectoria consolidada a este respecto como testifican el conjunto de instrumentos jurídicos a su haber: la Convención sobre Asilo de la Habana (1923); el Tratado sobre Asilo y Refugio Político de Montevideo (1939) y la Convención de Caracas sobre Asilo Territorial y Diplomático (1954) (Domínguez 2016; Orduña 2011).

Los refugiados son quienes intentan eludir conflictos armados o temen ante la coacción física por su “raza”, religión, nacionalidad, pertenencia a determinado grupo social u opiniones políticas. Estos son sujetos de protección de derecho internacional, especialmente por medio de la Convención sobre el Estatuto del Refugiado de 1951 y su protocolo de 1967. La principal obligación de los estados que deriva de su reconocimiento es la no devolución (Mathew y Harley, 2016; Oyarzún, 2018). También están quienes dejan su domicilio original con el propósito de mejorar su condición de vida en un país distinto al de nacimiento (OIM 2018). Aunque no siempre se trata de migrante forzado –como los casos anteriores- existe un debate respecto a cómo las condiciones de extrema carestía y adversidad para la sobrevivencia inciden en la decisión de migrar. De la misma manera, el súbito incremento en los niveles de violencia circundantes también puede mover a migrar, facilitando la aparición de “industria de la migración” que implica la participación de adláteres legales (agencias de viajes, compañías navieras y bancos) y colaboradores ilegales (Castles, 2003: 8). Desde luego, lo anterior implica el incremento de las responsabilidades estatales, más allá de los refugiados, lo que a menudo provoca un conjunto de resistencias nacionales al traducirse en la generación de nuevos menesteres sociales abocados a la construcción de un régimen de protección para un tipo más amplio de migrantes (Goodwin-Gill y Newland 2003).

En cualquier caso, ¿Cuándo se convierte la migración internacional en un problema de seguridad? La evidencia apunta a que surge un problema de seguridad si el Estado no puede abordar las consecuencias sociales a largo plazo de la migración (Thomázy, 2021; Tálas, 2019) Lo anterior también cuando la presencia migratoria es de tal magnitud que la recepción y asentamiento de los inmigrantes hace ineficaz la administración temática del Estado (Tálas, 2018).

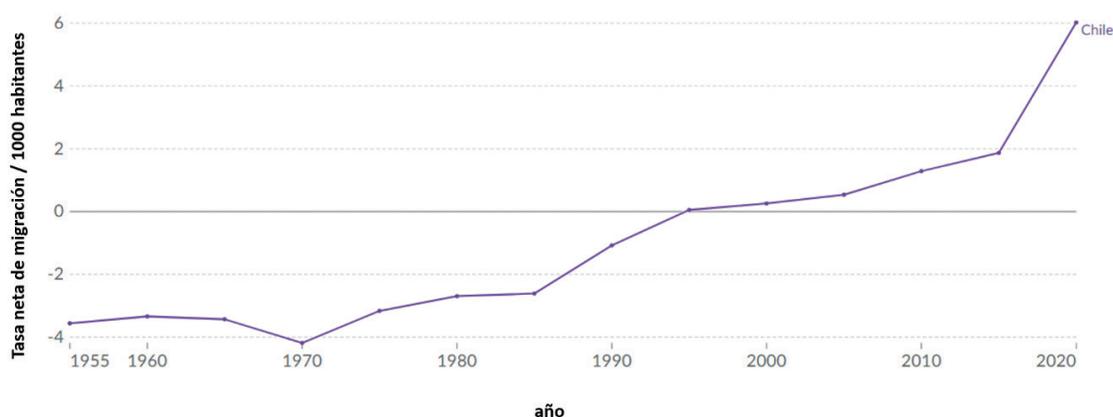
Desde luego dicho enfoque no presupone que la migración sea un problema en sí mismo, sino más bien su modalidad irregular, la cual se asocia comúnmente a riesgos de seguridad, es decir, a delitos como el tráfico ilícito de migrantes y la trata de

personas (Herrera-Lasso et al., 2011). La migración irregular se define como “movimiento de personas que se produce al margen de las leyes, las normas o los acuerdos internacionales que rigen la entrada o la salida del país de origen, de tránsito o de destino” (IOM). A este respecto, la tendencia es a desechar el uso del término de “migración ilegal”, dado que supone la criminalización migrante, siendo la definición de migración irregular o indocumentada, más aceptada.

## CHILE: UN PAÍS DE MIGRANTES

En el siguiente gráfico se aprecia la tasa neta de migración en Chile. El indicador refleja el efecto neto de la inmigración y la emigración por cada 1.000 habitantes durante un año específico (INEC). Se puede ver que Chile en 1955 era un país emisor de migrantes. Las leyes de inmigración chilenas, que entraron en vigor en 1854 (Ley de Colonización) y 1953 (Decreto con Fuerza de Ley 69 de 1953), se crearon para fomentar la colonización y la migración de modalidad selectiva (Norambuena, Navarrete y Matamoros: 2018). En particular, pretendían aumentar la migración italiana, alemana y española (Brower Beltramin, 2022: 556). Después de 1904 –año con 4,0% de migración la más alta del siglo XXI- aparecen un conjunto de disposiciones que restringieron la llegada o presencia de determinados grupos (judíos, gitanos), hasta que en 1975 se aprobó una ley de inmigración (Decreto de Ley N° 1094), bajo el gobierno de Pinochet, que estuvo vigente durante casi 50 años, con numerosas modificaciones. Durante la dictadura militar la seguridad estaba centrada en la defensa de las fronteras y los “enemigos internos”, y la tasa neta de migración fue negativa hasta el siglo XXI.

Como demuestra el gráfico 1, el flujo de migrantes empezó a aumentar desde 2005. Chile se convirtió en uno de los países más estables en la región con una institucionalidad sólida y confiable, y con una economía firme, ejerciendo atractivo para la población de los países vecinos y, desde 2010 para sociedades más lejanas como Haití o Venezuela. El paulatino aumento de extranjeros en el país desde 2005, llegó a más de 1,2 de inmigrantes entre 2014



**GRÁFICO 1.** Tasa neta de migración – Chile.

Fuente: Elaboración propia base de Our World in Data (1955-2020). Net Migration Rate

y 2021, y a los 1,6 millones actuales, más del 8 por ciento de la población total. Los venezolanos por primera vez, en 2018, superaron el mayor grupo de los migrantes (30%) anteriormente liderado por los peruanos, además los haitianos alcanzaron el tercer puesto (13%), entre total de los migrantes radicadas en el país (Thomázy, 2021: 15-16; Our World in Data, 1990-2020; SERMIG, 2021). Lo anterior, aunque el Servicio Nacional de Migraciones en Chile estima un número ligeramente menor de migrantes (2021: 1.482.390) que los datos (1,6 millones) internacionales (Our World in Data, 1990-2020; SERMIG, 2021).

### DESDE EL DECRETO DE LEY N.º 1094 HASTA LA NUEVA LEY DE MIGRACIONES

Con el retorno a la democracia, el presidente Eduardo Frei (1994-2000) realizó modificaciones al derecho de asilo, mientras que el presidente Ricardo Lagos (2000-2006) hizo cambios en la duración de los trámites (Orjuela, 2018: 207). Durante el primer mandato de Michelle Bachelet (2006-2010), se modernizó ligeramente la ley migratoria y se anunció una legalización extraordinaria (Jarufe Bader, 2018: 4; Orjuela, 2018: 208). En la primera presidencia de Sebastián Piñera (2010-2014), ya eran evidentes las

deficiencias del Decreto de Ley N.º 1094. En 2010 se establecieron disposiciones sobre protección de refugiados. En 2011 entró en vigor la primera ley que tipificó los delitos de tráfico ilícito de migrantes y trata de personas, además de establecer normas para su prevención y más efectiva persecución criminal (Ley 20.430, 2010; Ley 20.507, 2011). Pero en general la inercia había nutrido la tendencia restrictiva en la política migratoria de los gobiernos democráticos (Norambuena, Navarrete y Matamoros: 2018, 224)

En junio de 2013, diez meses antes del final de su mandato, Piñera presentó un nuevo proyecto de ley migratoria que proponía cambios radicales a la ley de 1975, abarcando todo el proceso de migración, incluyendo derechos y obligaciones de los migrantes. El proyecto de ley no fue aprobado debido a las elecciones presidenciales, y la iniciativa se estancó durante la segunda presidencia de Bachelet, ya que no reflejaba la posición del nuevo gobierno sobre el tema (Orjuela, 2018: 21).

Durante el segundo gobierno de Michelle Bachelet (2014-2018), en marzo de 2015, se introdujo la nueva visa temporal (visa por motivos laborales) que reemplazó la visa sujeta a contrato. El nuevo permiso permitía un empleo flexible, la posibilidad de trabajar con varios empleadores simultáneamente,

eliminaba la cláusula de viaje y ofrecía la opción de solicitar el permiso de residencia p después de 1 año (OIM, 2017: 24). Aunque el permiso se volvió extremadamente popular, no previó ciertas prácticas, como, por ejemplo, contratos falsos (Orellana, 2018; Thomázy 2021b).

“El nuevo gobierno de Sebastián Piñera (2018-2022) buscaba regularizar la situación de los migrantes, así que el Mandatario despachó un proyecto de ley de migración, y firmó un decreto con el que eliminó la visa de motivos laborales”, creadas por Michelle Bachelet en 2015, que hizo más fácil que los turistas se quedaran en Chile, además, entró en vigor la visa de turismo a los haitianos e implementó una nueva visa de responsabilidad democrática para los venezolanos. Conjuntamente, el 18 de octubre de 2018, fue implementada el plan de retorno humanitario para ayudar, principalmente, a los haitianos que quieran regresar a su país voluntariamente.” (Thomázy, 2021: 19).

Paralelamente a la presentación del nuevo proyecto de ley, Piñera anunció la regularización extraordinaria de los migrantes. La extranjería estimaba que el número de personas en situación irregular era de aproximadamente 300 mil (Thayer Correa, 2021: 12). Cabe destacar que durante el primer proceso regulatorio que se llevó a cabo el 8 de abril de 2018, junto a las solicitudes de regularización a través del procedimiento tradicional en la misma fecha, se regularizaron más de 210 mil extranjeros que habían ingresado de forma irregular al territorio nacional o que no tenían permiso de trabajo. Esto permitió cambiar su situación migratoria y obtener su documentación para vivir y trabajar en el país. (Extranjería, 2021).

Después de un prolongado debate, la nueva ley migratoria fue finalmente aprobada por el Congreso el 3 de diciembre de 2020 y entró en vigor en 2022. Paralelamente se establecieron nuevas subcategorías migratorias (Ley 21.325, 2021, Decreto 296, 2022, Decreto 23, 2022). Significativo de la nueva ley fue la prohibición de modificar la categoría migratoria en Chile es decir que exigió a la solicitud presentarse en el país de origen (Thomázy, 2021: 22).

## LA MIGRACIÓN IRREGULAR Y LOS DESAFÍOS DE LA SEGURIDAD

La polémica ley de migrantes y las medidas especiales fueron objeto de críticas por parte de organizaciones locales y la oposición. Sin embargo, detrás de eso se encontraba un sistema colapsado desde hacía décadas, ya incapaz de regularizar la llegada de migrantes. Los procesos para obtener permisos eran excesivamente largos, lo que llevaba a que los migrantes vivieran en Chile sin documentos ni permisos de trabajo, incrementando así el número de inmigrantes irregulares en el país y/o de empleos informales (Thomázy, 2021: 24).

Como mencionamos anteriormente, si el Estado no puede abordar las consecuencias sociales de la migración debido a la cantidad de migrantes, esta se convierte en un problema de seguridad, y el Estado debería implementar medidas especiales. Además, también se evidencia un problema de seguridad cuando la magnitud del número de personas es tan elevada que el Estado no puede gestionar la llegada de los migrantes.

A modo de ejemplo, según los datos del Censo 2017 la migración ha alcanzado una magnitud tan significativa en ciertas comunas de Santiago que los accesos a recursos básicos (supermercados, viviendas, educación, salud, etc.) podrían resultar insuficientes para la población. Comunidades como Lampa (26,9 %), San Miguel (26,4 %), Providencia (24,5 %), Pirque (24,3 %) y Vitacura (21,3 %) registran la mayor proporción de migrantes representando aproximadamente un cuarto de su población residente habitual (Censo, 2017, Thomázy, 2021: 24).

Se ha registrado un incremento en el número de niños migrantes, generando desafíos en diversas comunas o ciudades. Un ejemplo de ello es el caso de Mejillones, donde en el año 2023 se evidenciaron 600 sobrecupos de alumnos sin subvención.

El Departamento de Extranjería publicó anteriormente los plazos de espera para la obtención de permisos de residencia, que en el período 2010-2015 demoraban entre 6,35 y 24,25 meses, y esta

duración aumentaba progresivamente (Thomázy, 2020: 413). La mayoría de estos individuos ingresan al sector informal del mercado laboral mientras aguardan la obtención de la visa.

## COVID-19: LA MIGRACIÓN IRREGULAR-PROTESTAS CONTRA LOS MIGRANTES

La pandemia de Covid-19 y el cierre de fronteras han tenido un impacto significativo en los flujos migratorios en Chile. A raíz de los cierres fronterizos y las restricciones de viaje, muchos migrantes no pudieron regresar a sus países de origen. Aunque los flujos migratorios disminuyeron, no se detuvieron por completo. Además, se observó un aumento en los ingresos por pasos fronterizos no habilitados, poniendo en riesgo la vida de los migrantes, especialmente los más vulnerables.

La migración irregular empeoró desde el inicio de la pandemia de Covid-19. A partir de 2020 se apreció un incremento de la inmigración por pasos no habilitados desde Chacalluta y Colchane, en la frontera norte con Perú y Bolivia, llegando a las ciudades de Arica e Iquique, implicando un desafío para las políticas públicas y su institucionalidad (Liberona, 2015). Se refrenda el periplo, a menudo peatonal, de venezolanos/as siguiendo dos rutas: la Andina y la Amazónica, a través de Colombia, Ecuador, Perú y Brasil. Las políticas y programas para enfrentarlos tienen una doble naturaleza, de política doméstica, dado su impacto en el territorio nacional, y de política exterior, dados los efectos que genera en su relación con otros países (Oyarzún, Aranda y Gissi, 2021).

Es clave destacar que los flujos migratorios están en constante movimiento, a veces cruzando varios países. De esta manera, los migrantes indocumentados ingresan y salen por pasos fronterizos no habilitados. Como resultado de la crisis migratoria venezolana, han surgido redes de tráfico de migrantes y megabandas criminales (Tren de Aragua), principalmente en el norte de Chile. Asimismo, se ha incrementado el trabajo ilegal entre la población migrante.

El 25 de septiembre de 2021, en la ciudad de Iquique, alrededor de 5.000 personas atacaron a un grupo de migrantes e incendiaron su campamento temporal (BBC News, 2021). El 2 de octubre de 2021, también se llevaron a cabo protestas contra la "invasión de migrantes" en Santiago y Antofagasta (El Mostrador, 2021). No se trata de un fenómeno aislado; los expertos han observado incidentes similares en países vecinos, pero las protestas antimigración en Chile han recibido publicidad internacional.

En enero de 2022, las protestas fueron más fuertes, vinculando la migración con la delincuencia. Apareció el lema "fuera los delincuentes" y se atacó a un campamento de personas venezolanas. Estas protestas estuvieron principalmente dirigidas "contra la creciente inseguridad en Iquique, al norte de Chile, donde llegan masivamente migrantes irregulares" (DW, 2022).

Comenzó a extenderse una mirada doméstica de una frontera nacional fragilizada, cuando no porosa que permite la llegada descontrolada de migrantes que terminan ocupando espacios públicos en el territorio nacional, generando percepción de alarma, cuando no brotes de xenofobia. La encuesta Plaza Pública de CADEM mide la percepción de la población chilena sobre la migración desde 2016, pero no se ha realizado ninguna encuesta para 2022. La publicación 2023 resume la percepción de la migración para el período 2016-2023. Muestra que, en 2016, el 45% consideraba desfavorable la presencia de migrantes a la llegada de haitianos, y que la tendencia mejoró levemente después de las medidas por el gobierno de Piñera en 2018. Sin embargo, la encuesta alcanzó su nivel más desfavorable en abril de 2023, donde el 77% de los encuestados cree que la migración no es buena para el país. Además, la encuesta de CADEM reveló, un 86% está de acuerdo que deben ponerse más restricciones a la migración con que las actuales, y 87% piensa que los inmigrantes sin papeles al día sean detenidos (CADEM, 2023, 484: 16).

