CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS
Investigación, Tendencia y Concientización

Vol. Nº 3
Septiembre/2020
www.csirt.gob.cl

EMPRENDEDORES Y DESARROLLOS INNOVADORES EN CIBERSEGURIDAD

No sólo se trata de buenas ideas

Cooperación Internacional
CCN-CERT

Tendencia Digital
CREATIVIDAD PARA GESTIONAR LA CIBERSEGURIDAD

Comunidad Hackers
Ciberseguridad y Criptografía desde la Universidad de Chile

Legal
Emprendedores ojo con su propiedad intelectual

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT es el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile. Su misión es reducir los riesgos de la ciberseguridad en las redes del Gobierno de Chile, asesorando a las diferentes organizaciones que lo componen, actuando como socio estratégico en la defensa de las amenazas y colaborando para brindar mayor seguridad y robustez a las infraestructuras del Estado.

Cómo lo **hacemos?**

Contamos con un equipo multidisciplinario de profesionales y las tecnologías para proveer de asistencia técnica y logística a nuestros beneficiarios, así como prevenir la explotación de vulnerabilidades y actuar oportunamente frente a amenazas y ciberataques.

- MONITOREO DE LAS PLATAFORMAS DE INTERNET DE ORGANISMOS PÚBLICOS Y PRIVADOS **24/7**
- INVESTIGACIÓN Y CAPACITACIÓN PARA ENFRENTAR LAS AMENAZAS DEL FUTURO
- DETECCIÓN DE VULNERABILIDADES DE SITIOS Y SISTEMAS WEB DEL ESTADO
- GESTIÓN DE INCIDENTES Y DIFUSIÓN DE MEDIDAS PREVENTIVAS
- INCORPORACIÓN DE NUEVAS TECNOLOGÍAS Y HERRAMIENTAS DE SEGURIDAD INFORMÁTICA
- MEJORA CONTINUA DE LOS ESTÁNDARES DE CIBERSEGURIDAD DEL PAÍS

Alianza del Pacífico · FIRST · CSIRTamericas.org · MERIDIAN Connecting and Protecting

ÍNDICE

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

cibersucesos@interior.gob.cl

Director: Carlos Landeros Cartes
Jefa de contenidos y edición:
Katherina Canales Madrid

Colaboradores equipo CSIRT:
Carolina Covarrubias
Cristobal Hammersley
Patricio Quezada

Diseño y diagramación: black-book.cl

EDITORIAL

Carlos Landeros Cartes
Director Nacional
CSIRT de Gobierno

Entre enero y junio de este año, Chile tuvo 525 millones de intentos de ciberataque. Esta cifra refleja la realidad que se viene experimentado desde hace unos años en Chile y en el mundo. Hoy, en donde la crisis sanitaria aceleró el proceso de digitalización, se hace aún más necesario adoptar nuevas tecnologías que consideren la seguridad como un elemento fundamental para proteger los datos e información de las instituciones y organizaciones.

Pero no toda la tecnología requerida debe ser extranjera. Actualmente en Chile contamos con soluciones de ciberseguridad, creadas por chilenos, de grandes características técnicas y muy competitivas internacionalmente. Pyxsoft, Camel y Global Secure son algunos de estos emprendimientos, los que de alguna manera ofrecen soluciones a las diferentes necesidades que existen en el mundo de la ciberseguridad.

Pyxsoft es un programa que monitorea el tráfico de red y busca patrones anormales de comportamiento dentro de los servidores, almacenando y centralizando la información en una base de datos que se alimenta gracias a todos sus clientes. Por otra parte, Camel creó un producto que correlaciona las tecnologías y las adapta a las necesidades del negocio. Este software analiza los componentes del riesgo y cruza con la infraestructura del cliente. Finalmente, Global Secure, a través de la consultoría y su área de formación entregan herramientas para formar y capacitar profesionales en el área de la ciberseguridad.

Y así como existen estas alternativas de protección y educación, también vemos cómo el rol de los centros educativos es cada vez más esencial para el desarrollo de la industria. Un ejemplo de ello es CLCERT de la Universidad de Chile. En esta revista conocerán la experiencia de esta entidad en sus principales líneas de trabajo, relacionadas con la ciberseguridad.

Además, abordaremos un tema relacionado con el emprendimiento: la protección de la propiedad intelectual. Registrar el nombre de una empresa es fundamental para asegurar el derecho a utilizarla y evitar que otros usen signos similares a la marca registrada. Cómo se realiza este proceso y qué considerar a la hora de realizar este registro, les contaremos en esta edición.

Finalmente, en la sección internacional invitamos a participar al CCN CERT de España, quienes comparten el trabajo realizado junto con el sector privado para fortalecer la ciberseguridad en ese páis, desarrollando más de 22 soluciones, entre ellas, auditoría, detección, análisis, entre otros.

Esperamos que esta nueva edición de Cibersucesos sea de su interés, que conozcan a nuestros emprendedores en ciberseguridad, pero sobre todo, que nos llevemos la tarea y el deber de apoyarlos y seguir estimulando el desarrollo de nuevas tecnologías de ciberseguridad en Chile.

