DF
DIARIO FINANCIERO®
SUPLEMENTO
SANTIAGO DE CHILE
MARTES 16 DE MAYO DE 2023

LAS OPORTUNIDADES DE LA INTELIGENCIA ARTIFICIAL EN LAS EMPRESAS LOCALES

A pesar de que el uso de este tipo de tecnología aún se encuentra en una etapa incipiente, ya hay industrias que han evolucionado en su implementación, lo que se espera se incremente en los próximos años.

POR ANDREA CAMPILLAY

A nivel mundial, según datos de McKinsey, la adopción de la inteligencia artificial (IA) actualmente es 2,5 veces más alta que en 2017 y se evidencia un número cada vez mayor de organizaciones que han integrado el uso de esta tecnología. Un escenario que se repite en Chile, donde el estudio Technology Vision 2022 de Accenture reveló que un 70% de las empresas afirma que ya la está utilizando en sus procesos. "Seguramente esto se irá acrecentando en los próximos años", dice Carolina Gainza, subsecretaria del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación, sobre la base de sus beneficios para las empresas chilenas y la sociedad, como la rapidez en el procesamiento de datos, la automatización de procesos, la proyección de escenarios futuros o la creación de nuevos productos y servicios, entre otros.

Así, la adopción de la IA ya muestra avances significativos en industrias como la salud, donde ha permitido la clasificación de pacientes, predecir enfermedades o analizar resultados desde exámenes, y ha apoyado en la toma de decisiones basadas en datos. En el ámbito financiero, en tanto, ha contribuido a la clasificación de clientes, la predicción para la oferta de productos comerciales, la evaluación de riesgos y el análisis de estados financieros y operaciones comerciales.

"A nivel transversal, la mejora en la experiencia de usuario y el marketing digital es uno de los usos de mayor relevancia, posibilitando una mejor comunicación y contacto con los usuarios finales, entregando información cada vez más certera y de valor de sus productos y servicios, respondiendo de una mejor forma a las necesidades del cliente", detalla Carlos Lobos, director del programa de Ciberseguridad de Capacitación Usach. A nivel público, por ejemplo, destaca el desarrollo de la Defensoría Penal Pública, cuya solución busca promover la incorporación de estándares de responsabilidad y justicia en algoritmos, IA y sistemas automatizados, mientras que Fonasa implementará una solución tecnológica para optimizar la fiscalización de fraudes. En tanto, el Instituto de Previsión Social (IPS) está desarrollando un algoritmo para identificar a quienes no han cobrado ayudas estatales a las que tienen derecho.

Sin embargo, el académico advierte que, a pesar de que muchas organizaciones desean implementar o se encuentran explorando formas de integrar la IA a sus operaciones, no es seguro que puedan realmente aprovechar o rentabilizar eficientemente estas iniciativas pues dependerá principalmente de cómo evolucionen las barreras de entrada al acceso y desarrollo sobre esta tecnología.

Proyecciones y desafíos

Si bien los expertos coinciden en que se espera una masificación del uso de la IA a nivel local, señalan que para que esto ocurra es necesario contar con un infraestructura tecnológica, acceso a datos de calidad, capacitación y formación, y avanzar en un marco regulatorio y ético. Por esto, la subsecretaria Gainza asegura que se encuentran trabajando en una actualización y profundización de la Política Nacional de IA. "La IA tiene un potencial innovador enorme para el país. Utilizar este potencial dependerá de la articulación entre el sector público y el privado", agrega.

Para Nicolás Vilela, cofundador y CEO de ZTZ Tech Group, el uso de esta tecnología "está inmiscuyéndose entre organizaciones y los consumidores", por lo que califica su uso como mandatorio. De esta manera, para aprovechar al máximo los beneficios "es importante que las empresas chilenas inviertan en la adquisición de habilidades y conocimientos en IA, establezcan alianzas estratégicas con proveedores de tecnología y fomenten una cultura de innovación y experimentación", concluye Cristián López, CEO de Unitti.

ZTZ TECH GROUP

ZTZ:

La start-up que revoluciona el mundo empresarial con inteligencia artificial

Con su software personalizado capaz de dar solución inmediata a reclamos regulatorios de las más diversas empresas, ZTZ ha conquistado a gigantes del retail. Y ahora, apunta más allá para consolidarse como referente en el campo de la IA.