Las protestas y la deteriorada percepción de la migración en Chile evidencian que las respuestas proporcionadas por el gobierno no fueron satisfacto-

rias para la población. Desde 2005, se ha observado un aumento en los flujos migratorios, y la llegada de migrantes experimentó un crecimiento significativo entre 2015 y 2020. A pesar de los intentos de cada gobierno por modificar la ley de migración o presentar propuestas para una nueva legislación, y las iniciativas de regularización extraordinaria de los migrantes no lograron resolver de manera efectiva el asentamiento y la integración de los extranjeros.

Desde la perspectiva de La Escuela de Copenhague, la securitización: “se trata de un proceso por el cual una cuestión se presenta como una amenaza existencial mediante discursos” (Buzan et al. 1998) como, por ejemplo, el aumento de los migrantes.

“Un tipo de política que va más allá de la política, que genera un espectro en el cual se puede mover la problemática de la seguridad. Esto, desde lo que se puede denominar como lo “no politizado”, instancia en la que el Estado no se hace cargo de la problemática particular; lo “politizado”, en el que el tema forma parte de la agenda pública; y lo “securitizado”, circunstancia en la que el problema se presenta como una amenaza existencial, que requiere medidas de emergencia y justifica acciones fuera de los límites normales de los procedimientos políticos y/o garantías democráticas preestablecidas” (Buzan, Waever, & De Wilde, 1998: 23-24).

Esta perspectiva implica la salida del campo político habitual, bajo el supuesto que determinadas cuestiones públicas constituirían una amenaza, que desborda la política regular y democrática, por lo que requiere un tratamiento excepcional a menudo fuera del ámbito de los procedimientos y/o garantías jurídicas (Buzan, Waever, & De Wilde, 1998: 23). Presupone la existencia de seguridad societal, asociada a una cultura colectiva comunitaria, por lo que inseguridad es definida a partir de la identificación de un riesgo de carácter extrínseco (Buzan, Waever, & De Wilde, 1998: 119). Una inmigración masiva sin regulación constituiría una potencial amenaza social (Buzan, Waever, & De Wilde, 1998: 121).

Así la inmigración se constituye en precursor de la securitización fronteriza, facilitando la gestión de la “amenaza migratoria al dotar de sentido un con-

junto de significados y prácticas burocráticas (Bigo, 2002: 74).

El caso de Chile demuestra que la migración como tema de seguridad recientemente apareció en los discursos políticos, así los gobiernos no securitaron la migración en tiempo ¿Por qué es importante que el Estado securitiza la migración? “Si el Estado securitiza la migración, le otorga el derecho de tomar cualquier medida necesaria para contrarrestarla y, por lo tanto, motiva a otros Estados a tomar medidas, pero a la falta de la securitización, puede incluso a afectar negativamente su propia seguridad y la de otros Estados (Thomázy, 2021: 12).

## FOMENTAR LA MIGRACIÓN LEGAL Y LA INTEGRACIÓN

En diversos países europeos, las respuestas en torno al tema de seguridad relacionado con los migrantes son más rápidas. Ejemplo reciente de ello es el ataque terrorista perpetrado por un tunecino en octubre de 2023: “en cuestión de días se ha convertido en el nuevo rostro de la campaña de la Unión Europea para endurecer los controles fronterizos, deportar rápidamente a los migrantes y permitir que la policía y las agencias de seguridad intercambien información de manera más eficiente (Cook, 2023).

Mientras en varios países de la Unión Europea se promueve un discurso a favor del aumento de la migración legal, esto se debe al ineficiente sistema de pensiones de reparto y a sociedades que están experimentando un proceso de envejecimiento. Al fomentar la migración podría abordar la carencia de trabajadores, especialmente en las áreas de técnicos y mano de obra.

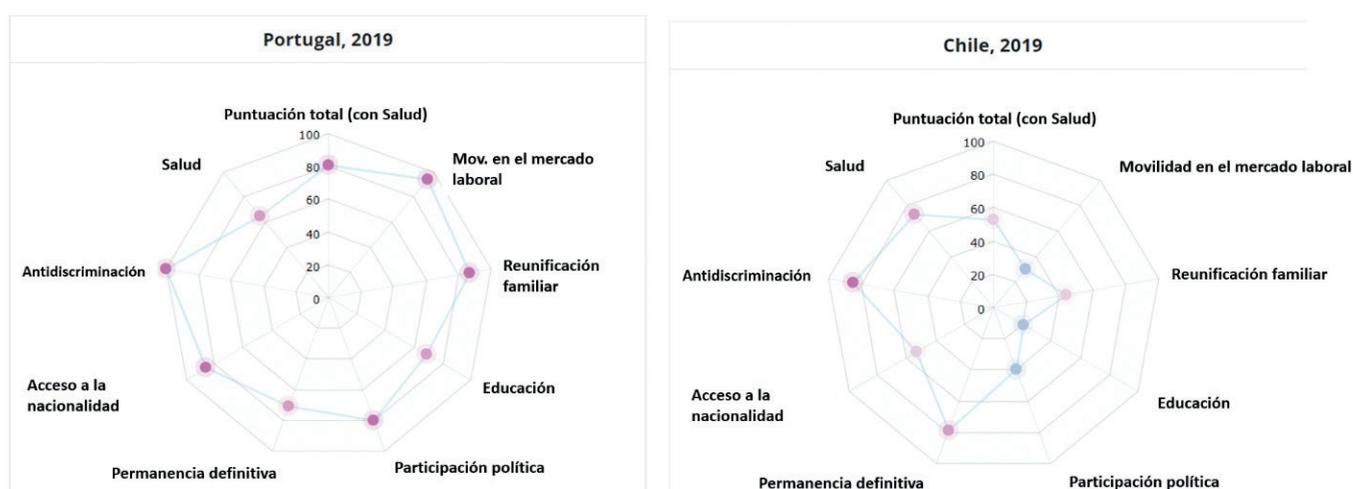
A modo de ejemplo, en España se publicó en mayo de 2021 un concepto estratégico para “España 2050”. En el texto, se menciona lo siguiente: “esta Estrategia asume que nuestro país seguirá acogiendo e integrando a cientos de miles de personas inmigrantes. En concreto, se proyecta un saldo migratorio de unas 191.000 personas al año de aquí a 2050” (España 2050, 2021: 221).

En caso de que la integración y las visas proporcionadas no sean adecuadas la legalidad de los migrantes se ve limitada, lo que dificulta la búsqueda de empleo y la permanencia en el país de acogida (Thomázy, 2022: 21).

El Índice de Política de Integración de los Inmigrantes (MIPEX-Migrant Integration Policy Index) se fundamenta en el concepto de integración adoptado por la Unión Europea, evaluando las iniciativas políticas que apoyan la integración de los inmigrantes. La encuesta de MIPEX, basada en la evaluación de expertos, contiene 167 preguntas que abarcan ocho ámbitos legislativos. El indicador resultante facilita comparaciones multidimensionales y clasifica a los países en una escala de 0 a 100 (0 = menos favorable, 100 = más favorable). Los ocho ámbitos principales abordados son: 1. Movilidad en el mercado laboral, 2. Educación, 3. Participación política, 4. Acceso a la nacionalidad, 5. Reunificación familiar, 6. Salud, 7. Permanencia definitiva, 8. Medidas contra la discriminación (MIPEX, 2019; Tarko et al., 2021: 320).

A modo de ejemplo, el índice MIPEX de Portugal se sitúa entre los más elevados de la Unión Europea (Total: 81 puntos). La movilidad en el mercado laboral para los extranjeros alcanza los 91 puntos de 100, lo que permite a los inmigrantes acceder fácilmente al mercado laboral al llegar al país. Además, las políticas públicas se extienden al acceso a la nacionalidad y a la reunificación familiar, contribuyendo así al fortalecimiento de la integración en el país (Gráfico 2).

Mientras que en Chile el puntaje total es considerablemente menor que en caso de Portugal (total: 53 puntos). Las políticas públicas dificultan la movilidad en el mercado laboral según el índice MIPEX (total: 30 puntos). El mercado laboral chileno se caracteriza por su segmentación, lo que dificulta la integración de los migrantes con educación terciaria (Thomázy, 2020 ej. caso de médicos extranjeros) y propicia la informalidad y el trabajo irregular de la mano de obra.



Escala de 0 a 100 (0 = menos favorable, 100 = más favorable)

**GRÁFICO 2.** El Índice de Políticas de Integración de los Inmigrantes (MIPEX) Chile, Portugal.  
Fuente: Elaboración propia base de Mipex (2019).

## CONCLUSIÓN

Este estudio revela la importancia de que los países deben establecer en tiempo las medidas extraordinarias para prevenir o reducir la migración irregular y/o los trabajos ilegales por los migrantes. De lo contrario, es probable que la migración irregular aumente y sus consecuencias variadas y complejas. Asimismo, a través de estas medidas, los gobiernos podrían disminuir la xenofobia, así como las protestas contra los migrantes lo que está aumentando en los países involucrados de la migración venezolana en la región. Es importante señalar que la imposición de barreras administrativas por parte de los países receptores, con el fin de restringir el ingreso de migrantes, puede contribuir al aumento de los ingresos por pasos no habilitados. Por lo tanto, es indispensable fomentar la migración legal y establecer políticas efectivas de integración.

Contrariamente, en ausencia de una posición sólida por parte del gobierno respecto a la migración, el descontento social fortalece a partidos populistas, particularmente de la derecha radical. A modo de ejemplo, se puede mencionar el caso de Países Bajos, el partido por la Libertad (PVV) de ultraderecha, obtuvo la victoria en las elecciones de noviembre de 2023. El líder de PVV, Geert Wilders propone: “el restablecimiento del control en las fronteras neerlandesas, la detención y expulsión de migrantes ilegales, el retorno de solicitantes de asilo sirios y la reintroducción de permisos de trabajo para trabajadores dentro de la UE” (France24, 2023).

## BIBLIOGRAFÍA

- Ahmed, Sara (2019). *La promesa de la felicidad*. Buenos Aires: Caja Negra.
- Álvarez, Silvina (2012). La interpretación contextualizada de los derechos humanos: multiculturalismo, cosmopolitismo y pluralismo de valores. *Isonomía*, 36. 49–82.
- Aranda, Gilberto – Bórquez, Alberto (2020). La cuestión venezolana y la fractura del regionalismo latinoamericano. *Historia* 396 /1. 33–72
- Baeza Freer, Jaime – Wehner, Leslie E. (2018). Los desafíos de seguridad para Chile: definiciones para escenarios múltiples. In: *Revista de Estudios en Seguridad Internacional*, 4/1. 19–35. DOI: <https://doi.org/10.18847/1.7.2>
- Basch, L. – Glick Schiller, N. – Szanton Blanc, C. (1993). *Nations Unbound: Transnational Projects, Postcolonial Predicaments, and Deterritorialized Nation-States*, Langhorne, Gordon and Breach Publishers.
- Bello, Martha Nubia (2005). *Migraciones, Redes Sociales y Ciudadanía*. En *América Latina, otras visiones desde la cultura*. Editores Jesús Martín Barbero et al. Bogotá: Convenio Andrés Bello.
- Bigo, D. (2002). Security and Immigration: Toward a Critique of the Governmentality of Unease. *Alternatives: Global, Local, Political* N°27. 63–92.
- Buzan, Barry – Waeber, Ole – Wilde, Jaap de (1998). *Security: A new Framework for analysis*. Linne Rienner, London
- Castles, Stephen. (2003). La política internacional de la migración forzada. *Migración y Desarrollo*, 1. 74-99. Recuperado de <http://www.migracionydesarrollo.org/>
- Chile: la marcha contra migrantes que terminó con la quema de pertenencias y carpas de extranjeros (2021). BBC News, 26.09.2021. <https://www.bbc.com/mundo/noticias-america-latina-58700359> [08.11.2021].
- Chile: protestan contra migrantes irregulares en Iquique. DW, 31.01.2022 <https://www.dw.com/es/chile-protestan-contra-migrantes-irregulares-en-iquique/a-60605627> [08-15-2022].
- Cook, Lorne (2023). Ataque en Bélgica impulsa a UE a endurecer leyes fronterizas y de deportación. AP-News, 19.10.2023. <https://apnews.com/world-news/general-news-79703f54214937a5cc9060a7e9fed4a1> [30.10.2023].
- Domínguez, Claudia (2016). Derecho chileno migratorio a la luz del derecho migratorio internacional: ¿Ceden los derechos humanos mínimos de los extranjeros ante las prerrogativas soberanas de control migratorio? *Revista Chilena de Derecho*, 43/1. 189–217.
- Gana la extrema derecha en Países Bajos; Geert Wilders enfrenta el desafío de formar una coalición. France24, 23.11.2023. <https://www.france24.com/es/europa/20231123-gana-la-extrema-derecha-en-pa%C3%ADses-bajos-geert-wilders-enfrenta-el-desaf%C3%ADo-de-formar-una-coalici%C3%B3n> [24.11.2023].
- García, Lila (2016). Migraciones, Estado y una política del derecho humano a migrar: ¿hacia una nueva era en América Latina? *Colombia Internacional* 88. 107–133. doi: <http://dx.doi.org/10.7440/colombiaint88.2016.05>
- Goodwin-Gill, Guy – Newland, Kathleen (2003). *Forced Migration and International Law*, En Aleinikoff, Alexander and Chetail, Vincent (eds.), *Migration and International Legal Norms*, Migration Policy Institute. La Haya: TMC Asser. 123-136.
- Herrera-Lasso, Luis – Artola, Juan B. (2011). Migración y seguridad: dilemas e interrogantes. In: Armijo Canto, Natalia (eds): *Migración y Seguridad: nuevo desafío en México*, Casede, México, 2011.
- Hollifield, James (2012). *Migration and International Relations*. En *The Oxford Handbook of the Politics of International Migration*. Rosenblum, Marc & Tichenor, Daniel. Oxford: Oxford University Press.
- IOM-South American Migration Report No. 2. (2017). Asequible en: <https://displacement.iom.int/reports/south-america-%E2%80%94-regional-migration-report-2-%E2%80%94-recent-migration-trends-south-america-2017> [08.02. 2022].
- Flemes, Daniel – Radseck, Michael (2012). Gobernanza multinivel de seguridad en América del Sur. *Papel Político*. 17/1. 203–238.
- Jarufe Bader, Juan Pablo (2018). *Historia de la legislación migratoria nacional*. [https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/25549/1/Historia\\_de\\_la\\_legislacion\\_migratoria\\_nacional.pdf](https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/25549/1/Historia_de_la_legislacion_migratoria_nacional.pdf) [10.11.2023].