EMPRENDEDORES Y DESARROLLOS INNOVADORES EN CIBERSEGURIDAD

No sólo se trata de buenas ideas

Innovar y emprender en ciberseguridad implica complejos desafíos, pero también, grandes satisfacciones. Esa es la postura con la que enfrentan sus desarrollos y gestiones las personas que fueron entrevistadas en este reportaje. Ellos no solo produjeron soluciones en un mercado en el que existía una necesidad, en ese esfuerzo también se la jugaron por mover un poco más allá el horizonte de lo conocido.

REINVENTARSE Y SURGIR EN **MEDIO DE LA CRISIS**

Manuel Moreno,
fundador Global Secure

Manuel Moreno sufrió las consecuencias de una crisis económica que tuvo lugar en el hemisferio norte de América. La crisis subprime que azotó a los Estados Unidos lo dejó en una situación difícil. Pero supo reinventarse rápidamente y aprovechar su experiencia adquirida en ciberseguridad en la empresa en la que había trabajado por varios años y decidió emprender en el rubro de la consultoría. Fue así como fundó Global Secure.

Esta empresa cuenta con dos áreas de consultoría bien especializadas. Una de ellas consiste en servicios de CiberSeguridad Ofensivos y de Defensa. "Nos dedicamos a hacer temas técnicos duros principalmente desde ethical Hacking a la banca y a grandes compañías hasta responder a incidentes de ciberseguridad en empresas financieras y grandes corporaciones. Para esto, utilizamos, por una parte, la metodología que se usa tradicionalmente en la industria como OSSTMM y OWASP. Sin embargo, al ser una compañía con más de 13 años de experiencia, sumamos nuestra experiencia y creamos nuestra propia metodología y forma de operar con los clientes", explica su fundador.

Durante estos años, ya han confiado en Global Secure más de 150 empresas. El grupo, compuesto por un equipo multidisciplinario, a diferencia del mercado entrega pruebas de concepto (PoC) donde le muestran a los clientes cómo validar la vulnerabilidad encontrada y se les entrega el código para ejecutarlo si es necesario.

La segunda área que desarrolló Global Secure el año 2013 está relacionada con la educación en ciberseguridad. "La academia nació a raíz de una solicitud del Estado Mayor Conjunto (ECMO). Fue entonces cuando crearon un modelo que dio buenos resultados y se convirtió en un excelente producto replicable en todos lados. Desde ahí que no hemos parado", asegura Manuel.

Con alumnos en más de 15 países, hoy Global Secure está preparando su arribo al mercado de Estados Unidos para el año 2021 y ya registró GLOBALSECURE LLC en Delaware para comenzar este proceso. Lo que diferencia a esta empresa de la competencia es que "nuestro enfoque es 90% práctico y 10% teórico, enfocándonos en traspasar las habilidades a nuestros alumnos en un campo real de trabajo, similar a los entrenamientos que hacemos para nuestro propio equipo técnico cuando están comenzando", explica Manuel.

Los cursos, dirigidos a profesionales con experiencia laboral y que desean iniciar una carrera profesional en ciberseguridad, pueden ser de defensa (Blue Team) u ofensiva (Red Team). Además, cuentan con ocho cursos de distintas áreas: Auditoria, Hacking Ético, Pentest Web, Forense, Hacking a Sistemas Industriales y otros.

"La mayoría de nuestros entrenamientos son en modalidad Bootcamp de 40 a 45 horas promedio, con una duración de más de tres meses de laboratorios 100% prácticos con ambientes de servidores reales vulnerables donde los alumnos pueden practicar y romper sistemas de forma segura", cuenta Manuel, quien agrega: "Tenemos cuatro niveles. En los niveles 1 y 2, los exámenes de certificación son teóricos, mientras que los exámenes de certificación en los niveles 3 y 4 son totalmente prácticos, y van desde las 48 horas de examen para el curso GPPT (Professional Penetration Tester) y Web Penetration Tester hasta 14 días para el examen de investigador forense GCFI (Computer Forensic Investigator). En este tipo de pruebas, se le entrega al alumno un caso real con cadena de custodia para que realice un peritaje real y decida si el sospechoso es culpable o inocente del crimen que se le está imputando, en base a un informe que debe ser válido en la corte".

Para conocer más sobre Global Secure y sus productos puedes ingresar a **https://www.globalsecure.academy**

Ximena Valderrama y
Pablo Lagos, fundadores de Pyxsoft

INNOVAR A PARTIR DE UNA **NECESIDAD DEL MERCADO**

Ximena y Pablo son apasionados por la ciberseguridad, lo que los ha llevado a desarrollar diversos programas tecnológicos. Uno de ellos es Pyxsoft, un anti malware que monitorea el tráfico de red y busca patrones anormales de comportamiento dentro de los servidores y que es reconocido internacionalmente.