En cinco años, ZTZ ha logrado posicionarse como una start-up de Inteligencia Artificial (IA) capaz de dar solución inmediata a reclamos regulatorios de las más diversas empresas, siendo grandes compañías como Mercado Libre, Uber, Starken, entre otras, las que ya han implementado el software para responder en minutos y con precisión a sus clientes.

ZTZ destaca por su capacidad de implementar la solución en dos semanas y customizar el programa en tan solo dos reuniones para adaptarse a las necesidades específicas, procesos y documentos de cada organización. Esto le ha permitido comprobar los importantes resultados obtenidos con sus clientes, convirtiéndose en un referente para Directorios y CEOs que buscan implementar la inteligencia artificial en sus organizaciones.

Nicolás Vilela, CEO de ZTZ, lidera este innovador proyecto que "ha logrado reducir los tiempos de respuesta de días a minutos, sin comprometer la precisión y tomando el control del proceso".

Pero el enfoque de ZTZ va más allá. Además de su destacado software, la empresa está incursionando en otros campos de la Inteligencia Artificial. Uno de ellos es el desafío de Legal Operations, "donde buscamos abordar la productividad y los indicadores que implica generar textos rápidos, así como tener indicadores en tiempo real. También estamos lanzando herramientas enfocadas en la navegación y gobernanza de grandes cantidades de información", agrega Nicolás Vilela.

Nicolás Vilela, CEO de ZTZ.

Para obtener más información sobre ZTZ y sus soluciones de inteligencia artificial, visita www.ztz.ai

PUBLIRREPORTAJE

OCTOPUSS:

Líder en Soluciones Tecnológicas con Inteligencia Artificial para el mundo que viene

Tali Haviv, senior business development de OCTOPUSS Chile.

Descubre cómo OCTOPUSS está revolucionando diferentes industrias con su enfoque único en seguridad y eficiencia, utilizando tecnologías basadas en Inteligencia Artificial.

OCTOPUSS, una empresa líder en proveer soluciones tecnológicas basadas en Inteligencia Artificial (IA), está transformando la manera en que las industrias abordan la seguridad y la eficiencia. Con casi 15 años en el mercado chileno, esta compañía se ha destacado por su compromiso con la innovación y su capacidad para ofrecer productos y servicios de vanguardia para diversos sectores.

La propuesta de valor de OCTOPUSS se enfoca en dos grandes áreas de productos o soluciones. Por una parte, en soluciones de seguridad, que incluyen sistemas de vigilancia digital, cámaras de seguridad, intrusión y alarmas. Por otro lado, ofrece soluciones orientadas a la inspección y eficiencia en distintos procesos. Con una amplia gama de soluciones en ambas áreas, OCTOPUSS es capaz de adaptarse a las necesidades específicas de cada industria a la que se dirige.

"Cuando hablamos de Inteligencia Artificial tenemos dos opciones. La primera es que empecemos a ser desarrolladores de AI, porque por ahí va el mundo; o bien, aprender verdaderamente cómo usar la Inteligencia Artificial y cómo aplicarla a nuestros clientes de una forma para que ellos sean más eficientes", señala Tali Haviv, senior business development de OCTOPUSS Chile.

La ejecutiva agrega que "hemos venido estudiando el impacto de la IA en nuestra industria durante varios años, y vemos cómo esta herramienta tecnológica está cambiando la forma en que trabajamos, ofreciendo numerosas oportunidades. Según las estadísticas, en los próximos 10 años se estima que se perderán mil millones de empleos debido a la automatización, pero también se generarán más de 350 millones de nuevas profesiones gracias a IA".

Hablando de industrias, OCTOPUSS se orienta hacia diversos sectores, entre ellos la minería, la industria forestal y muchos otros. Pero en todo caso, su oferta es transversal y puede ser aplicada en diferentes industrias y sectores.

En cuanto a la aplicación de la Inteligencia Artificial en la oferta de soluciones de OCTOPUSS, la compañía está lanzando dos líneas de negocios fuertes. "La primera es una herramienta de seguridad que llamamos 'el perrito', que es un robot que opera en ambientes peligrosos o complejos para los humanos, por ejemplo, en minería donde hay sectores tóxicos. Este robot puede escalar, subir, y moverse en sectores que implican un alto costo de recursos para las empresas. La otra línea de soluciones es más informática y dice relación con herramientas de inspección, por ejemplo, de escáner de stock para diversas industrias", comenta la ejecutiva.