- Elias, Manuel (2018). La ONU confirma su respaldo al Pacto Mundial de Migración en la Asamblea General. 19-12-2018. <https://news.un.org/es/story/2018/12/1448301>, [06.01.2021].
- España 2050. Fundamentos y propuestas para una Estrategia Nacional de Largo Plazo. 2021. [https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/200521-Estrategia\\_Espana\\_2050.pdf](https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/200521-Estrategia_Espana_2050.pdf) [27.05.2021].
- Kaldor, Mary (2010). El poder y la fuerza. La seguridad de la población civil en un mundo global. Barcelona: Tusquets.
- Liencura, Jaime (2018). Migración: la frontera que divide a los gobiernos de Bachelet con el de Piñera, 12-11-2018. Publimetro, <https://www.publimetro.cl/cl/noticias/2018/12/11/bachelet-versus-pinera-migracion.html>, [23.10.2020].
- Norambuena, Carmen; Bernardo Navarrete y Rodrigo Matamoros (2018). "Entre continuidades y rupturas, mejor la continuidad. Política migratoria chilena desde comienzo de siglo XX". Revista Austral de Ciencias Sociales 34 : 217-237
- Marchas por crisis migrante se realizaron en Iquique, Antofagasta y Santiago (2021). El Mostrador, 02.10.2021. <https://www.elmostrador.cl/noticias/multimedia/2021/10/02/manifestaciones-por-crisis-migrante-se-realizaron-en-iquique-antofagasta-y-santiago/> [07.11.2021].
- Mathew, Penelope – Harley, Tristan (2016). Refugees, Regionalism and Responsibility. Cheltenham, UK: Edward Elgar Publishing
- Orduña, Leticia (2011). La migración en el Derecho Internacional. Revista de la Facultad de Derecho de México, 61/255. 329-352.
- Orjuela, Fernando Neira (2018). La normatividad migratoria chilena entre el debate político y la realidad social. O Social em Questão. 21/41. 199–224. Pontifícia Universidade Católica do Rio de Janeiro Brasil.
- Oyarzún, Lorena (2018). Movement of People in the Pacific Alliance: The Chilean Case. In: César, Álvarez and Hernández, José (eds.) Latin America Geopolitics: Migrations, Cites and Globalización. New York, Palgrave Mc Millan, 68.
- Oyarzún Serrano, L. – Aranda, G. – Gissi, N. (2021). Migración internacional y política migratoria en Chile: tensiones entre la soberanía estatal y las ciudadanía emergentes. Colombia Internacional, 84–114. <https://revistas.uniandes.edu.co/doi/pdf/10.7440/colombiaint106.2021.04>
- Sen, Amartya (2000). Why Human Security? International Symposium on Human Security.
- Stefoni, C. – Stang, F. (2017). La construcción del campo de estudio de las migraciones en Chile: notas de un ejercicio reflexivo y autocrítico. Íconos Revista de Ciencias Sociales, 58, 109–129. DOI: <https://doi.org/10.17141/iconos.58.2017.2477>
- Tálas, Péter (2019). A migráció, mint biztonságpolitikai probléma. Magyar Tudomány, 2019, 180/1. 67–78. DOI: <https://doi.org/10.1556/2065.180.2019.1.6>
- Tálas, Péter (2018). Az európai migrációs válság értelmezési kereteiről. Dialog Campus, Budapest
- Tatarko, Alexander – Jurcik, Toma – Hadjar, Andreas (2021). How Migration Policy Shapes the Subjective Well-Being of the Non-Immigrant Population in European Countries. Journal of Cross-Cultural Psychology 52/3. 316–333. DOI: <https://doi.org/10.1177/00220221211001531>.
- Tijoux, María E. – Ambiado, Constanza (2019). Informe-racismos y migración contemporánea en Chile. Racismos y Migraciones. Contemporáneas de la Vicerrectoría de Extensión y Comunicaciones de la Universidad de Chile, 31-10-2019. [https://tbinternet.ohchr.org/Treaties/CERD/Shared%20Documents/CHL/INT\\_CERD\\_NGO\\_CHL\\_38614\\_S.pdf](https://tbinternet.ohchr.org/Treaties/CERD/Shared%20Documents/CHL/INT_CERD_NGO_CHL_38614_S.pdf), [24.10.2020].
- Thayer Correa, Luis Eduardo (2021). Puertas cerradas y huellas abiertas: migración irregular, trayectorias precarias y políticas restrictivas en Chile. Migraciones internacionales 12. DOI: <https://doi.org/10.33679/rmi.v1i1.2270>.
- Thomázy, Gabriella (2020). Tendencias actuales y nuevos desafíos de los migrantes en Chile. Acta Hispanica–Acta Universitatis Szegediensis de Attila József Nominatae 2. 409–421. DOI: <https://doi.org/10.14232/actahisp.2020.0.409-421>
- Thomázy, Gabriella (2022). Regularización extraordinaria de los migrantes durante el Covid-19: América del Sur y Europa del Sur – un análisis comparativo. Acta Hispanica–Acta Universitatis Szegediensis de Attila József Nominatae, (IV), 19–31. DOI: <https://doi.org/10.14232/actahisp.2022.0.19-31>
- Thomázy, Gabriella (2021). Aspectos de seguridad de la migración haitiana y venezolana en Chile. Iberoamericana Quinquecclesiensis. 19. 9–31. <http://real.mtak.hu/133880/>

Wohlfeld, Monica (2014). Is Migration a Security Issue? In: GRECH, Omar. – WOHLFELD, Monica (eds.): Migration in the Mediterranean: Human Rights, Security and Development Perspectives. Malta: MEDAC, 61–77.

## BASE DE DATOS / DEFINICIONES

CADEM (2023, 484). Encuesta Plaza Pública. Estudio: 484, abril. <https://cadem.cl/wp-content/uploads/2023/04/Track-PP-484-Abril-S3-VF.pdf> [10.08.2023].

Censo (2017). Migración Interna en la Región Metropolitana. Instituto Nacional de Estadísticas noviembre de 2020. [https://www.ine.cl/docs/default-source/demografia-y-migracion/publicaciones-y-anuarios/migraci%C3%B3n-interna/censo-2017/migraci%C3%B3n-interna-en-la-regi%C3%B3n-metropolitana-censo-de-2017.pdf?sfvrsn=e76d4567\\_4/](https://www.ine.cl/docs/default-source/demografia-y-migracion/publicaciones-y-anuarios/migraci%C3%B3n-interna/censo-2017/migraci%C3%B3n-interna-en-la-regi%C3%B3n-metropolitana-censo-de-2017.pdf?sfvrsn=e76d4567_4/) [10.08.2022].

Extranjería (2021). Gobierno inicia segundo proceso de regularización migratoria 100% en línea. Noticias-Extranjería, 21.04.2021. <https://www.extranjeria.gob.cl/noticias/gobierno-inicia-segundo-proceso-de-regularizacion-migratoria-100-en-linea> [06.08.2021].

IOM Migración irregular. <https://www.iom.int/es/terminos-fundamentales-sobre-migracion> [10.11.2023].

INE y DEM (2021). Estimación de personas extranjeras residentes habituales en Chile al 31 de diciembre de 2019. Informe técnico: desagregación regional y comunal. Santiago.

MIPEX–Migrant Integration Policy Index [https://knowledge4policy.ec.europa.eu/dataset/ds00052\\_en](https://knowledge4policy.ec.europa.eu/dataset/ds00052_en) [21.11.2023].

Our World in Data (1990-2020). Chile: Total number of international immigrants <https://ourworldindata.org/explorers/migration?tab=chart&facet=none&country=~CHL&hideControls=false&Metric=Net+migration+rate&Period=Total&Sub-metric=Per+capita+%2F+Share+of+population> [21.11.2023].

Our World in Data (1955-2020). Net migration rate. <https://ourworldindata.org/explorers/migration?tab=chart&facet=none&country=~CHL&hideControls=false&Metric=Number+of+international+immigrants&Period=Total&Sub-metric=Total> [21.11.2023].

INEC–Tasa neta de migración. [https://www.inec.gob.pa/redpan/sid/glosario/WebHelp/Tasa\\_neta\\_de\\_migracion\\_1.htm#:~:text=La%20tasa%20neta%20de%20migraci%C3%B3n,%C3%A1rea%20durante%20un%20a%C3%B1o%20determinado](https://www.inec.gob.pa/redpan/sid/glosario/WebHelp/Tasa_neta_de_migracion_1.htm#:~:text=La%20tasa%20neta%20de%20migraci%C3%B3n,%C3%A1rea%20durante%20un%20a%C3%B1o%20determinado) [20.11.2023].

SERMIG (2021). Servicio Nacional de Migraciones. <https://serviciomigraciones.cl/estudios-migratorios/estimaciones-de-extranjeros/> [18.11.2023].

## LEYES E INSTRUMENTOS JURÍDICOS

Decreto Ley 1094. (1975). Establece normas sobre extranjeros en Chile Ministerio del Interior. <https://www.bcn.cl/leychile/navegar?idNorma=6483> [20.11.2023].

Ley 20.507 (2011). Ley N° 20.507 que tipifica los delitos de tráfico ilícito de migrantes y trata de personas. <https://www.bcn.cl/leychile/navegar?idNorma=1024319> [18.11.2023].

Ley 20.430 (2010). Ley N° 20.430 que establece disposiciones sobre protección de refugiados <https://www.bcn.cl/leychile/navegar?idNorma=1012435> [18.11.2023].

Decreto 296 (2022). Aprueba reglamento de la ley N° 21.325, de migración y extranjería. <https://www.bcn.cl/leychile/navegar?idNorma=1172573> [18.11.2023].

Decreto 23. (2022). Establece las subcategorías migratorias de permanencia transitoria. Ministerio del Interior y Seguridad Pública; Subsecretaría del Interior. <https://www.bcn.cl/leychile/navegar?idNorma=1173324> [18.11.2023].

Ley 21.325 (2021). Ley de migración y extranjería Ministerio del Interior y Seguridad Pública. <https://www.bcn.cl/leychile/navegar?idNorma=1158549> [18.11.2023].

Ministerio de Relaciones Exteriores y Movilidad Humana del Ecuador, Declaración de Quito sobre movilidad humana de ciudadanos venezolanos en la región. Quito. 4 de septiembre de 2018. <https://www.cancilleria.gob.ec/declaracion-de-quito-sobre-movilidad-humana-de-ciudadanos-venezolanos-en-la-region/> [27.05.2021].



# Seguridad y Desinformación: RETOS CONTEMPORÁNEOS Y RECOMENDACIONES EN UNA ERA DIGITAL

Por MARÍA JOSÉ ESCOBAR



**María José Escobar**, Ingeniera Civil Electrónica y Magíster en Ingeniería Electrónica de la Universidad Técnica Federico Santa María (UTFSM), Valparaíso, Chile. Doctora en Procesamiento de Imágenes y Señales en la Université Nice-Sophia Antipolis, Francia. Entre diciembre del 2019 y marzo 2022 se desempeñó como la primera Secretaria Regional Ministerial de Ciencia, Tecnología, Conocimiento e Innovación, Macrozona Centro. Desde el 2011 se desempeña como Académica del Departamento de Electrónica de la UTFSM. Desde el 2014 participa como investigadora del Centro Avanzado de Ingeniería Eléctrica y Electrónica AC3E. Durante el 2022 se incorpora al Centro Nacional de Inteligencia Artificial (CENIA) como investigadora colaboradora. Actualmente, se desempeña como Directora General de Vinculación con el Medio de la UTFSM. Además, participa como directora suplente de la fundación Data Observatory y como presidenta del del Ecosistema de Emprendimiento e Innovación de la Región de Valparaíso, EIVA. Es integrante de la Comisión Asesora contra la Desinformación del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación de Chile.

## RESUMEN

En el panorama actual de la información digital, la desinformación se ha convertido en una amenaza creciente para la seguridad global. El artículo habla sobre el fenómeno de la desinformación, que ha adquirido nuevas dimensiones en la era digital, afectando la toma de decisiones informadas. A pesar de los esfuerzos internacionales, no hay una definición única del fenómeno. La desinformación se manifiesta en diversas áreas como la salud, medio ambiente y seguridad nacional. Respecto a esta última, se ha intensificado debido a estrategias sofisticadas, incluyendo ciber tropas y deepfakes.

**Palabras claves:** Desinformación – Seguridad Global – Era Digital

## ABSTRACT

In the current landscape of digital information, des and misinformation has become a growing threat to global security. The article discusses the phenomenon of des/misinformation, which has taken on new dimensions in the digital age, impacting informed decision-making. Despite international efforts, there is no singular definition of the phenomenon. Des/misinformation manifests in various areas such as health, the environment, and national security. Concerning the latter, it has intensified due to sophisticated strategies, including cyber troops and deepfakes.

**Keywords:** Misinformation – Global Security – Digital Age

09.03.2020 - 15.03.2020  
Week 11

SCI  DAY

Nº157

# FAKENEWS

INNOVATION & TECHNOLOGY

Pellentesque diam volutpat  
com modo sed egestas egestas  
fringil la phasellus faucibus. Sit  
amet facilisis magna etiam

RADIATION & ECOLOGY

**Strontium-90.**

AGRICULTURAL INDUSTRY

**Fertilizers and**

## INTRODUCCIÓN

**E**l fenómeno de la desinformación es tan antiguo como la humanidad, pero ha alcanzado nuevas dimensiones en la era digital, trascendiendo fronteras y desafiando las bases que sustentan la sociedad. El incremento en la producción y circulación de información, más conocido como *Infodemia* en el contexto de la salud pública, pueden provocar una amenaza en la toma de decisiones informadas por las personas.

Sin embargo, uno de los mayores desafíos al intentar delimitar el concepto es que no existe hoy una definición única del fenómeno y, a pesar de los esfuerzos internacionales por relevar y definir los bordes del problema, su naturaleza política no ha permitido un consenso general al respecto. Por algunos autores ha sido descrito como “desorden informativo”<sup>1</sup> y da cuenta de la complejidad del problema, y sus consecuencias efectivas atraviesan múltiples áreas de interés público, tales como la salud, la gestión de los desastres naturales, el medio ambiente, las relaciones internacionales, el cambio climático, y la seguridad nacional, entre otros tópicos.

Al alero de los recientes conflictos en el mundo, la desinformación se ha convertido en una nueva arma para la desestabilización y socavamiento de los Estados. Sus implicancias están siendo exploradas, y aunque lejanas para nuestra realidad, plantean nuevos desafíos de cómo abordar este fenómeno en general.

## SEGURIDAD NACIONAL Y DESINFORMACIÓN

En junio del 2023, el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación crea la Comisión Asesora contra la Desinformación, instancia que reúne a un grupo de expertas y expertos para realizar dos informes asociados a la desinformación, el primero sobre el estado actual del fenómeno en términos de investigación y avances académicos, y el segundo, que entregará orientaciones y recomendaciones respecto a la formulación de posibles medidas o políticas públicas.

En ese sentido, dentro del primer informe de la Comisión<sup>2</sup>, es una de las principales amenazas de las sociedades libres. Su producción es sistemática e influye en el fuero más íntimo de las personas: la toma de decisiones. Así lo han descrito y publicado diferentes instituciones globales, como el Foro Económico Mundial (2013), la Unión Europea (2018), la UNESCO (2020), la OMS (2022) y la APEC (2022), entre otras organizaciones que ven en la desinformación un problema para la sociedad.

Las acciones impulsadas por distintos países y entidades supranacionales abordan la desinformación desde diversos ángulos. Se busca proteger los procesos democráticos ante las amenazas de contenidos falsos y engañosos, con diferentes objetivos, entre ellos, resguardar la seguridad nacional, creando herramientas para detectar y contrarrestar campañas de injerencia externa que utilizan técnicas de desinformación.

1 Wardle, Claire. 2018. «The Need for Smarter Definitions and Practical, Timely Empirical Research on Information Disorder». *Digital Journalism* 6(8): 951-63.

2 Anguita, P., Bachmann, I., Brossi, L., Elórtégui, C., Escobar, M.J., Ibarra, P., Lara, J.C., Padilla, F. y Peña, P., (2023). El fenómeno de la desinformación: Revisión de experiencias internacionales y en Chile. Santiago: Comité Asesor contra la Desinformación; Ministerio de Ciencia, Tecnología, Conocimiento e Innovación.

En relación con la seguridad, la comisión destaca que la “preocupación por la desinformación se ha intensificado en el marco del actual escenario geopolítico mundial” y donde “lo delicado de esta situación es que las estrategias de desinformación se sofistican y pueden materializarse a través de lo que se denomina “cibertropas”, que producen de manera activa contenidos como memes, videos, sitios web de noticias falsas o medios manipulados para engañar a los usuarios.

En marzo del presente año, el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno de España publicó su Informe Anual de Seguridad Nacional, que señala en su introducción que “la creciente conectividad, que nos llega de la mano de la globalización, tiene importantes beneficios, pero también contribuye a la materialización de riesgos y amenazas” tal como los ataques rusos a infraestructuras críticas ucranianas y el sabotaje de gasoductos, como también, “el empleo de estrategias híbridas que pueden implicar campañas de desinformación”<sup>3</sup>.

Técnicas de propaganda, usuarios y grupos falsos en plataformas digitales, publicidad engañosa, bots, inteligencia artificial y uso de deepfakes son algunas de las técnicas que adoptan las campañas de desinformación para influir en los comportamientos y decisiones de la ciudadanía, las cuales ante todo persiguen influenciar en la opinión pública, afectando la percepción que tienen los ciudadanos de la realidad y sobre su forma de relacionarse con su entorno, tanto social como políticamente. Se trata de un fenómeno cada vez más prevalente, que presenta un riesgo de seguridad para los Estados democráticos y de Derecho, sobre todo en contextos específicos y delicados socio políticamente hablando.

## EL ROL DE LA TECNOLOGÍA Y LA INTELIGENCIA ARTIFICIAL

Para poner en relieve, el uso de la inteligencia artificial, con su capacidad para analizar grandes volúmenes de datos y crear contenidos mediante algoritmos generativos, ha sido tanto una oportunidad como un riesgo en la era de la desinformación.

Los chatbots, y socialbots, que utilizan IA, pueden generar una importante confusión entre las personas, dado que alcanzan un elevado nivel de sofisticación al punto que, como humanos, tenemos gran dificultad en distinguir entre un mensaje creado por un socialbot o uno creado por alguna persona. Más aún, la redacción puede ser personalizada y extremadamente convincente al momento de transmitir alguna información errada, influyendo aún más en nuestra percepción sobre un tema en particular. También, es posible imitar estilos de escritura y generar “alucinaciones”, que responden a la generación de información a partir de bases de datos inconsistentes y con fuertes sesgos.

No obstante a lo anterior, es importante mencionar que la IA nos permite también poder construir herramientas para detectar algoritmos que estén siendo utilizados en la propagación de información errónea o incompleta, o bien, para opacar relegando a un segundo plano mensajes reales sobre algún tema en particular. Los algoritmos desarrollados para la detección de noticias falsas han ido poco a poco tomando posicionamiento, en donde uno de los principales elementos distintivos es el comportamiento que dichos mensajes tienen en las plataformas digitales, tal como la rápida propagación, el gran número de “likes”, etc.

Existen además otros desafíos en donde herramientas basadas en IA pueden tener un rol en la detección del uso malicioso de las plataformas digitales, como son los *deepfakes*. Conocido es el ejemplo del “primer deepfake” usado en contexto de un conflicto armado, donde se muestra al presidente de Ucrania, Zelenski ordenando la rendición

3 Informe Anual de Seguridad Nacional 2022 | DSN

de su ejército y el pueblo ucraniano. Como *deepfake* entendemos algún audio, imagen o video que nos genera la percepción de capturar algún evento real, imitando la voz, apariencia o gestos de alguna persona, pero que en realidad, ha sido generado de forma artificial. El poder detectar de forma automática si algún audio, imagen o video ha sido manipulado requiere un alto nivel de sofisticación, en donde el trabajo multidisciplinar es fundamental. Por dar un ejemplo, el software *DeepCatcher* @ Intel utiliza como validador para videos de personas los colores en el rostro, asociados a variaciones del flujo sanguíneo, que se encuentran alineados con la emocionalidad del hablante. Es muy importante mencionar que este tipo de algoritmos puede también fallar, catalogando como *deepfake* algún audio, imagen o video que no ha sido manipulado.

Sin embargo, el desafío radica en equilibrar la seguridad con la protección de las libertades civiles, evitando así que la vigilancia excesiva socave los valores democráticos. Es por ello que el dilema entre seguridad, IA como mecanismo para combatir la desinformación y democracia es complejo. Los Estados implementan sistemas de IA para mejorar la seguridad, pero esto puede llevar a la vigilancia masiva que amenaza la privacidad y las libertades individuales. La transparencia y la rendición de cuentas son fundamentales por lo que los gobiernos deben establecer políticas que regulen el uso de la IA en el ámbito de la seguridad, garantizando que se utilice para proteger a los ciudadanos sin socavar los principios democráticos.

En ese sentido, conflictos como Rusia-Ucrania y Hamas-Israel, sin bien distantes geográficamente a Chile, están moviendo la barrera de las campañas de desinformación, poniendo en relieve la necesidad de contar con mecanismos nacionales, regionales e internacionales que permitan tener herramientas de prevención, coordinación, límites y mitigación de sus efectos.

## EL ROL DE LA TECNOLOGÍA Y LA INTELIGENCIA ARTIFICIAL

A nivel mundial, entre las iniciativas concretas para combatir la desinformación se incluyen comisiones de expertos de análisis y recomendaciones, grupos de trabajo al interior de los gobiernos, y proyectos que invitan a los ciudadanos a reportar casos de desinformación. Varios países han impulsado medidas legislativas y de corregulación para abordar este fenómeno. La Unión Europea ha sido pionera con la implementación de códigos de conducta y buenas prácticas dirigidos a plataformas digitales. También creó un observatorio independiente para monitorear la desinformación en medios digitales. En Estados Unidos se han alzado voces que piden mayor liderazgo del gobierno en materia de gobernanza de plataformas, con participación conjunta de empresas, autoridades y sociedad civil. La OCDE promueve respuestas integrales y multidimensionales, que combinen regulación, políticas públicas, educación mediática, apoyo al factchecking y cooperación entre sectores, siempre sobre la base del respeto a los derechos humanos.

El desafío radica en equilibrar la seguridad con la protección de las libertades civiles, evitando así que la vigilancia excesiva socave los valores democráticos

Pero en general, las soluciones implican una educación pública robusta sobre cómo identificar noticias que desinformen o malinformen y entender cómo funciona la IA en estos contextos. Contextos como los actuales en donde la convivencia con un mundo híbrido donde la IA es parte de nuestra cotidianidad, nos impone una serie de desafíos que debemos abordar como individuos, como sociedad y como humanidad. Para ello, primero que todo, debemos establecer un léxico común, preciso y consensuado, de los diferentes fenómenos producidos por la interacción entre la IA y las plataformas digitales. Por otro lado, debemos generar conciencia sobre el alcance y limitaciones de los algoritmos actuales de IA, desmitificando creencias y sensibi-

lizando sobre las implicancias éticas del desarrollo tecnológico. Más aún, necesitamos contar con algoritmos de detección entrenados para nuestros ecosistemas informativos, pudiendo éstos ser más efectivos a la hora de levantar alertas de detección de algún fenómeno de desinformación. Además, debemos transitar hacia desarrollos tecnológicos abiertos que den cuenta de las bases de datos utilizadas para generar los entrenamientos, del seguimiento de los algoritmos entrenados al momento de discernir si siguen ejecutando la tarea originalmente encomendada con la misma confiabilidad, y por sobre todo, conformar equipos de trabajo diversos que permitan evaluaciones más completas e integrales del impacto del desarrollo tecnológico en nuestra sociedad.

Por otro lado, la colaboración global entre Estados, empresas y ciudadanos es esencial para preservar la integridad democrática en la era digital, donde la inteligencia artificial y la desinformación son fuerzas poderosas que moldean nuestras percepciones y decisiones políticas.



# LA ARMADA DE CHILE EN RIMPAC Y SU CONTRIBUCIÓN A LAS RELACIONES INTERNACIONALES

Por ALBERTO GUERRERO GARCÍA



**Alberto Guerrero García**, Capitán de Navío de la Armada de Chile, es especialista en Estado Mayor e Ingeniero Naval en Armamentos con mención en Guerra de Superficie. Posee el grado Académico de Magister en Ciencias Navales y Marítimas y Master in Business Administration de la Universidad Salve Regina en Rhode Island, Estados Unidos. En 1996 asistió al "International Sub lieutenant Course" en Britannia Royal Naval College y en 1998, participó en la Patrulla Antártica Naval Combinada a bordo del ARA Gurruchaga. El año 2006 asistió al Department Head Course en el Surface Warfare School de la Armada Norteamericana y el año 2008 efectuó el International Principal Warfare Officer's Course en HMS Collingwood en Reino Unido. Entre los años 2016 y 2018 se desempeñó como alumno del Naval War College y posteriormente como international fellow de dicha academia. Su carrera operativa se ha desarrollado en unidades de la Escuadra y Comando de Misileras, ejerciendo el mando de la LPC Bolados, el ATF Galvarino y la FF Condell. Entre los años 2021 y 2022 se desempeñó como Jefe del Departamento de Planes de la Subsecretaría de Defensa, hasta enero del 2023 cuando asume como Secretario del Comandante en Jefe de la Armada.

## RESUMEN

El ejercicio "Rim of the Pacific", conocido internacionalmente como RIMPAC, es hoy en día, el ejercicio naval multinacional más grande del mundo, que se desarrolla cada dos años en las costas del archipiélago de Hawái. El ejercicio constituye uno de los entrenamientos conjuntos y combinados más desafiantes del ámbito marítimo, congregando a las marinas más poderosas y profesionales de la Cuenca del Pacífico y Europa, con el propósito de perfeccionar las capacidades para interoperar en un escenario de crisis internacional, bajo un mandato de las Naciones Unidas.

Consecuentemente, la participación de la Armada de Chile en este ejercicio, contribuye directamente al fortalecimiento de las relaciones internacionales del país en el Asia Pacífico, ya que no sólo potencia su preparación profesional para la defensa de nuestra soberanía, si no que permite establecer lazos para cooperar y construir medidas de confianza mutua con naciones amigas y, de esa forma, velar por la seguridad de los océanos, la protección del comercio internacional, el resguardo de los puertos y el cuidado de las áreas marinas protegidas y las líneas de comunicaciones marítimas, elementos que conforman verdaderos pilares del desarrollo y prosperidad de nuestra nación.

**Palabras clave:** RIMPAC – Ejercicios Navales – Marinas del Pacífico y Europa

## ABSTRACT

The "Rim of the Pacific" exercise, known internationally as RIMPAC, is today the largest multinational naval exercise in the world, which takes place every two years off the coast of the Hawaiian archipelago. The exercise constitutes one of the most challenging joint and combined training in the maritime field, bringing together the most powerful and professional navies of the Pacific Rim and Europe, with the purpose of perfecting the capabilities to interoperate in an international crisis scenario, under a mandate of the United Nations. Consequently, the participation of the Chilean Navy in this exercise directly contributes to the strengthening of the country's international relations in the Asia Pacific, since it not only enhances its professional preparation for the defense of our sovereignty, but also allows establishing ties to cooperate and build measures of mutual trust with friendly nations and, in this way, ensure the security of the oceans, the protection of international trade, the protection of ports and the care of marine protected areas and maritime lines of communications, elements that make up true pillars of the development and prosperity of our nation.

**Keywords:** Rimpac – Naval Exercises – Pacific and European Navies



RIMPAC

## HISTORIA DE RIMPAC

La primera versión de RIMPAC se desarrolló en 1971 y, en sus orígenes, contaba con la participación exclusiva de las Armadas de Estados Unidos, Canadá, Nueva Zelanda, Reino Unido y Australia, quienes se enfrentaban a un escenario de Guerra Fría, donde el adversario era la desaparecida Unión Soviética.

A través de los años, el ejercicio RIMPAC ha ido evolucionando y creciendo en tamaño e importancia, ajustándose a las nuevas potenciales amenazas, debido fundamentalmente al hecho que el Océano Pacífico y la región Asia Pacífico, se han convertido en el centro de gravedad de los asuntos mundiales del siglo XXI, en virtud del peso y dinamismo de las economías y la trascendencia de los países y poblaciones que se ubican en sus riberas.

Actualmente, en RIMPAC se entrenan operaciones navales combinadas y conjuntas, en un escenario donde dos países ficticios, se encuentran en crisis y uno de ellos, contraviene el derecho internacional en desmedro del otro. Este suceso genera la reacción del Consejo de Seguridad de las Naciones Unidas (ONU), el que, como medida de mitigación, dicta una resolución que insta al país agresor a depone su actitud ofensiva lo antes posible.

De acuerdo al libreto del ejercicio, el país agresor hace caso omiso a la primera Resolución del Consejo de Seguridad de la ONU, debiendo emitir una segunda resolución que considera la advertencia de la imposición de la paz de una fuerza multinacional, junto con ciertas sanciones y establecimiento de zonas de exclusión, como también medidas que impidan la importación de armas y ciertos elementos que pudiesen ser utilizados por el país agresor en beneficio de sus fuerzas militares.

Consecuentemente, la ONU solicita a los países adherentes, conformar una fuerza multinacional, con el propósito de conminar al país agresor a depone su actitud y dar cumplimiento al mandato del Consejo de Seguridad de la ONU, amparados en el derecho internacional y el manejo de reglas de enfrentamiento.

Durante el desarrollo de las distintas etapas del ejercicio, se realizan operaciones antisubmarinas, antiaéreas y anti superficie, así como lanzamiento de armas, simulaciones antipiratería, operaciones de abordaje y registro y maniobras de reaprovisionamiento, tanto aéreas como en el mar. Paralelamente, en las distintas islas del archipiélago de Hawái, se realizan otras actividades en el marco de RIMPAC, como ejercicios con equipos de fuerzas especiales, simulaciones de barrido de minas y ejercicios anfíbios.

En sus versiones más recientes, RIMPAC ha incluido otros ejercicios adicionales, donde se simula la ocurrencia de un desastre natural, que exige el apoyo internacional en funciones de asistencia humanitaria (HADR en sus siglas en inglés). Esta nueva faceta de RIMPAC ha permitido incorporar distintas ONG, la Cruz Roja Internacional y a la Academia, a través de universidades norteamericanas y europeas, trabajando codo a codo, junto a fuerzas armadas de diversas naciones del Asia Pacífico.

Dada la diversidad de los medios participantes, RIMPAC también ha servido como plataforma de prueba de nuevas tecnologías y prototipos, como fue el caso del año 2012, donde aeronaves australianas y norteamericanas emplearon un combustible de aviación menos contaminante que los actualmente en uso, ya que era de origen vegetal<sup>1</sup>.

En estos más de 50 años de existencia, 35 naciones han participado en las distintas versiones de RIM-

<sup>1</sup> La prueba de dicho combustible resultó exitosa, ya que las aeronaves operaron sin observaciones, aunque el combustible no se ha masificado, dado que es una tecnología aún en desarrollo y su costo es ostensiblemente mayor al combustible de origen fósil.

PAC, incluyendo a Rusia en el año 2012 y China en el 2014<sup>2</sup>.

Por lo general, cada versión congrega a más de 20 naciones, donde las armadas que habitualmente han participado con medios navales y aéreos son: Australia, Canadá, Chile, Francia, Indonesia, Japón, Malasia, Corea del Sur, Singapur, Tailandia, Reino Unido, Estados Unidos, India, México, Nueva Zelanda, Noruega, Filipinas, Singapur y Tonga. Asimismo, con medios navales o en calidad de observadores o integrantes de un staff, han concurrido otras marinas como Bangladesh, Brasil, Brunei, Camboya, Colombia, Dinamarca, Ecuador, Holanda, Italia, Maldivia, Papua Nueva Guinea, Perú, Sri Lanka y Vietnam.

La última versión de RIMPAC ocurrió en el año 2022 y fue la de mayor dimensión realizada hasta la fecha, ya que contó con la participación de 27 naciones, 45 buques de superficie, 6 submarinos (nucleares y convencionales), más de 200 aeronaves y 25.000 efectivos provenientes de las distintas marinas participantes. La Armada de Chile participó con la fragata FF Lynch, un helicóptero SH-32, una compañía de infantería de marina y personal que integró los staff y puestos de mando en tierra.

La complejidad del ejercicio y la vastedad de medios humanos y materiales involucrados, demandan una exhaustiva planificación, la cual se desarrolla durante 18 intensos meses previos al inicio de RIMPAC, por lo que, al término de cada versión, se dice que comienza inmediatamente la preparación de la que le sucederá dos años después, incorporando las experiencias y lecciones aprendidas durante las jornadas de navegación.

Dada la magnitud del ejercicio y la cantidad de naciones participantes, es que se puede afirmar que RIMPAC se ha convertido en un hito importante de las relaciones internacionales de los países de la región, ya que la protección y resguardo del buen

orden en el mar, la estabilidad y el comercio internacional en el Asia Pacífico, requieren de un sistema de alianzas entre los países que le circundan, por lo que es habitual durante el ejercicio, que las unidades participantes, sean visitadas en puerto y en el mar por diversas autoridades, como ministros, embajadores y subsecretarios, que buscan interiorizarse de las capacidades alcanzadas y estrechar lazos entre los países participantes.

## LA ARMADA DE CHILE EN RIMPAC

Siendo Chile una nación esencialmente marítima, cuya economía se sostiene principalmente por el intercambio comercial en el Asia Pacífico, surgió la necesidad imperativa que la Armada se incorporase al ejercicio RIMPAC, como un actor relevante en la protección de la puerta sur del Océano Pacífico, en directa contribución a la política exterior del estado y resguardo de los intereses nacionales en la región.

Fue así como en 1996, Chile pasó a ser el primer país sudamericano en participar en RIMPAC, con la fragata PFG Lynch y un helicóptero SH32. Desde entonces, la Armada de Chile ha participado de manera ininterrumpida en cada versión del ejercicio<sup>3</sup>, asumiendo cada vez mayores responsabilidades y un rol más relevante en el desarrollo y conducción de éste.

En estos 27 años de participación activa, la Armada ha desplegado distintos buques, submarinos, aeronaves y recientemente unidades de infantería de marina, dando cuenta de la versatilidad de los medios involucrados. Lo anterior, requiere de un esfuerzo logístico, técnico y personal significativo, donde la preparación profesional, el empleo del idioma inglés y la incorporación de procedimientos OTAN en la operación habitual de las unidades na-

2 Tanto Rusia como China, sólo han participado en una ocasión. Rusia suspendió su participación con motivo de anexión de la Península de Crimea, mientras que China decidió no participar nuevamente producto de sus reclamaciones de soberanía en el mar de China.

3 Excepto el año 2010, debido a las consecuencias ocasionadas por el terremoto y posterior tsunami que afectó al país.

cionales, han resultado fundamentales para estar a la par de las principales marinas de la región.

De forma paralela y, gracias al profesionalismo y compromiso de las dotaciones, a lo largo de los años la Armada de Chile ha ganado un importante espacio en la planificación y conducción del ejercicio. Fue así como en el año 2012 fue la primera marina no anglo parlante invitada a asumir la conducción de fuerzas en la estructura orgánica de RIMPAC, comandando el Grupo de Tarea 170.1 dependiente de la Fuerza de Tarea 170, Carrier Strike Group (CSG), integrado por el portaviones USS Nimitz y quince unidades de combate de distintos países, siendo la primera vez en la historia de RIMPAC que una marina que no fuera una de las fundadoras del ejercicio ocupara dicho puesto.

del ejercicio, al reunir la mayor cantidad de medios navales y aéreos bajo su mando, lo que marcó un verdadero hito en la historia de RIMPAC.