Pero, ¿cuál es la inspiración del nombre de la empresa? OCTOPUSS, que en español significa "pulpo", "refleja la naturaleza versátil y adaptable de la compañía. Al igual que un pulpo, OCTOPUSS tiene la capacidad de abarcar múltiples áreas y soluciones, es como la IA, ocho manos, puede abarcar diferentes tareas, cosa que el humano no puede hacer", concluye Tali Haviv.

www.octopuss.cl

OTROS MUNDOS POSIBLES: LOS RIESGOS QUE VIENEN CON EL AUGE DE LA IA

Herramientas como ChatGPT están ayudando a la optimización de generación de contenido para esparcir fake news y hasta enviar mails de phishing más sofisticados. Pero hay formas de resguardarse. Los expertos explican cómo. POR AIRAM FERNÁNDEZ

Los 100 millones de usuarios que alcanzó ChatGPT solo dos meses después de su lanzamiento, según un estudio de la firma UBS, dan cuenta del furor que genera este modelo capaz de entender y generar textos cargados de naturalidad -aunque no libres de errores- usando técnicas de lenguaje de máquina y aprendizaje automático. Pero a la par de abrir un mundo nuevo de oportunidades, se abren otros mundos posibles para la creación de ataques cibernéticos más sofisticados, a partir del mismo uso que podría darle una persona común. Es decir, un ciberatacante consultando a la inteligencia para que le ayude en sus procesos.

Cómo construir un artefacto explosivo o realizar un código malicioso son dos cosas que la IA no puede responder, al menos si se le pregunta directamente de esa forma, dice Miguel Caruso, Head of Research and Development de Ubiquo Latam. El experto explica que fue una precaución que tomaron los creadores de la firma OpenAI. Pero advierte que hay que tener cuidado porque ya existen diferentes técnicas para burlar a la inteligencia y que entregue la información.

Lo que sí puede hacer sin muchos rodeos o intentos, y que preocupa a los expertos en general, es ayudar a redactar mensajes que pueden usar los ciberdelincuentes para perfeccionar métodos de estafa o suplantación de identidad, dada su capacidad de "conversar" tan naturalmente.

"Con esta nueva modalidad de chatbot hasta el menos creativo de los ciberatacantes puede crear un texto para poder realizar un phishing", añade Caruso.

Coincide Sol González, investigadora de Seguridad Informática de ESET Latinoamérica, mientras recuerda que años atrás era mucho más sencillo detectarlos, ya que la redacción de estos correos maliciosos era "simplemente absurda", incluso con faltas ortográficas.

Para Hermes Romero, director para Centro, Sudamérica y Caribe de Tenable, es posible que cualquier IA proporcione herramientas a los atacantes para producir correos electrónicos de phishing "más convincentes", entrenando a los modelos para que utilicen un lenguaje específico que "puede extraerse de sitios web, comunicados de prensa o cuentas en redes sociales de una organización objetivo".

Alejandro Martínez, CTO de JAG Cybersecurity, pone un ejemplo: "Imaginemos un delincuente pidiendo a ChatGPT que le genere un diálogo que será usado en Roblox (plataforma de juegos infantiles), usando modismos e íconos para engañar a un menor y lograr sacarle información o llevarlo a su terreno en el plano físico. Esto es realmente serio", advierte.

Martínez añade que este tipo de herramientas también pueden ser utilizadas para el desarrollo de exploits y descubrimiento de vulnerabilidades zero-day. Es decir, que los atacantes "pueden encontrar y explotar nuevas debilidades en sistemas y aplicaciones sin que los desarrolladores hayan tenido tiempo para solucionarlas".

> US$ **10** MIL MILLONES PREVÉ JUNIPER RESEARCH QUE GASTARÁN LAS COMPAÑÍAS EN SOLUCIONES PARA LA PREVENCIÓN Y DETECCIÓN DEL FRAUDE FINANCIERO MEDIANTE IA.

A este abanico de riesgos, la experta de ESET Latinoamérica añade otros, como la generación de fake news, para redactar noticias falsas y distribuirlas a lo largo de Internet, robo de identidad y desarrollo de malware, para la generación de código en diversos lenguajes de programación.

Los resguardos

Por más lógico que parezca, lo primero que sugiere Hermes Romero es desconfiar y prestar atención a esas señales que un humano puede reconocer, como una solicitud extraña con un alto sentido de urgencia o requerimientos de datos que no son comunes, como alguien que te pida que le envíes tu contraseña de correo electrónico. Además, dice que utilizar más de un factor de verificación es clave en estos tiempos. "Aquí, la aplicación del concepto de Zero Trust es de gran valor, desde el uso personal hasta el profesional", añade.

Alejandro Martínez insiste en que las empresas, los profesionales de TI, OT y ciberseguridad deben comprender que los planes y acciones aisladas ya no funcionan: "Hay que tener una estrategia de defensa en capas, que se solapen unas a otras, para hacerles el trabajo difícil a los delincuentes, y entender que no hay forma de evitar que ingresen a nuestros sistemas, porque si lo quieren hacer lo van a hacer. La pregunta es ¿será fácil?", plantea.

Como la IA no es exacta, invertir tiempo en su entrenamiento, validación y evaluación es una buena estrategia, sugiere Carlos Lobos, director del programa de Ciberseguridad de Capacitación Usach, quien cree que uno de los principales desafíos que hoy tienen las empresas es justamente el desarrollo de competencias en IA por parte de sus especialistas. Como todos los expertos, no duda que la tecnología está generando importantes beneficios, pero dice que el no comprender los riesgos de su adopción significa que procesos clave de las organizaciones que empleen IA pueden ser vulnerados: "No solo se trata de problemas de ciberseguridad. Las brechas de seguridad y vulnerabilidades a las cuales pueden estar expuestas las organizaciones pueden ser muy significativas, y los cibercriminales están observando y esperando el momento de poder aprovecharlas".

GRUPO DF
DF · DF LIVE · DE MAS · ED · BAZARED

Director: José Tomás Santa María / **Subdirectora:** Paula Vargas / **Gerente Comercial:** José Ignacio De la Cuadra / **Editora:** Claudia Marín / **Director Creativo y Arte:** Rodrigo Aguayo
Coordinadora: Marcia Aguilar / **Dirección** Edificio Fundadores, Badajoz 45, piso 10, Las Condes, Fono: 23391000 / e-mail: buzondf@df.cl / **Impreso por** COPESA IMPRESORES S.A., que sólo actúa como impresor.

EL PANORAMA QUE ENFRENTAN LAS EMPRESAS ANTE LA SOFISTICACIÓN DE AMENAZAS

Las vulnerabilidades que surgen con las nuevas formas de trabajo son los ejes que están llamando la atención de los ciberdelincuentes. Así, se están multiplicando cada vez más los ataques de malware. POR PAULINA SANTIBÁÑEZ T.

Así como las empresas han cambiado sus modelos de trabajo y negocios gracias a la adopción tecnológica, los ciberdelincuentes han adaptado sus herramientas para sofisticar sus amenazas y modelos.

Según el Informe de Ciberamenazas 2023 de SonicWall, pese a que los ataques de ransomware cayeron un 21% en todo el mundo, 2022 sigue siendo el año con la segunda mayor cantidad registrada de intentos de este tipo a nivel mundial. El malware, por su parte, tuvo un aumento del 87% en la cantidad de ataques en IoT y una cifra récord (43%) de ataques de cryptojacking.

Esto estaría marcando una tendencia y "un cambio estratégico", analiza Rodrigo Albagli, managing partner de Albagli Zaliasnik. "En 2023 estaremos viendo un crecimiento del malware, sobre todo de IoT. Los ataques están en constante evolución, por eso las empresas deben adelantarse al adversario", plantea, mientras advierte la relevancia de que las empresas sean más ágiles respecto al cambio de objetivos y nuevas herramientas que están teniendo los ciberdelincuentes.

Coincide Iván Toro, CEO de ITQ Latam, al sugerir que este contexto cambiante está marcado por el mejoramiento de las técnicas de ataque de los delincuentes, como "los software que utilizan para robar datos e información, los cuales muchas veces no son detectados por las víctimas".

Interconectividad y protección

Para el C-CISO y director de Seguridad de la Información para América Latina en TCS, Gabriel Croci, hoy nos enfrentamos a "una interconectividad sin precedentes", donde la protección de datos ha pasado a ser el objetivo a defender y cobra mayor sentido en los tiempos actuales: "Las nuevas formas de trabajar hacen que sea crítico contar con socios estratégicos que apoyen a las organizaciones para estar protegidas frente a las ciber amenazas".