Adicionalmente, con el transcurso de los años, se han sumado delegaciones del Ejército, la Fuerza Aérea y del Estado Mayor Conjunto de Chile (EMCO), integrando los distintos staff y fuerzas terrestres, demostrando la relevancia que significa para nuestro país la participación en RIMPAC y el compromiso conjunto en un ejercicio combinado esencialmente marítimo.

Resulta evidente, que la Armada de Chile ha sido pionera en posicionarse en un sitio destacado, frente a sus pares en el Asia Pacífico, contribuyendo a las relaciones internacionales de nuestro país.

## Siendo Chile una nación esencialmente marítima, cuya economía se sostiene principalmente por el intercambio comercial en el Asia Pacífico, surgió la necesidad imperativa que la Armada se incorporase al ejercicio RIMPAC

Los años 2014 y 2016, la Armada enfrentó un desafío de mayor responsabilidad, al asumir como segundo al mando de la Componente Marítima del ejercicio (Deputy Combined Forces Maritime Component Commander—DCFMCC), lo que requirió de un mayor número de oficiales y gente de mar para conformar el staff y dotar al Centro de Operaciones Marítimas<sup>4</sup>, desde donde se dirige el ejercicio, de personal idóneo y angloparlante para la conducción de las fuerzas combinadas marítimas.

Estas destacadas participaciones, proveyeron la experiencia y preparación necesarias para asumir aún mayores responsabilidades en la jerarquía y conducción del ejercicio. Fue así como en el año 2018, en el marco de nuestro bicentenario, se invitó a la Armada a asumir como Comandante de la Componente Marítima (CFMCC), que es uno de los roles de más alta responsabilidad en la estructura

Los éxitos alcanzados son fruto de un trabajo serio y coherente en el tiempo, donde el dominio del idioma inglés y los protocolos de comunicaciones, así como los estándares de entrenamiento y el desarrollo de procedimientos de operación y su compatibilidad con otras marinas, dan garantías de poder operar en forma segura y coordinada con otras naciones, para hacer frente a escenarios multi amenaza, con alto grado de incertidumbre, velando por la protección y resguardo de los intereses nacionales, donde sea que ellos se encuentren.

## COMENTARIOS FINALES

En un mundo globalizado, las amenazas que pueden afectar la estabilidad y seguridad de los océanos, así como el comercio internacional, son tan variadas y cambiantes en su origen y naturaleza, que

4 En inglés Maritime Operations Center (MOC)

no se ven disuadidas de actuar por la sola existencia de fuerzas navales. Por lo anterior, resulta fundamental robustecer la presencia de esas fuerzas navales en aquellas áreas de interés para la nación, ya que su ausencia es la que habilita el actuar de amenazas como el narcotráfico, la piratería, la pesca ilegal y el terrorismo, por nombrar algunas.

La vastedad de los espacios marítimos en el Asia Pacífico, hace imposible que un solo país pueda, por sí sólo, resguardar simultáneamente todos los intereses nacionales en la región, por lo que la cooperación internacional, por medio de acuerdos y alianzas, resulta vital en la protección de aquellas áreas de interés y líneas de comunicaciones marítimas.

Chile es un país esencialmente marítimo, cuyo futuro se encuentra en el Asia Pacífico. Ahora bien, para poder aprovechar las oportunidades que ofrece esta región, se debe aceptar un rol protagónico y asumir las responsabilidades y compromisos internacionales, acordes a la estatura político-estratégica que se intenta alcanzar y, es ahí donde la Armada y su participación en el ejercicio RIMPAC, contribuyen directamente a las relaciones internacionales del país.

El ejercicio RIMPAC busca promover la estabilidad regional en el Asia Pacífico y ofrece una estructura de mando y control similar a la de una coalición

multinacional, que, frente a un escenario realista de un posible de conflicto en la región, permite a los participantes entrenar en operaciones navales, tanto como a nivel de unidad, grupo y fuerza de tarea, incorporando múltiples variables, propias del mundo contemporáneo, como manejo de crisis, medios de prensa, apoyo humanitario, control del tráfico marítimo, cuidado del medio ambiente y respeto del derecho internacional bajo mandato de la ONU.

La participación de la Armada de Chile en RIMPAC, sólo ha traído beneficios y oportunidades para el país, ya que por más de 27 años ha sido un actor relevante en el ejercicio naval más grande del mundo, accediendo a los mayores estándares de entrenamiento, posicionándose como una marina de primer nivel en el Pacífico. Adicionalmente, ha contribuido a estrechar lazos de colaboración y cooperación internacional en la región, sobrellevando brechas culturales e idiomáticas, construyendo lazos y medidas de confianza mutua con naciones amigas, que perduran en el tiempo y que permiten diariamente proteger nuestro desarrollo económico, bienestar y progreso.

Ya está en marcha la preparación del ejercicio RIMPAC 2024, donde una vez más, la Armada de Chile estará presente con medios humanos y materiales, contribuyendo a la política exterior del país, resguardando la soberanía y los intereses nacionales, donde sea que ellos se encuentren.

## BIBLIOGRAFÍA

1. Niemann Figari Federico, "Chile en Rimpac, un Desafío de Esfuerzo Planificado", Revista de Marina, 2012.
2. Oxley Lizana Arturo, "En Acción con las Principales Marinas del Mundo", Revista de Marina, 2013.
3. Betancourt Marchant, Javier. "Experiencias y lecciones aprendidas en RIMPAC 2014", Revista de Marina, 2014.
4. Emol. (2000). Destacada participación chilena en ejercicios navales. 2016, de Emol Sitio web: <http://www.emol.com/noticias/nacional/2000/07/14/26507/destacada-participacion-chilena-en-ejerciciosnavales.html>
5. GlobalSecurity.org. / Rim of the Pacific Exercise (RIMPAC). 2016, de Global Security Sitio web: <http://www.globalsecurity.org/military/ops/rimpac.htm>

# INNOVACIÓN EN CIBERDEFENSA

Por KENNETH PUGH OLAVARRÍA



**Kenneth Pugh Olavarría**, Ingeniero Naval de Armamentos con mención en Electrónica. Magíster en Ciencias Navales y Marítimas con mención en Estrategia de la Pontificia Universidad Católica de Valparaíso. Durante los años 2004 y 2005, se desempeñó como Agregado de Defensa en la Embajada de Chile en Canadá. Entre 2006 y 2007, fue Jefe del Estado Mayor de la Cuarta Zona Naval. El año 2009 asume como Comandante en Jefe de la Cuarta Zona Naval. Al año siguiente es designado como Director de Inteligencia de la Armada y en enero de 2012 es nombrado Director General del Personal de la Armada. El 11 de marzo de 2018 asume el cargo de Senador por Valparaíso por el pacto Chile Vamos.

## RESUMEN

Este texto es una introducción al entendimiento de las bondades y peligros del Ciberespacio y su importancia en materia de Defensa y Seguridad. A su vez, expone ejemplos de casos reales y las medidas tomadas por diferentes Estados para impedir, disuadir, defenderse y contrarrestar nuevos Ciberataques, que puedan transformarse definitivamente en Ciberguerras.

**Palabras claves:** Ciberespacio – Defensa – Ciberataques – Ciberamenazas – Control

## ABSTRACT

This text is an introduction to understanding the benefits and dangers of Cyberspace and its importance in matters of Defense and Security. At the same time, it presents examples of real cases and the measures taken by different States to prevent, deter, defend and counteract new Ciberattacks, which can definitively transform into Cyberwars.

**Keywords:** Cyberspace – Defense – Ciberattacks – Ciber threats – Control



FREEPIK

**L**as grandes crisis traen las más grandes Innovaciones y muchas veces, de la mano del sector de la Defensa. En octubre del año 1962 el mundo estuvo a punto de entrar en una guerra nuclear, la que la extinta Unión Soviética denominó como “La Crisis del Caribe” y que en el mundo occidental conocemos como la “Crisis de los Misiles en Cuba”.

Esta crisis gatilló la necesidad de la Defensa de EE.UU. de contar con una red de mando y control que sobreviviera a un ataque nuclear. A pesar de todos los detractores, un científico de origen polaco de la Corporación RAND, Paul Baran<sup>1</sup>, fue el que propuso y probó una red robusta basada en la “redundancia” y “digital”. Él también desarrolló el concepto de dividir la información en “bloques de mensajes” antes de enviarlos por la red. Estos bloques, que se enviaban por separado, se volvían a unir cuando llegaban a destino. El británico Donald Davies ideó un sistema muy similar, pero llamó a los bloques de mensajes “paquetes”, término que acabó adoptándose hasta el día de hoy.

Fue la “Agencia de Proyectos de Investigación Avanzada” del Departamento de Defensa de EE.UU. (DARPA), a cargo del científico jefe Larry Roberts<sup>2</sup> quien en 1969 creó en la primera red de “conmutación de paquetes de datos” y en 1970 conectaron los primeros computadores llamándola ARPANET<sup>3</sup>, la que recopilaba las mejores ideas de los equipos del MIT, del “National Physics Laboratory” en UK y de la RAND Corporation, contando en 1971 con 24 computadores conectados. Curiosamente ese mismo año Robert Thomas, un ingeniero de Tecnologías BBN creó el que se reconoce como el primer “virus informático”<sup>4</sup>.

En 1972 Vinton Cerf y Robert Kahn<sup>5</sup> presentan el protocolo TCP/IP que sería la semilla para el nacimiento del “World Wide Web” en 1989, con la creación de los protocolos HTTP por Sir Tim Berners-Lee<sup>6</sup> en el CERN en Suiza. Sin embargo, el año anterior ya había ocurrido el primer ataque de denegación de servicios por un virus creado por el alumno Robert Morris de la Universidad de Cornell.

En apenas 30 años el “Ciberespacio” se ha convertido en la quinta dimensión o dominio de los conflictos armados, comenzando a ser considerado así desde 1995, y reafirmado el año 2000 cuando se publica la “Visión Conjunta al 2020”<sup>7</sup> de las Fuerzas Armadas de Estados Unidos que lo denominó como el “Dominio de la Información”. En la Cumbre de la OTAN de 2016 en Varsovia<sup>8</sup>, los Jefes de Estado y de Gobierno Aliados reafirmaron el mandato defensivo de la OTAN y reconocieron el Ciberespacio como un dominio de operaciones en el que la OTAN debe defenderse.

## PRIMERAS ACCIONES MILITARES EN EL CIBERESPACIO

Se reconoce como el primer ciberataque paralizante a un Estado el efectuado el 27 de abril de 2007 a Estonia, por parte de grupos desconocidos de ciberatacantes desde Rusia, los cuales protestaban por el movimiento de estatuas de héroes soviéticos. Fue tal el impacto en los sistemas financieros y estatales, que los cajeros automáticos dejaron de funcionar y los funcionarios del estado no pudieron usar sus correos electrónicos, ni los medios de prensa publicar noticias. Este fue el primer ciberataque a un estado miembro de la OTAN y no se pudo invocar el artículo cinco de dicha alianza, porque no se había causado una pérdida masiva de vidas humanas.

La respuesta de la OTAN fue crear al año siguiente el 2008 en Tallinn, la capital de Estonia, el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (NATO Cooperative Cyber Defence Centre of Excellence) o CCDOE<sup>9</sup>, cuya misión es apoyar a los países miembros y a la OTAN con una experiencia interdisciplinaria única en el campo de la investigación, la formación y los ejercicios de ciberdefensa, abarcando las áreas de tecnología, estrategia, operaciones y legislación.

Actualmente el CCDOE cuenta con 25 estados miembros y contribuyentes: Alemania, Bélgica, Bulgaria, Dinamarca, Eslovaquia, España, Estados Unidos, Estonia, Francia, Grecia, Hungría, Italia, Letonia,

Lituania, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumanía y Turquía. También cuenta con Austria, Finlandia y Suecia como "Miembros Participantes" y recibe países fuera del área europea por invitación de alguno de los Estados miembros, como es el caso de Japón con un oficial de enlace permanente y Brasil que es invitado a los ejercicios internacionales por Portugal.

La Armada de los EE.UU. creó a fines del año 2009 un nuevo Cuerpo profesional, fusionando varias especialidades, que pasó a llamarse el "Cuerpo de Dominio de la Información" (INFORMATION DOMINANCE CORPS), con los especialistas de Inteligencia, Guerra de Información, Tecnología de Información, Espacio; y Meteorología y Oceanografía. Hoy se conocen como la "Comunidad de Guerra de la Información de la Armada de los EE.UU."

Recién en enero del año 2010, la Armada de los Estados Unidos creó el "Cibercomando de la Flota de EE.UU." (U.S. Fleet Cyber Command) y reactivó una flota numerada para dedicarla al enfrentamiento en el Ciberespacio, la que designó como la "Décima Flota", tomando el nombre de la flota que enfrentó la amenaza submarina alemana de la Segunda Guerra Mundial, coordinando entonces todos los medios para enfrentarla mediante medidas de guerra antisubmarina basadas en inteligencia, pero ahora usa esta "Flota" para enfrentar las amenazas globales en el ciberespacio.

Este comando quedó al mando de un Vicealmirante y la Décima Flota al mando de una Contralmirante. Su ámbito de acción no solo se circunscribe al Ciberespacio, también considera el espectro electromagnético y el uso del espacio, según detallan ellos mismos<sup>10</sup> en su visión y misión.

La "Visión" del Cibercomando de la Armada de EE.UU. es llevar a cabo operaciones en y a través del ciberespacio, el espectro electromagnético y el espacio para garantizar la libertad de acción y la superioridad de decisión de la Armada y de las Fuerzas Conjuntas/Coalición, negando al mismo tiempo lo mismo a nuestros adversarios. Ganaremos en estos dominios a través de nuestro compromiso colectivo con la excelencia y mediante el fortaleci-

miento de nuestras alianzas con entidades de todo el gobierno de EE.UU., el Departamento de Defensa, el mundo académico, la industria y nuestros socios extranjeros.

La "Misión" del Cibercomando de la Armada de EE.UU. es planificar, coordinar, integrar, sincronizar, dirigir y llevar a cabo todo el espectro de actividades operativas en el ciberespacio necesarias para garantizar la libertad de acción en todos los ámbitos de combate de la Armada en, a través y desde el ciberespacio, y denegar dicha libertad a los adversarios de la Armada.

La Misión de la Décima Flota de los Estados Unidos es planificar, supervisar, dirigir, evaluar, comunicar, coordinar y ejecutar operaciones para permitir el mando y control y establecer las condiciones para los mandos subordinados:

- 1) Servir como flota numerada para el Mando Cibernético de la Flota de EE.UU. y ejercer el control operativo sobre las fuerzas asignadas al Cibercomando de la Flota de EE.UU..
- 2) Dirigir y proporcionar los efectos tácticos y operativos deseados en y a través del ciberespacio, el espacio y el espectro electromagnético a los mandos de la Armada en todo el mundo y garantizar la ejecución satisfactoria de las áreas de misión asignadas al Cibercomando de la Flota de los Estados Unidos.

Ese mismo año 2010 se produce el primer empleo militar de una "Ciberarma"<sup>11</sup>. Esta operación fue ejecutada a partir de Enero 2010, en contra de las plantas de enriquecimiento de uranio del programa Natanz, de Irán, la que se percibió como una falla mecánica de más de 1.000 centrifugas de enriquecimiento, deteniendo por completo el desarrollo nuclear Iraní.

El virus que afectó a esas plantas fue descubierto en junio del año 2010 por un investigador de ciberseguridad en Bileorusia de la empresa VirusBlokAda que lo denominó primero Rootkit.Tmpher y luego fue confirmado por la empresa antivirus Karspesky (creada por ingenieros rusos), los que informa-

ban de un nuevo virus que atacaba por primera vez sistema industriales SCADA, basados en software “Step 7” (S7) de Siemens para visualizar datos de los PLC. Al revisar el código se encontraron con las palabras “.stub” and “mrxnet.sys” de donde sacaron el acrónimo STUXNET, la primera de las Ciberarmas con capacidad de destrucción masiva, en este caso centrífugas de enriquecimiento de uranio, cambiando sus parámetros de operación para que entraran en un movimiento destructivo, enmascarando al mismo tiempo su acción para que no fueran presentados los parámetros de operación en los sistemas de monitoreo industrial.

Se estima que ese virus pudo haber ingresado a esa red industrial, desconectada de internet, a través de un pendrive, el que ejecutó un código malicioso que explotó cuatro vulnerabilidades de día cero, y atacó sistemas industriales, haciendo uso del conocimiento mecánico de funcionamiento de las centrífugas, para destruirlas usando principios físicos de movimientos armónicos.

Sin lugar a duda una tremenda arma solo capaz de ser concebida por un grupo selecto de expertos y con apoyo de uno o más Estados. Esta notable acción militar, que substituyó un ataque convencional de fuerzas especiales o un bombardeo aéreo estratégico, comprueba que el “Cibertalento” es la fuente más importante para generación de capacidades estratégicas en el Ciberespacio.

La creación y despliegue del virus STUXNET es considerado el inicio de la carrera de armamentos en el Ciberespacio, donde cada país puede construir sus propias ciberarmas ofensivas, para lo que requiere de capacidades nacionales propias, donde la más importante y escasa es el cibertalento.

Es en el Ciberespacio donde los Estados desarrollan sus operaciones militares para explotar las bondades del Ciberespacio en beneficio propio y negarle su empleo al adversario. La Ciberguerra es pues propia de “Actores Estatales”.

Los “Actores No Estatales” que hacen un uso malicioso del Ciberespacio para otros fines, ya sea por motivaciones para lograr protagonismo o re-

conocimiento, motivaciones por causas sociales, medioambientales o políticas que considera el ciberactivismo y el ciberterrorismo o definitivamente bandas criminales o el crimen organizado que persiguen obtención de dinero o influencia mediante extorsión o coerción, son los que cometen Ciberdelitos y son perseguidos usando las capacidades de investigación especializada en cibercrimen, como los es el “Convenio de Budapest”<sup>12</sup>, que permite perseguir a los cibercriminales en más de 68 países donde ya hay convenios, para que incluso las policías compartan evidencia digital entregada por las empresas tecnológicas relacionadas con el delito.

Las Operaciones Militares en el Ciberespacio son tradicionalmente agrupadas en tres grandes áreas y se las conoce como las “Operaciones Defensivas” (Ciberdefensa), las “Operaciones de obtención de información o Inteligencia” (Ciberinteligencia) y las “Operaciones Ofensivas” en el ciberespacio que pueden ir desde Ciberataques (CYBEROPS) hasta operaciones de manipulación de información (INFOOPS) mediante campañas de desinformación en línea, que abarca una serie de acciones que se conocen como la “Guerra de Información”.

Esta ha generado en la última década una nueva forma de conflictos, denominados “híbridos”, que van desde simples amenazas o escaramuzas en el ciberespacio hasta el empleo del concepto de la Estrategia Total de General André Beaufre (1902 – 1975) incluyendo al ciberespacio, para el desarrollo del empleo de todo el poderío militar en una guerra, en lo que se ha denominada la “Guerra Híbrida”.

El principal estrategia actual de la “Guerra Híbrida” es el General Ruso Valery Gerasimov, Jefe de Estado Mayor de las Fuerzas Armadas de Rusia, que la comienza a probar el año 2014 en la ocupación rusa de Crimea y de forma contundente el día 24 de Febrero 2022 cuando Rusia inició su “Operación Especial” e invadió Ucrania, atacando simultáneamente con fuerzas militares en los dominios tradicionales a los que agregó el ataque coordinado y sincronizado en el ciberespacio, buscando lograr una parálisis estratégica de su adversario, lo que no logró, dado que las fuerzas ucranianas ya estaban preparadas para este tipo de conflicto.

En diciembre de 2016, la OTAN y la Unión Europea acordaron más de 40 medidas para mejorar la colaboración entre ambas organizaciones, entre ellas la lucha contra las amenazas híbridas, la ciberdefensa y mejorar la estabilidad y seguridad de su vecindario. En materia de ciberdefensa, la OTAN y la Unión Europea acordaron reforzar su participación mutua en ejercicios y fomentar la investigación, la formación y el intercambio de información.

En febrero de 2017, los ministros de Defensa aliados aprobaron un “Plan de Acción de Ciberdefensa” actualizado, así como una hoja de ruta para implementar el ciberespacio como dominio de operaciones. Esto aumentó la capacidad de los Aliados para trabajar de forma combinada, desarrollar capacidades y compartir información.

También en febrero de 2017, la OTAN y Finlandia (que en ese momento era un país asociado y se adhirió a la OTAN en 2023) intensificaron su compromiso con la firma de un “Acuerdo Marco Político sobre Cooperación en Ciberdefensa”. El acuerdo permite a la OTAN y a Finlandia proteger mejor y mejorar la resistencia de sus redes.

En diciembre de 2017, los ministros de la OTAN y la Unión Europea acordaron intensificar la cooperación entre ambas organizaciones en una serie de ámbitos, entre ellos la ciberseguridad y la defensa. Las áreas de cooperación incluyen el análisis de las ciberamenazas y la colaboración entre los equipos de respuesta a incidentes (CSIRT), así como el intercambio de buenas prácticas relativas a los aspectos cibernéticos y las implicaciones de la gestión de crisis.

En la Cumbre de la OTAN de 2018 en Bruselas, los líderes aliados acordaron crear un nuevo “Centro de Operaciones del Ciberespacio” como parte de la estructura de mando reforzada de la OTAN. El Centro proporciona conocimiento de la situación y coordina la actividad operativa de la OTAN en y a través del ciberespacio. Los Aliados también acordaron que la OTAN puede recurrir a las capacidades cibernéticas nacionales para sus operaciones y misiones.

En febrero de 2019, los Ministros de Defensa de la OTAN aprobaron una guía de la OTAN que establece una serie de herramientas para fortalecer aún más la capacidad de la OTAN para responder a actividades cibernéticas maliciosas significativas. La OTAN necesita utilizar todas las herramientas a su disposición, incluidas las políticas, diplomáticas y militares, para hacer frente a las amenazas cibernéticas a las que se enfrenta. Las opciones de respuesta descritas en la guía ayudan a la OTAN y a sus Aliados a mejorar su conocimiento de la situación sobre lo que está ocurriendo en el ciberespacio, aumentar su capacidad de recuperación y colaborar con sus socios para disuadir, defenderse y contrarrestar todo el espectro de ciberamenazas.

En la Cumbre de la OTAN de 2021 celebrada en Bruselas, los Aliados aprobaron una nueva “Política Global de Ciberdefensa” para apoyar las tres tareas principales de la OTAN, así como su postura global de disuasión y defensa. La OTAN debe disuadir, defender y contrarrestar activamente todo el espectro de ciberamenazas en todo momento -en tiempos de paz, de crisis y de conflicto- y a nivel político, militar y técnico. Los Aliados reconocieron que el impacto de actividades cibernéticas acumulativas maliciosas significativas podría considerarse, en determinadas circunstancias, como un ataque armado. Los Aliados también acordaron hacer un mayor uso de la OTAN como plataforma de consulta política entre los Aliados, compartiendo preocupaciones sobre actividades cibernéticas maliciosas e intercambiando enfoques y respuestas nacionales, así como considerando posibles respuestas colectivas.

En septiembre de 2021, el Consejo del Atlántico Norte nombró al primer Director de Información (CIO) de la OTAN para facilitar la integración, alineación y cohesión de los sistemas TIC de toda la Alianza.

En la Cumbre de la OTAN de 2023, celebrada en Vilnius (Capital de Lituania), los Aliados aprobaron un nuevo concepto para mejorar la contribución de la ciberdefensa a la postura global de disuasión y defensa de la OTAN. Este concepto mejorará el conocimiento compartido de la situación y la resistencia cibernética de la OTAN, haciendo que la Alianza sea

más segura y capaz de mitigar el potencial de daños significativos provocados por las ciberamenazas.

En la Cumbre de Vilnius los Aliados también reafirmaron y reforzaron el Compromiso de Ciberdefensa y se comprometieron a alcanzar objetivos más ambiciosos para reforzar con carácter prioritario las ciberdefensas nacionales, incluyendo las infraestructuras críticas. Reconociendo la necesidad de recibir ayuda con rapidez, la OTAN también lanzó la "Capacidad Virtual de Apoyo a Incidentes Cibernéticos (VCISC)" para apoyar los esfuerzos nacionales de mitigación en respuesta a actividades cibernéticas maliciosas significativas. Los líderes también anunciaron la celebración de la primera Conferencia de Ciberdefensa de la OTAN en Berlín en noviembre de 2023, que reunirá a responsables políticos, militares y técnicos.

## EJERCICIOS MILITARES EN EL CIBERESPACIO

El Ciberejercicio anual más importante del mundo es organizado por el CCDCOE en Tallinn desde el año 2010, y permite a los expertos en ciberseguridad militar mejorar sus capacidades para defender los sistemas informáticos nacionales y las infraestructuras críticas en caso de ataques en tiempo real. Se centra en escenarios realistas, tecnologías de vanguardia y la simulación de toda la complejidad de un ciberincidente masivo, incluyendo la toma de decisiones estratégicas y los aspectos legales y de comunicación.

El ejercicio se llama "Locked Shields"<sup>13</sup> y es de doble acción, con equipos rojos (atacantes) contra equipos azules (los que defienden), estos últimos formados por países miembros del CCDCOE. En el año 2021 participaron 22 Equipos Azules con una media de 40 expertos en cada equipo. Los Equipos asumen el papel de Equipos de Reacción Rápida de Ciberseguridad nacionales que se despliegan para ayudar a un país ficticio a gestionar un Ciberincidente a gran escala con todas sus implicaciones. En el ejercicio de 2021 participaron unos 5.000 sistemas virtualizados que fueron objeto de más de 4.000 ataques.

Los equipos deben ser eficaces a la hora de informar sobre incidentes, ejecutar decisiones estratégicas y resolver problemas forenses, legales y mediáticos. Para mantenerse al día de los avances tecnológicos, el ejercicio "Locked Shields" se centra en escenarios realistas y tecnologías de vanguardia, redes relevantes y métodos de ataque.

El último ejercicio "Locked Shields" del año 2022, participaron más de 2000 ciberexpertos de 32 países en dos días de entrenamiento, donde practicaron la protección de sistemas informáticos nacionales e infraestructuras críticas bajo la presión de un ciberataque a gran escala en el ejercicio anual de ciberdefensa con "fuego real". Además de proteger numerosos sistemas ciberfísicos, los equipos participantes practicaron la toma de decisiones tácticas y estratégicas, la cooperación y la cadena de mando en una situación de crisis en la que también tuvieron que abordar cuestiones forenses y jurídicas y responder a retos de operaciones de información.

También a mediados de años se realiza en el CCDCOE en Tallin la "Conferencia de Ciberconflicto"-CyCon<sup>14</sup>, la que se ha consolidado como una destacada conferencia multidisciplinar que presenta ponencias y paneles centrados en las perspectivas técnicas, jurídicas, políticas, estratégicas y militares de la ciberdefensa y la seguridad. Esto se debe sin duda a la cantidad de investigaciones académicas originales de alta calidad que se presentan en la conferencia. Chile hasta la fecha no ha participado con ninguna ponencia.

El Ciberejercicio anual más importante del mundo es organizado por el CCDCOE en Tallinn desde el año 2010, y permite a los expertos en ciberseguridad militar mejorar sus capacidades para defender los sistemas informáticos nacionales y las infraestructuras críticas en caso de ataques

Cada año, más de 600 responsables de la toma de decisiones, líderes de opinión, expertos en derecho y tecnología de los gobiernos, las fuerzas armadas, el mundo académico y la industria de casi 50 países se reúnen en CyCon para abordar de forma interdisciplinar los retos actuales de la ciberseguridad. A lo largo de dos días y medio, los expertos abordan los temas clave de la conferencia en conferencias magistrales, sesiones plenarias, sesiones específicas y debates en grupos reducidos. Los talleres de CyCon permiten debatir en profundidad temas específicos relacionados con la tecnología y el desarrollo de malware, cuestiones de educación y formación, aspectos legales, etc., o proporcionan formación práctica. CyCon 2023 tuvo lugar en Tallinn del 30 de mayo al 2 de junio de 2023 con ponentes de 47 países de todo el mundo.

El otro ejercicio militar especializado en Ciber guerra realizado por el CCDOC es "Crossed Swords"<sup>15</sup>, un Ciberejercicio técnico anual de "equipos rojos" (Red Teaming), en el que se forma a especialistas en pruebas de penetración, expertos en análisis forense digital y expertos en conocimiento de la situación. A lo largo de los años, los Ciberejercicios "Crossed Swords" ha pasado de ser un taller de formación técnica relativamente sencillo a un ejercicio que también incluye formación en liderazgo para el elemento de mando, aspectos jurídicos y operaciones cibercinéticas conjuntas. El ejercicio también proporciona una oportunidad de entrenamiento para los miembros del Equipo Rojo que interpretan al adversario en el ejercicio de ciberdefensa "Locked Shields".

En 2021, tras dos años de confinamiento por la pandemia de COVID-19, el ejercicio se llevó a cabo íntegramente in situ. Reunió a un centenar de participantes de más de 21 países, incluidos Estados miembros y no miembros de la OTAN. Las últimas acciones de "Crossed Swords" han sido organizadas conjuntamente por el CCDCOE de la OTAN y CERT.LV (de Latvia).

El CCDCOE de la OTAN es la sede del Manual 2.0 de Tallin sobre el Derecho Internacional Aplicable a las Ciberoperaciones y Ciber guerra. El Centro también organiza el mayor y más complejo ejercicio técnico

internacional de ciberdefensa del mundo: "Locked Shields", la Conferencia Anual sobre CiberConflictos "CyCon", que reúne anualmente a más de 600 expertos.

Un nuevo Centro de Excelencia ha sido recientemente creado por el último miembro en incorporarse a la OTAN. En Helsinki, Finlandia, desde el año 2017 se basa en nuevo "Centro Europeo de Excelencia para la Lucha contra las Amenazas Híbridas" (Hybrid CoE)<sup>16</sup>, como una organización internacional autónoma, basada en una red, que lucha contra las amenazas híbridas.

En cuando al desarrollo del pensamiento estratégico en el empleo del ciberespacio, el profesor Charles M. Crowell, asociado del Centro de Estudios de Políticas Marítimas del Kings College de Londres, publicó en su paper<sup>17</sup> de enero 2017: "Algunos principios de la Ciber guerra, usando a Corbett para entender la guerra a principios del siglo XXI".

Crowell señala la necesidad de una nueva teoría de la guerra, pero emplea la visión estratégica marítima de Sir Julian Corbett (1854 -1922). En palabras de Crowell este señala que existe "consonancia con la idea de Clausewitz de que los objetivos que adopten los beligerantes se ajustarán al espíritu y al carácter de la época, muchos grupos contemporáneos ya están utilizando el ciberespacio y adaptando la tecnología para sus propios fines. Militares y civiles por igual utilizan ahora las operaciones del ciberespacio para alcanzar objetivos en materia de comunicación, selección de objetivos, navegación (sistemas de posicionamiento global-GPS), logística, formación, educación, compras, banca, entretenimiento y mucho más".

El ciberespacio ha impulsado cambios en la economía y la política nacional de muchos países, y las redes sociales han contribuido a modificar el poder político. El Profesor Crowell es académico del "Naval War College" de la Armada de EE.UU y es uno de los miembros fundadores del Instituto de Políticas Ciber e Innovación (originalmente el Centro de Estudios del Ciberconflicto), de dicha academias.

Aplicando los principios de la Estrategias Marítima de Corbett, el profesor Crowell propone los principios de la Ciberguerra, asociándola a la guerra en el mar.

El primer principio que propone es el “Control del Ciberespacio” como un objetivo positivo que debe alcanzarse para lograr la libertad de acción en todos los ámbitos. Es relativo al tiempo y al espacio y, al igual que el control marítimo, existe en grados, tal como lo señala en la página 18 de su paper.

El segundo principio lo basa en que, dado que el ciberespacio proporciona la capacidad de afectar los procesos de toma de decisiones y a los equipos o dispositivos tecnológicos, la función principal de una Ciberfuerza es favorecer o dificultar la toma de decisiones en operaciones y dominios de la guerra.

El tercer principio señala que el ciberespacio proporciona una nueva capacidad para interferir en cualquier economía moderna del mundo e influir así en el potencial militar-económico de los Estados.

Y el cuarto y último principio señala que una ciberdefensa eficaz será clave para que las fuerzas pasen a la ofensiva estratégica en futuros conflictos.

## LA CIBERDEFENSA EN CHILE

En Chile también se ha abordado el tema desde la perspectiva académica y de política pública.

El Centro de Estudios Estratégicos CEEAG de la Academia de Guerra del Ejército publicó el año 2018 el libro “La Ciberguerra: Sus Impactos y Desafíos”<sup>18</sup> con seis capítulos, los cuales cubrieron distintos aspectos.