En ese sentido, Croci aconseja la combinación de soluciones técnicas, y destaca la implementación de medidas de seguridad como IAM (Gestión de Identificación y Autentificación) tanto en la red local como en la nube, además de controles de seguridad híbridos.

Por su parte, Iván Toro resalta la importancia del rol de la educación en ciberseguridad, junto al monitoreo permanente de amenazas, la detección de vulnerabilidades, así como políticas y protocolos, "tanto técnicos como sociales".

OPINIÓN

Vulnerabilidades conocidas detrás del 77% de los incidentes de ciberseguridad

Por Hermes Romero
Director para Centro, Sudamérica y Caribe de Tenable

Los Zero Days, amenaza o ataque de Día Cero, se han convertido en el gran temor cuando hablamos de ciberseguridad, ya que estos fallos, desconocidos para el mercado general, aún no tienen una solución de seguridad. A primera vista, esto se presenta como algo alarmante, sin embargo, de acuerdo con un informe realizado por Tenable, los ataques de Zero Day representan solamente un 7.5% de los identificados el último año.

Ahora bien, hablemos de lo verdaderamente alarmante, que son las vulnerabilidades conocidas. Estas son aquellas que se descubren y para las que ya hay un parche, es decir una solución que remedia esa puerta de entrada de los cibercriminales. Este tipo de vulnerabilidades se han convertido en una de las prácticas más rentables para los cibercriminales. De hecho, en 2022, el mencionado estudio de Tenable muestra que el 77% de los ataques fueron con vulnerabilidades conocidas, algunas incluso del 2017.

Habiendo pintado esta realidad, es fundamental poner el tema sobre la mesa y es que la solución no es buscar Zero Days y atacarlas, que por cierto el generar este tipo de nuevas vulnerabilidades a veces es una estrategia de los atacantes para distraer de lo verdaderamente importante, es decir, las vulnerabilidades conocidas. La verdadera solución al problema es corregir las vulnerabilidades conocidas que son sin duda las que más impacto pueden tener.

Seguramente cuando llegues a este punto en tu lectura te preguntarás, ¿pero si ya son vulnerabilidades conocidas por qué no se resuelven? No es tan sencillo como parece y es que los cibercriminales consiguen explotar con frecuencia este tipo de vulnerabilidades, que previamente fueron reportadas y solventadas por el desarrollador del software, pero que aún no se han arreglado por distintas razones. Fácil sería culpar a las organizaciones de no priorizar la corrección de vulnerabilidades. La realidad es que el promedio de organizaciones utiliza más de 130 soluciones de ciberseguridad, pero esta amplia variedad de herramientas y sistemas actúan aislados en silos y no ayuda a reducir el riesgo. Los equipos de seguridad se enfrentan al reto de mantenerse al día con la constante afluencia de datos procedentes de múltiples soluciones y de analizar eficazmente todos esos datos para tomar decisiones informadas y proactivas sobre qué exposiciones suponen el mayor riesgo para la organización.

Dicho todo lo anterior, es muy claro que debemos evolucionar nuestra estrategia de ciberseguridad. Hoy debemos hablar de gestión de exposición y no de remediación de una u otra vulnerabilidad. Gestionar la exposición de una organización implica tener una visión holística y constante de las vulnerabilidades con una mentalidad y visión estratégica sobre la priorización de vulnerabilidades. Esto marcará la diferencia entre tener a un arquero salvando goles a un estratega que busca salvaguardar la continuidad del negocio, y especialmente en América Latina, que en el informe es enlistado como la región con mayor volumen de datos expuestos en el mundo.

En conclusión, vivimos en una superficie de ataque moderna donde las vulnerabilidades crecen tan rápido como las innovaciones en el mundo digital. Es fundamental ver la fotografía completa y evaluar antes de tomar una decisión sobre qué parchar, utilizando herramientas que validen dónde están los puntos de atención, para que puedan ser resueltos de forma proactiva, reduciendo el riesgo de la organización. Últimamente, todo el mundo está esperando el próximo "fin del mundo digital", cuando en realidad lo que más nos afecta está presente: son las vulnerabilidades conocidas que siguen sin corregirse.