El libro contiene lo siguiente: “Aparece la ciber guerra” por el General René Leiva Villagra, “Infraestructura crítica vulnerable a la ciber guerra” por Hernán Díaz Mardones, “La lógica de la ciber guerra y su relación compleja con la disuasión” por René Leiva Villagra, “El desafío del combate por el mando y control” por Mario Arteaga Velásquez, “Efectos de los riesgos y amenazas de la ciber guerra en la in-

fraestructura crítica” por Carl Marowski Pilowsky y “El Derecho Internacional como marco regulatorio de la ciber guerra” por Mario Polloni Contardo.

La Ciber guerra requiere de un nuevo perfil de combatientes, algunos de ellos seleccionados a temprana edad por sus talentos Ciber, otros como parte de una Ciber reserva activa. No solo se requieren destrezas y certificaciones adecuadas, se requiere mantenerlos permanentemente entrenado, tanto con Ciberejercicios Nacionales, como con Ciberejercicios Internacionales.

En Chile se publica por primera vez la “Política Nacional de Ciberdefensa” el día viernes 9 de marzo de 2018 en el Diario Oficial<sup>19</sup>, la que consta de seis capítulos<sup>20</sup>:

“La Introducción” aborda de forma general la rápida introducción las TIC en Chile y América Latina, tanto en las actividades privadas como en el sector público, así como el aumento de los ataques o incidentes sufridos por dichos sectores, dando cuenta de la creciente vulnerabilidad y dependencia que genera la utilización de este tipo de herramientas, lo que hace necesaria la adopción de una Política de Estado para hacer frente a estos nuevos riesgos y amenazas.

“El Diagnóstico” describe sucintamente el tipo de amenazas cibernéticas, desde el punto de vista de su periodicidad, sofisticación e impacto, al que están expuestas las instituciones del sector Defensa, proyectándose un aumento constante de aquellas a futuro.

“Los Principios de la Defensa Nacional y su aplicación al ciberespacio”, ahondan en los principios en los que se sostiene la Política de Ciberdefensa, poniendo énfasis en el respeto del marco institucional vigente, así como de los tratados y acuerdos internacionales firmados por Chile. En virtud de ello, dispone que el sector Defensa debe procurar una infraestructura de la información robusta y resiliente frente a los incidentes de ciberseguridad, respetando los derechos de las personas en el ciberespacio. Asimismo, debe velar por la promoción de una cultura de buenas prácticas y educación en este

ámbito. En materia de cooperación internacional, se señala como objetivo la prevención de acciones cibernéticas ilícitas desde Chile a otros estados, en el campo de la Defensa.

“La Política de la Defensa Nacional y su aplicación al ciberespacio”, aborda los efectos que puede tener un ciberataque, señalando que sus daños pueden ser comparables a los de un ataque armado, y por ello -en su derecho de legítima defensa, consagrado en el Artículo 51 de la Carta de las Naciones Unidas- el Estado chileno podrá hacer uso de los medios que estime necesarios para su respuesta, protección de infraestructura crítica de la información y correcta atribución de ataques, entre otros.

“La elaboración de un plan para la implementación de la política de Ciberdefensa”, distribuye los roles entre los distintos actores del sector Defensa. Asimismo, consagra un periodo de revisión de cuatro años de la Política, o cuando las circunstancias lo ameriten, proceso que será coordinado por la Subsecretaría de Defensa.

“El Glosario”, donde se definen los términos: Ciberataque, Ciberdefensa, Ciberespacio y Ciberseguridad. Adicionalmente, en un segundo artículo se establecen las disposiciones en relación con el gasto que genere la ejecución de la política de Ciberdefensa.

Hasta la fecha esta Política de Ciberdefensa no ha sido actualizada y varias instituciones de la defensa han sido atacadas, al igual que varios organismos estatales. No se cuenta aún con una organización nacional que permita enfrentar el problema con todas las capacidades del Estado, unidas a las del sector público de los diferentes sectores industriales, que permita anticiparse a acciones como esta, y en caso ocurran hechos graves en el ciberespacio, determinar la atribución del ataque y volver a poner los sistemas en servicio, recuperando las capacidades de operación en este medio, demostrando la resiliencia que se deben tener para enfrentar este tipo de ataques.

Este tema ha sido abordado en la nueva ley de “Gobernanza de Ciberseguridad” del país, próxima a

publicarse, donde se considera al “CSIRT de DEFENSA” como el encargado de gestionar los incidentes que ocurran en ese ámbito militar, el que se encuentra en proceso de crear un “Cibercomando Conjunto”, tal como lo hacen todos los países miembros de la OTAN, como lo es en España el “Mando Conjunto del Ciberespacio” (MCCE)<sup>21</sup> creado en febrero de 2013.

Esto también se hace desde más de una década a nivel regional por entidades similares como el Comando Conjunto de Ciberdefensa en Argentina<sup>22</sup> creado en mayo de 2014, o el Comando de Ciberdefensa de Brasil (ComDCiber), el más antiguo de Iberoamérica creado el año 2010, el mismo año en que por primera vez se usó una Ciberarma, el virus STUXNET, contra las plantas de enriquecimiento de uranio en Irán.

Sin lugar a dudas el Ciberespacio es el conjunto de los dominios de combate, lo que requiere además de las capacidades de ciberdefensa y ciberinteligencia institucionales, una capacidad de desarrollo de operaciones ofensivas en el Ciberespacio, de acuerdo a la planificación nacional.

Esta capacidad ofensiva, que es la que caracteriza toda Ciberguerra, requiere de personas altamente capacitadas y con talento ciber, de infraestructura digital adecuada, tanto para investigación como desarrollo de ciberarmas propias, junto con un avanzado sistema de entrenamiento, tanto en el país, como en el extranjero.

## LA INNOVACIÓN EN CIBERDEFENSA

Para poder enfrentar todas estas amenazas las fuerzas de la OTAN usan la información de “vulnerabilidades” detectadas en los distintos programas en uso, tanto en el mundo militar como en el mundo en base a un catálogo internacional actualizado a medida que se van encontrando por investigadores independientes, universidades o por las mismas empresas desde 1999 gracias al trabajo de la “Corporación MITRE”<sup>23</sup>.

Esta gran base de datos se conoce como el Programa CVE®<sup>24</sup>, cuya misión es identificar, definir y catalogar las vulnerabilidades de ciberseguridad divulgadas públicamente. CVE proviene del inglés: “Common Vulnerabilities and Exposures” y se identifican con un número de serie y año en que son encontradas, de acuerdo al siguiente patrón: CVE-2023-0051 que corresponde a reporte 51 asignado por una de las “Autoridades Designadoras de Vulnerabilidades” o CNA, siendo Chile incluido en como una de ellas gracias al trabajo de investigación que hace VULNSCOPE<sup>25</sup>.

Una vulnerabilidad es una debilidad que puede ser explotada para obtener acceso no autorizado o realizar acciones no autorizadas en un sistema informático. Las vulnerabilidades pueden permitir a los atacantes obtener acceso directo a un sistema o a una red, ejecutar código, instalar malware y acceder a sistemas internos para robar, destruir o modificar datos sensibles. Si no se detecta, podría permitir a un atacante hacerse pasar por superusuario o administrador del sistema con plenos privilegios de acceso.

Una exposición es un error que da acceso a un atacante a un sistema o red. Las exposiciones pueden permitir a los atacantes acceder a información personal y exfiltrarla. Algunas de las mayores violaciones de datos se debieron a una exposición accidental y no a sofisticados ciberataques.

A la fecha se han reportado más de 130.000 CVE, con una media anual entre 12.000 a 15.000 reportes, lo que da cuenta de la fragilidad del ciberespacio a los ataques para explotar vulnerabilidades o exposiciones conocidas. Las que se conocen por primera vez se les llama “Vulnerabilidades de día Cero” y son las más utilizadas para desarrollo de ciberarmas, por la sorpresa que generan.

Los actores criminales y estatales más peligrosos, que hacen uso malicioso del ciberespacio, han sido listados a partir del año 2005 por EE.UU. y UK y a partir del año 2007 se acuñó el término APT por el entonces coronel de la Fuerza Aérea Greg Rattray<sup>26</sup> que las denominó “Amenazas Persistentes Avanzadas” (APT: Advanced Persistent Threat).

El trabajo para levantar el listado de estas ATP ha demandado un considerable esfuerzo público – privado como por ejemplo el realizado a partir del año 2004 por la empresa “MANDIANT” hoy parte de Google, después de su compra en septiembre del 2022 por un valor de 5.400 millones de dólares.

Ese listado se hizo público sólo el año 2010, pese a que en año 2006 se identificó a la primera APT la que se conoce como “APT1”<sup>27</sup>, un grupo de ciberespionaje basado en China, el que se cree depende de un órgano del Ejército Chino encargado de las Operaciones en Redes de Computadores, la “Unidad 61398”, del Tercer Departamento de la Segunda Oficina del Estado Mayor del Ejército Popular de Liberación<sup>28</sup>. Empresas como Microsoft han usado recientemente los nombres de la tabla periódica de elementos para nombrar las amenazas persistentes avanzadas.

MITRE Corporation de EE.UU., ha levantado el catálogo completo de las taxonomías de los ataques lo que le ha permitido generar una gran base de datos de: Tácticas, Técnicas y Procedimientos, conocidos como TTP y las ha sistematizado en su modelo MITRE ATT&CK®<sup>29</sup> que es una base de conocimientos de acceso global sobre tácticas y técnicas de los adversarios basada en observaciones del mundo real. La base de conocimientos ATT&CK se utiliza como fundamento para el desarrollo de modelos y metodologías de amenazas específicas en la defensa, en el sector privado, en la administración pública y en la comunidad de productos y servicios de ciberseguridad.

Con la creación de ATT&CK, MITRE cumple su misión de resolver problemas para un mundo más seguro, reuniendo a las comunidades para desarrollar una ciberseguridad más eficaz. MITRE es una organización privada sin fines de lucro, financiada por el gobierno de EE.UU.

En Europa, las naciones de dicho continente que pertenecen a la OTAN, a partir del año pasado conmemoran el día de la “Innovación en Defensa”<sup>30</sup> el 31 de mayo para promover el reconocimiento a los talentos que han sido capaces de generar nuevas tecnologías de uso dual (civil y militar) y también

han instalado un HUB de Innovación en Defensa, conocido como HEDI<sup>31</sup> y una Aceleradora de Innovación del Atlántico Norte a la que denomina DIANA<sup>32</sup> ("Defence Innovation Accelerator for the North Atlantic").

En Chile es factible crear por ley el día de la "Innovación en Defensa" y una Corporación de derecho privado, sin fines de lucro y con financiamiento estatal aportado por las industrias estratégicas nacionales y los recursos de I+D+i que contemplan los fondos de desarrollo de capacidades estratégicas, al igual que la Corporación MITRE en EE.UU. y DIANA en Europa, permita acelerar el desarrollo de tecnologías duales de uso civil y militar mediante la: "Innovación en el Ciberespacio", la "Investigación en Ciberdefensa" y que sea a la vez el "Instituto Nacional de Ciberseguridad", que al igual que en España, que se encuentra en León, esté radicado en Valparaíso, cuya misión sea: "Resolver problemas complejos para hacer más seguro a Chile".

## BIBLIOGRAFÍA

- 1 Ver en <https://www.rand.org/about/history/baran.html>
- 2 Ver en: <https://computerhistory.org/profile/larry-roberts/>
- 3 Ver en <https://www.britannica.com/topic/ARPANET>
- 4 Ver en [https://www.worldscientific.com/doi/pdf/10.1142/9789811233128\\_0001](https://www.worldscientific.com/doi/pdf/10.1142/9789811233128_0001)
- 5 Ver en <https://www.fpa.es/es/premios-princesa-de-asturias/premiados/2002-lawrence-roberts-robert-kahn-vinton-cerf-y-tim-berners-lee.html?texto=trayectoria&especifica=0>
- 6 Ver en <https://www.w3.org/People/Berners-Lee/>
- 7 Ver en [https://rdl.train.army.mil/catalog-ws/view/100.ATSC/CE5F5937-49EC-44EF-83F3-FC25CB-0CB942-1274110898250/aledc\\_ref/joint\\_vision\\_2020.pdf](https://rdl.train.army.mil/catalog-ws/view/100.ATSC/CE5F5937-49EC-44EF-83F3-FC25CB-0CB942-1274110898250/aledc_ref/joint_vision_2020.pdf)
- 8 Ver en [https://www.nato.int/cps/en/natohq/topics\\_78170.htm#:~:text=At%20the%202016%20NATO%20Summit,conduct%20its%20missions%20and%20operations.](https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=At%20the%202016%20NATO%20Summit,conduct%20its%20missions%20and%20operations.)
- 9 Ver en <https://ccdcoe.org/>
- 10 Ver en <https://www.fcc.navy.mil/ABOUT-US/MISSION-VISION/>
- 11 Ver en <https://revistamarina.cl/revistas/2016/2/efrederickr.pdf>
- 12 Ver en [https://www.oas.org/juridico/english/cyb\\_pry\\_convenio.pdf](https://www.oas.org/juridico/english/cyb_pry_convenio.pdf)
- 13 Ver en <https://ccdcoe.org/exercises/locked-shields/>
- 14 Ver en <https://ccdcoe.org/cycon/>
- 15 Ver en <https://ccdcoe.org/exercises/crossed-swords/>
- 16 Ver en <https://www.hybridcoe.fi/about-us/> \*
- 17 Ver en <https://www.kcl.ac.uk/dsd/assets/corbett-paper-no19.pdf>
- 18 Ver en <https://www.ceeag.cl/wp-content/uploads/2020/06/LA-CIBERGUERRA-SUS-IMPACTOS-Y-DESAFIOS.pdf>
- 19 Ver en <https://www.diariooficial.interior.gob.cl/publicaciones/2018/03/09/42003/01/1363153.pdf>
- 20 Citados de [https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/31943/1/Informe\\_BCN\\_Politica\\_Nacional\\_de\\_Ciberdefensa.pdf](https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/31943/1/Informe_BCN_Politica_Nacional_de_Ciberdefensa.pdf)
- 21 Ver en <https://emad.defensa.gob.es/unidades/mcce/>
- 22 Ver en <https://www.fuerzas-armadas.mil.ar/Comando-Conj-Ciberdefensa/index.html>
- 23 Ver en <https://www.mitre.org/>
- 24 Ver en <https://cve.mitre.org/>
- 25 Ver en <https://www.cve.org/PartnerInformation/ListofPartners/partner/Vulnscope>
- 26 Ver en <https://ieeexplore.ieee.org/document/9380629>
- 27 Ver en <https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units>
- 28 Ver en <https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf>
- 29 Ver en <https://attack.mitre.org/>
- 30 Ver en <https://eda.europa.eu/news-and-events/events/2022/05/31/default-calendar/european-defence-innovation-day-31-may>
- 31 Ver en <https://eda.europa.eu/news-and-events/news/2022/05/17/hub-for-eu-defence-innovation-established-within-eda>
- 32 Ver en <https://www.diana.nato.int/>

# LA NUEVA CRIMINALIDAD QUE ENFRENTAMOS

Por EDUARDO CERNA LOZANO



**Eduardo Cerna Lozano** con 35 años de servicio, al momento de su nombramiento como Director General de la PDI, se desempeñaba como subdirector de Administración Logística y Administración, habiendo egresado en 1991 con la segunda antigüedad de su promoción. Además, como parte de su carrera integró las comisarías judiciales de San Miguel y Concepción; la Brigada de Delitos Económicos Metropolitana, la Fuerza de Tarea Sur (para las comunas de La Legua y La Victoria), y la Inspectoría General. En cargos de jefatura se ha desempeñado en la Brigada de Reacción Táctica Metropolitana; Escuela de Investigaciones Policiales (como subdirector) y Centro de Capacitación Profesional (director); Brigada de Investigación Criminal Santiago; Prefectura de Operaciones Especiales; Jefatura Nacional de Logística y Grandes Compras.