CULTURA DE CIBERSEGURIDAD: LA CLAVE PARA UNA PROTECCIÓN EFECTIVA

Aplicar programas de concientización en seguridad, simulaciones de ataques y ejercicios de respuesta a incidentes son parte de las tareas que las compañías deben desarrollar para preparar a sus colaboradores y hacer frente a las amenazas.

POR PAULINA SANTIBÁÑEZ T.

Para los expertos, no hay un sector en específico de una organización que esté más expuesto a un ciberataque que otra, porque una vulnerabilidad podría generarse en diversas áreas. Sin embargo, sí hay coincidencia en que serían los colaboradores los más vulnerables a amenazas como el phishing, esto debido "a que están más expuestos, muchas veces por su falta de conocimiento en prevención y respuesta", explica Rodrigo Albagli, managing partner de Albagli Zaliasnik.

De hecho Gabriel Croci, C-CISO y director de Seguridad de la Información para América Latina en TCS, puntualiza que los ataques de "ingeniería social" buscan y aprovechan el error humano. Para poder defenderse, dice, es clave la necesidad de "una sólida gestión de la capacitación interna", y hace hincapié en considerar también a los proveedores como una extensión en esta tarea, ya que no siempre "les dan el mismo tipo de cuidado que se tiene hacia adentro de la empresa". Y es que, para asegurar una protección efectiva, la alineación del capital humano es esencial.

El eslabón débil

Para lograr tener una organización con sus diversas cadenas alineadas, Marcelo Díaz, socio de Cyber Risk Deloitte, dice que es clave aplicar programas de concientización en seguridad, simulaciones de ataques y ejercicios de respuesta a incidentes.

"Hay que recordar que las personas son el eslabón más débil. Se debe fomentar, entonces, una mentalidad proactiva en la identificación y respuesta a posibles ataques, así como fomentar la colaboración y el intercambio de información entre empresas, organizaciones y gobiernos", añade Díaz.

En ese sentido, Albagli destaca la práctica de fomentar los mecanismos de prueba: "El envío de mails imitando ataques phishing es, por ejemplo, una buena medida para capacitar a las personas".

También es relevante establecer políticas de seguridad en las cuales toda la organización esté involucrada, como Zero Trust, "un marco basado en el principio de 'nunca confíes, siempre verifica', aplicado no solo a los humanos sino también a las máquinas y sus procesos", dice Croci.

Para que estas políticas funcionen, el ejecutivo de TCS puntualiza que las compañías deben potenciar estrategias integrales de ciberseguridad que incluyan evaluaciones periódicas, formación de empleados y capacidades de detección, monitoreo y respuesta, siendo "primordial que las organizaciones inviertan en ciberseguridad para prevenir amenazas y adelantarse a los ciberatacantes".

PUBLIRREPORTAJE

Desafíos de la Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información

A paso sostenido avanza la tramitación de la Ley que posibilitará establecer la gobernanza de la ciberseguridad a nivel nacional. Importantes desafíos plantea la adopción de esta nueva normativa, que entre otras cosas define: los principios rectores en la materia, la forma de determinar y los requisitos para las organizaciones y servicios que formarán parte de infraestructura crítica de la información del país, tanto públicos como privados, la creación y articulación de la Agencia Nacional de Ciberseguridad, el CSIRT Nacional, CSIRT sectoriales y CSIRT de Gobierno.

La Ley Marco sobre Ciberseguridad e Infraestructura Crítica de la Información avanza a paso firme en el Congreso. El cuerpo legal en trámite, establece en primer término las disposiciones generales de la Ley, definiciones base y los principios rectores mínimos, tales como el principio de responsabilidad, de protección integral, de confidencialidad de los sistemas de información, de integridad de los sistemas informáticos y de la información, de disponibilidad de los sistemas de información, control de daños, de cooperación con la autoridad, y por último, el principio de especialidad en la sanción.

En el artículo 4° se establece una de las principales definiciones de la Ley, la cual es la determinación de la Infraestructura Crítica de la Información, siendo el Consejo Técnico de la Agencia Nacional de Ciberseguridad quien cada dos años detalle cuáles son los sectores o instituciones que serán calificados como críticos, estableciendo una serie de parámetros mínimos para su calificación, agregando que se entenderá que todos los órganos del Estado son parte de la Infraestructura Crítica de la Información. Carlos Lobos de Medina, Director del Programa de Ciberseguridad de Capacitación USACH, señala: "Es una interrogante la forma específica de definición de estos sectores o instituciones, se espera este muy en línea con lo que se entiende como infraestructura crítica a nivel internacional, siendo una muy buena jugada separarla de la Ley de Infraestructura Crítica, dado que esta se estaba politizando en demasía y podría retrasar esta Ley. Que todos los organismos del Estado sean parte de la Infraestructura Crítica de la Información sin duda que es un gran acierto".

En los artículos 5° y 6° se establecen los deberes generales y específicos de quienes formarán parte de la Infraestructura Crítica de la Información, donde básicamente se plantea la implementación de un Sistema de Gestión de Riesgo, el cual posibilite el tratamiento de estos, junto con la implementación de planes de continuidad operacional y de ciberseguridad, el desarrollo de ejercicios de ciberdefensa y ciberataque coordinados con el CSIRT sectorial o gubernamental según corresponda, la gestión de incidentes y la certificación de los sistemas de gestión y procesos. Al respecto, el profesor Lobos señala: "Son elementos mínimos de desarrollo, es una excelente opción que estén las definiciones articuladas a un Sistema de Gestión de Riesgos, en dicho ámbito es muy destacable en la Ley la certificación de estos sistemas y procesos. Básicamente existen dos opciones: avanzar hacia la certificación de marcos conocidos como ISO 27001 o NIST, siendo el primero el único que posee un esquema de certificación definido y formalizado en la actualidad; o bien desarrollar un propio esquema nacional de certificación, basado en los requisitos que se establezcan, tal como lo es el caso de España".

La creación de la Agencia Nacional de Ciberseguridad sin duda que es unos de los mayores logros de esta Ley, la cual adicionalmente se articula con el CSIRT Nacional, el CSIRT de Gobierno y los CSIRT sectoriales. En dicho ámbito el profesor Lobos sostiene que "la Ley es bastante clara en la definición de los diversos entes y la articulación de estos, es un gran paso en la gobernanza de la ciberseguridad, los roles están muy claros y definidos. Sin embargo, es clave que para la formalización de la institucionalidad se cuente con muy buenas definiciones de roles y funciones, así como las diversas interacciones y comunicación con los que serán regulados, de manera que no se solapen en su quehacer ni generen burocracia innecesaria".

La Agencia enfrentará el desafío de establecer las normas técnicas y estándares de ciberseguridad a quienes sean parte de la Infraestructura Crítica de la Información, así como desarrollar y fortalecer la formación, investigación, el fomento y difusión para el desarrollo de una cultura de la ciberseguridad a nivel nacional, desde la perspectiva de la ciberdefensa, la colaboración y coordinación con organismos de inteligencia para enfrentar amenazas que puedan afectar a la Infraestructura Crítica de la Información, estableciendo además el rol de fiscalización y sanciones aplicables. En base a lo anterior el profesor Lobos señala que "se esperaría que la Agencia se transforme en un agente catalizador de iniciativas en diversos ámbitos, la colaboración es clave en el ámbito de la ciberseguridad no solo en lo operacional, sino que a nivel de formación, concientización, investigación y desarrollo. Sería muy importante que no solo se articule con el Ministerio de Ciencias y Tecnologías, la articulación con CORFO, el Ministerio de Educación, Ministerio de Economía, entre otros, resultan fundamental para el desarrollo de Capital Humano Avanzado y fortalecer la industria de la ciberseguridad, así como más apoyo en el emprendimiento e innovación con base científico tecnológica".

Por último, el profesor Lobos hace algunas reflexiones generales en torno a la Ley: "Plantea muchos desafíos su implementación a nivel gubernamental, es un excelente avance que nos acerca a las mejores prácticas internacionales, la definición de la Infraestructura Crítica de la Información y que en ellas estén considerados los órganos del Estado es de altísimo valor, al igual que se piense en la implementación de Sistemas de Gestión de Riesgos, los cuales sean certificados. En general quienes trabajamos en ciberseguridad estamos muy esperanzados con su promulgación y que prontamente se comience a trabajar con ella, lo que involucra un importante desafío para las organizaciones públicas y privadas que son parte de la Infraestructura Crítica de la Información en la formación de su capital humano y en la adopción de Sistemas de Gestión con miras a una certificación".