## RESUMEN

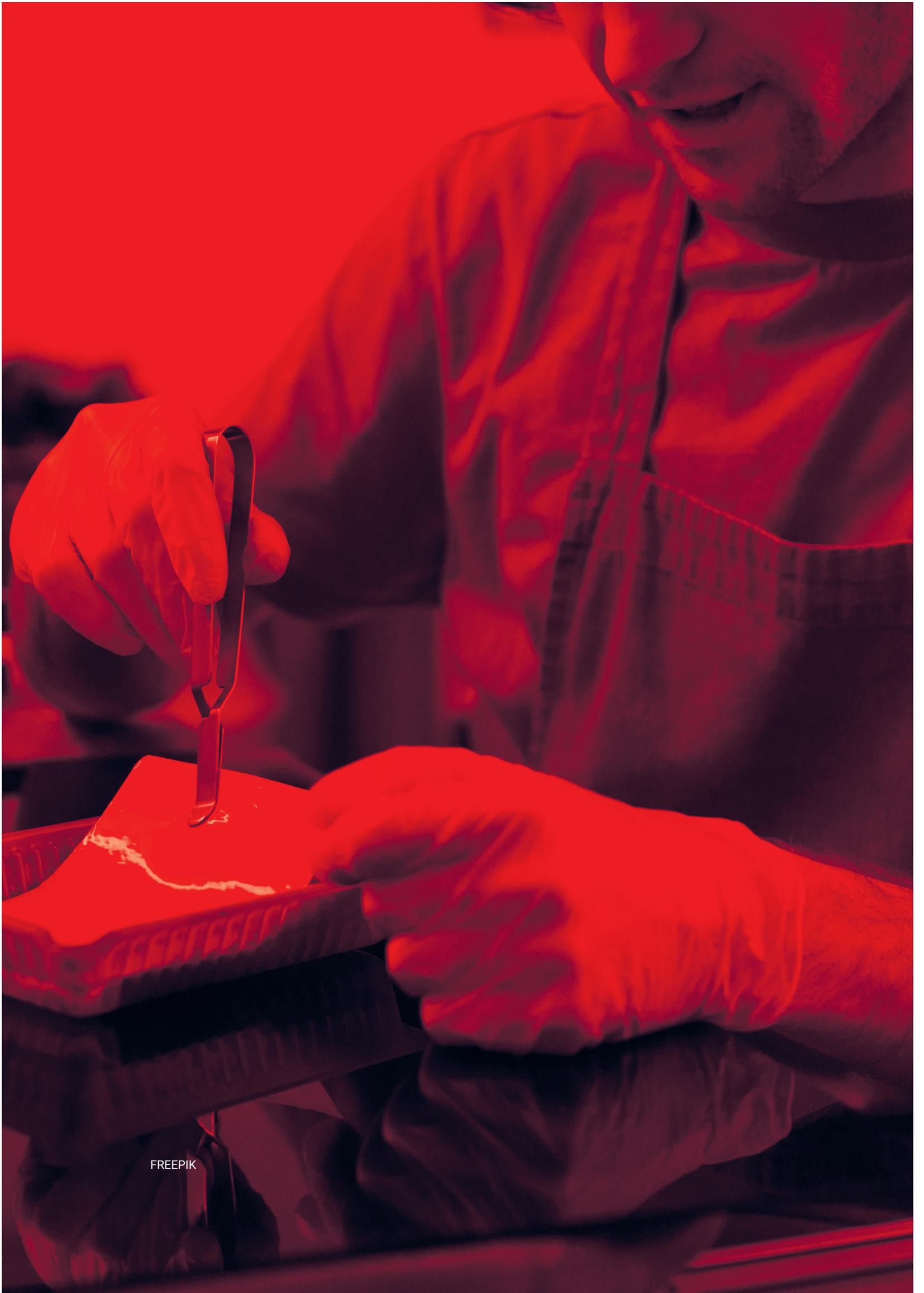
Este texto resume el Plan Estratégico de Desarrollo de la Policía de Investigaciones de Chile en materia de investigación de delitos complejos y crimen organizado transnacional; proyectando escenarios criminales emergentes e impulsando la transformación digital, a través de la creación del Centro Nacional de Análisis Criminal (Cenacrim).

**Palabras clave:** Crimen Organizado – Delitos Complejos–Cenacrim

## ABSTRAT

This text summarizes the Strategic Development Plan of the Chilean Investigative Police regarding the investigation of complex crimes and transnational organized crime; projecting emerging criminal scenarios and promoting digital transformation, through the creation of National Center for Criminal Analysis.

**Keywords:** Organized Crime – Complex Crimes–Cenacrim



FREEPIK

**C**on 90 años de historia, la Policía de Investigaciones de Chile proyecta el camino a su centenario, con importantes desafíos para enfrentar los cambios en la criminalidad del país.

Con poco más de 12.800 funcionarias y funcionarios, sus diversas áreas de servicio están unidas por un objetivo trascendental que es su compromiso con la búsqueda de la verdad, haciendo lo que más disfrutan y mejor saben hacer que es investigar delitos.

El presente institucional no ha sido producto del azar, sino que responde a una planificación intencionada, para desarrollarnos y responder adecuadamente a las demandas de una ciudadanía cada vez más exigente.

En este sentido, el trabajo en equipo pavimentó el camino del desarrollo actual, pues desde nuestros inicios nos hemos propuesto el adelantarnos a los cambios de la criminalidad.

La modernización constante de la Policía de Investigaciones no se detiene. Servir a la gente es lo que nos mueve, y nos reinventamos continuamente para brindar el mejor servicio, con un compromiso absoluto para con la sociedad, bajo las políticas y acciones propuestas por el gobierno y trabajo analítico y de campo coordinado con el Ministerio Público.

## PLANIFICACIÓN PARA CRECER

En los años 90, la PDI comenzó a trabajar en base a Planes Estratégicos, buscando estar a la altura de los crecientes desafíos de cada época en materia de seguridad. Hoy, en su sexto proceso consecutivo, denominado "Plan Estratégico de Desarrollo Policial (PEDP) 2023-2028", se afianza el objetivo de ser referentes en materia de investigación de delitos complejos y crimen organizado transnacional; prospectando escenarios criminales emergentes e impulsando la transformación digital, entre otros, todos ellos propios de una institución profesional, moderna y globalizada.

En esa línea de planificación, evolución y crecimiento institucional, la PDI ya en el año 2000 creó las primeras unidades especializadas en investigación de ciberdelitos, las que hoy ya son parte de una Jefatura Nacional de Ciberdelitos, desde donde ven con atención el aumento en delitos relativos a espionaje informático, irrupción de las criptomonedas, amenazas vía medios tecnológicos, así como el de adquisición, almacenamiento, producción, distribución y/o comercialización de material de abuso sexual infantil, donde la policía civil ha trabajado cohesionadamente -a nivel global- en las mega operaciones coordinadas por INTERPOL, denominadas Operaciones Orion I y II, que permitieron desbaratar una red de adquisición, almacenamiento, producción, distribución y/o comercialización de material de abuso sexual infantil.

**El concepto de crimen organizado transnacional se ha tomado la agenda en el último tiempo y la PDI sabe de ello, siendo un factor clave para desbaratar diversos grupos que han intentado operar en Chile**

El concepto de crimen organizado transnacional se ha tomado la agenda en el último tiempo y la PDI sabe de ello, siendo un factor clave para desbaratar diversos grupos que han intentado operar en Chile, como el "Tren de Aragua", "La Mafia del Norte", "Los Pulpos", "Los Gallegos" y "Bang de Fujian". Estos son ejemplos de investigaciones robustas y exitosas, que han desarticulado grupos criminales de carácter internacional, vinculados al tráfico de drogas, tráfico de armas, sicariatos, contrabando, lavado de activos y trata de personas. Todas han sido intervenidas, evitando que se asienten en nuestro territorio. Cada vez que afloren facciones de estas u otras estructuras, estaremos ahí para enfrentarlos, para esto nos hemos preparado durante 90 años.

## INNOVACIÓN Y COHESIÓN COMO EJE CENTRAL

El énfasis institucional para generar coproducción de seguridad para enfrentar delitos complejos y emergentes -de cierta manera figuras delictivas que han mutando- es incorporar nuevas dinámicas de análisis, complementadas con tecnologías, sumando fortalecer la cooperación y cohesión intra e inter institucional.

Ejemplo de ello es la creación del Centro Nacional de Análisis Criminal (Cenacrim), quien dirige técnicamente a las 27 Oficinas de Análisis Criminal (OFAN) de la PDI en el país, las cuales son las encargadas de almacenar, analizar, distribuir y generar conocimiento sobre fenómenos criminales, el cual luego es utilizado por las unidades operativas.

A su vez, orientaremos esfuerzos, en aumentar nuestra capacidad y oferta investigativa a nivel nacional, para debilitar estructuras criminales, desincentivando a través de la investigación patrimonial y lavado de activos, su enriquecimiento ilícito, fin último de una estructura criminal. Con ello, se busca aminorar su asentamiento, crecimiento y desarrollo, junto con determinar sus dinámicas delictivas bajo los ejes: "estructura organizativa, roles delictivos, rutas y métodos de ocultamiento" y desalentar sus operaciones y conexiones desde Chile a otras urbes del mundo.

Sumaremos mejoras en nuestros mecanismos de control corporativo, incorporando "compliance", para robustecer las políticas y procedimientos institucionales, garantizando un acabado y aplicado cumplimiento normativo, para minimizar riesgos y vulnerabilidades.

A su vez, el relacionamiento con cuerpos policiales del mundo es clave y extenso, siendo también parte de los desafíos del actual PEDP, donde su estrecha relación con organizaciones como INTERPOL, Euro-pol y Ameripol, no hacen más que destacar el buen pie en que se encuentra nuestra Policía Civil.

Hoy, cuando debemos responder a expresiones de una criminalidad más organizada y extremadamente compleja, una vez más, analizando el entorno criminal, de manera flexible, adaptativa e innovadora mejoramos nuestras capacidades, siendo vital incorporar tecnología, herramientas y logística necesaria para ello, complementando un despliegue cohesionado con otros actores gravitantes a nivel nacional en materia de seguridad. Agradezco y estoy orgulloso del compromiso de nuestro personal. Sé que contamos con los profesionales idóneos para enfrentar las nuevas dinámicas delictuales actuales y venideras, pues por 90 años ellos han sido los grandes responsables de nuestro crecimiento.

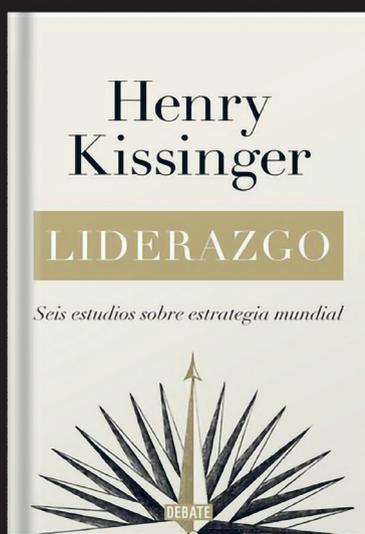




# reseña de libros

# “LIDERAZGO” DE HENRY KISSINGER

Por CATALINA SCHERPING



**H**enry Kissinger es probablemente uno de los políticos internacionales más influyentes de nuestros tiempos. Interviniendo en la escena internacional entre el siglo XX y XXI, la experiencia y bagaje histórico que posee lo hacen sin duda uno de los escritores más relevantes, cuando de Relaciones Internacionales hablamos. Su comprensión sobre el complejo entramado de vínculos que conforma el sistema internacional, lo han hecho un experto en la materia y esto queda demostrado en cada uno de sus escritos.

En su nuevo libro “Liderazgo”, Kissinger analiza a seis líderes internacionales que marcaron el rumbo de sus naciones en momentos críticos, definiendo así su futuro, y como él mismo lo diría; *“siendo artífices de la evolución de sus sociedades y del orden internacional durante la postguerra”*. Konrad Adenauer, Charles de Gaulle, Richard Nixon, Anwar Sadat, Lee Kuan Yew y Margaret Thatcher, fueron protagonistas en un mundo titubeante, en el cual lo que primaba era la resolución de conflictos mediante la vía armada. En base a este contexto, y en los escombros de lo que alguna vez fueron las naciones más estables y democráticas del mundo, estos líderes se replantearon la forma en cómo la humanidad manejaba sus asuntos.



**Catalina Scherping**, Socióloga de la Universidad de Valparaíso y Magíster en Relaciones Internacionales de la Pontificia Universidad Católica de Valparaíso. Durante su carrera se ha especializado en temáticas latinoamericanas. Actualmente se desempeña como consultora para diferentes Gobiernos Regionales en Chile en Temas de políticas públicas y descentralización.

De esta manera a lo largo de las 648 páginas que componen el libro, Kissinger inicialmente establece las características que para él definen a un líder y que justifican la elección de los seis políticos mencionados anteriormente. Es así que, un líder es aquel que piensa y actúa en la intersección de dos ejes; el pasado y el futuro, y entre los valores perdurables y las aspiraciones de aquellos lideran, en base a esto los líderes deben analizar realísticamente a sus sociedades, equilibrando su conocimiento con sus intuiciones sobre el futuro. Para enfrentar la tarea de liderar una nación, Kissinger indica la existencia de dos atributos vitales, estos son la valentía y el carácter; *la valentía para elegir una dirección entre diversas opciones complejas y difíciles, y la fuerza de carácter para mantener un curso de acción cuyos beneficios y peligros sólo se vislumbran de forma incompleta.*

Posterior a esta definición se repasa la historia personal y política de cada líder seleccionado, haciendo énfasis en las situaciones específicas y formativas, que contribuyeron a su toma de decisiones. Konrad Adenauer siendo el responsable de sacar a Alemania del momento más bajo de su historia, eliminando las aspiraciones de dominar Europa, reconstruyendo a la nación sobre una base moral que reflejaba sus propios valores cristianos y convicciones democráticas. Charles De Gaulle por su parte reconstruyó la estructura política de Francia en dos oportunidades (1944 y 1958) dando paso a un Estado nación estable y próspero bajo una constitución sólida. Richard Nixon, sacó a Estados Unidos de la Guerra de Vietnam y modificó las tensiones existentes entre las superpotencias durante la Guerra Fría. Anwar Sadat le devolvió la confianza a Egipto, como también los territorios perdidos y puso término al conflicto con Israel. Lee Kuan Yew convirtió a Singapur en una ciudad-Estado segura, bien administrada y próspera, entregándole una identidad nacional que unificó su diversidad cultural. Finalmente, Margaret Thatcher renovó a un alicaído Reino Unido mediante la reforma económica y una política exterior equilibrada entre la audacia y la prudencia.

Liderazgo, es una invitación para que el lector se adentre en cómo cada uno de estos políticos se fue forjando en el camino, analizando acontecimientos descritos de una manera tan única, como sólo Kissinger puede conseguir. Es un libro cuya audiencia puede estar enfocada tanto para interesados en Relaciones Internacionales, como también para una audiencia transversal.

\* Al cierre de esta publicación se dio a conocer el fallecimiento del político Henry Kissinger a la edad de 100 años.



# calendario de actividades



ACTIVIDAD	DESCRIPCIÓN	FECHA Y LUGAR
<p><b>Conferencia RC21 2024 PUC</b> <i>“Las políticas y los espacios de encuentro: avanzando en los diálogos entre y dentro del norte global y el sur global”.</i></p>	<p>La conferencia es una invitación a analizar conflictos sociopolíticos globales y locales intensos, tales como estallidos sociales, populismos, crisis económicas, crisis climáticas, y crisis humanitarias y sanitarias. Además, esperamos examinar cómo los procesos urbanos en el Norte Global y el Sur Global interactúan e influyen entre sí, centrándonos en las políticas y los espacios de encuentro. La conferencia busca abarcar variadas escalas (transnacional, nacional-regional, nivel de calle) y enfoques, abriendo espacio para diversas metodologías para la investigación empírica y corrientes de pensamiento (por ejemplo, desde ideas radicales hasta el pensamiento decolonial y feminista actual en estudios urbanos).</p> <p><b>Enlace:</b> <a href="https://estudiosurbanos.uc.cl/agenda/conferencia-rc21-2024-las-politicas-y-espacios-de-encuentro-avanzando-en-los-dialogos-entre-y-dentro-del-norte-global-y-el-sur-global/">https://estudiosurbanos.uc.cl/agenda/conferencia-rc21-2024-las-politicas-y-espacios-de-encuentro-avanzando-en-los-dialogos-entre-y-dentro-del-norte-global-y-el-sur-global/</a></p>	<p><b>24 al 26 de julio 2024,</b> Santiago de Chile, Chile.</p>
<p><b>ONU Cumbre del Futuro 2024: Soluciones multilaterales para un mañana mejor</b></p>	<p>La Cumbre del Futuro es una oportunidad única para mejorar la cooperación cuando hay retos críticos y subsanar las deficiencias en la gobernanza global, reafirmar los compromisos existentes, incluidos los Objetivos de Desarrollo Sostenible y la Carta de las Naciones Unidas, y avanzar hacia un sistema multilateral revitalizado que pueda influir positivamente en la vida de las personas. Basándose en la Cumbre sobre los ODS de 2023, los Estados Miembros estudiarán la manera de sentar las bases de una cooperación mundial más eficaz que pueda hacer frente a los retos actuales y a las nuevas amenazas de ahora en adelante.</p> <p><b>Enlace:</b> <a href="https://www.un.org/es/common-agenda/summit-of-the-future">https://www.un.org/es/common-agenda/summit-of-the-future</a></p>	<p><b>22 y 23 de septiembre 2024,</b> New York, Estados Unidos.</p>