Pero la historia de estos emprendedores parte en el año 2014, cuando Ximena Valderrama y Pablo Lagos decidieron crear su propia empresa de web hosting. Si bien este emprendimiento dio muy buenos frutos, tenían un gran problema: frecuentemente eran hackeados, lo que significaba que perdían clientes y tiempo. Aburridos de esto, Pablo decidió crear un programa anti hacker, el cual resultó muy efectivo y, desde ese momento, nunca más fueron atacados.

Al obtener buenos resultados, esta pareja ofreció a otras empresas de hosting el programa a un buen precio y, sin imaginarlo, tuvieron una buena acogida por parte del mercado. Fue entonces, cuando el año 2016 decidieron regalar la empresa inicial y dedicarse a tiempo completo a este nuevo negocio al que llamaron Pyxsoft.

Este programa monitorea el tráfico de red y busca patrones anormales de comportamiento dentro de los servidores. A través de un algoritmo, el software se anticipa al hacker e intuitivamente identifica si esa dirección IP está catalogada como maliciosa o no, y lo bloquea. Esto permite almacenar y centralizar la información en una base de datos que se alimenta gracias a todos sus clientes. Es así como por ejemplo, hasta la fecha tienen más de 100 mil malware identificados a nivel mundial.

"Pyxsoft es una compañía chilena que cuenta con tecnología de punta y la gran diferencia que tiene con otras empresas de seguridad es su capacidad investigativa, tenemos una base de datos muy robusta, por lo que entregamos 100% de protección. Hasta la fecha, nunca hemos sido hackeados", cuenta Ximena.
Los excelentes resultados que han tenido, tanto grandes como pequeñas empresas, con Pyxsoft han llevado a este emprendimiento chileno a tener 600 clientes no sólo en nuestro país, sino también en Singapour, Alemania y España.

Debido a las diversas necesidades que tienen las empresas, Pyxsoft ofrece otro tipo de soluciones como el CDN, una red de distribución de contenidos que mejora la velocidad de los sitios web y le aporta ciberseguridad a la vez, es ideal para el e-commerce y retail.

Un segundo producto es POWERWAF que protege contra ataques de DDoS, OWASP, robo de datos top 10, entre otros. Además, tiene la capacidad de hacer balanceo de carga para configuraciones mono y multicloud; control y bloqueo de bots y optimiza sitios web.

Junto con brindar protección a las distintas plataformas web, este programa entrega un reporte en tiempo real del comportamiento del tráfico. "Nosotros le entregamos al cliente un sistema donde puede ver la información sobre la actividad que tiene su sitio y, en caso que ocurra un ciberataque, un registro de ataques", explica la fundadora.

Para los creadores de este programa es un orgullo ser una de las empresas chilenas en contar con tecnología propia y haber sido pioneros en el desarrollo de un producto único, el que hoy no sólo les ha dado grandes satisfacciones en Chile, sino también en otras partes del mundo.

Para conocer más sobre Pyxsoft y sus productos
puedes ingresar a **https://www.pyxsoft.com/**

PONER EL FOCO EN LAS **NECESIDADES DEL CLIENTE**

Fabián Rodríguez y Luis Montenegro, fundadores de Camel Secure

Es un hecho que las tecnológicas de seguridad que se consumen en todas las sociedades provienen de múltiples fuentes. No existe un mercado que pueda proveer de todas las soluciones, ni un solo proveedor que las pueda ofrecer.

El problema de fondo, es que los sistemas están compuestos de una suma de productos, los que están obligados a comunicarse. Si fuera un traje, probablemente tendríamos mangas y hombros disparejos, texturas distintas y un sinfín de irregularidades. La mayoría no vestiría un traje así, pero cuando se trata de tecnología, nos resignamos a aceptar esa realidad, y tenemos que adaptar el negocio a la oferta tecnológica.

Pero todas las sociedades tienen excepciones. Los emprendedores detrás de Camel desafiaron el paradigma y crearon una solución que correlaciona las tecnologías y las adapta a las necesidades del negocio. Siguiendo la analogía, ellos son verdaderos sastres de la ciberseguridad, que ajustan las soluciones a la medida del cliente.

A diferencia del mercado, Camel permite interactuar y correlacionar el ecosistema de seguridad del cliente y darle una visión más cercana al negocio, muy distinto a la visión tradicional de infraestructura TI, esto para que el cliente conozca en línea los riesgos de su negocio particular, ya sea asociado a una plataforma crítica o su sitio web.

“Hace 10 años tuve la idea de crear una plataforma que me permitiera tener la información de distintos software en un solo lugar. Cuando trabajé en el sector de telecomunicaciones me tocó hacer muchos diagramas del comportamiento de los servicios para el usuario final, por lo que siempre tratamos de tener el resultado de un servicio o proceso crítico, pero para lograrloteníamos que hacerlo con un montón de plataformas y si bien intentamos unirlos, fue básicamente imposible, porque todas las plataformas dependían de su propia marca”, cuenta Fabián Rodríguez, uno de los creadores de Camel.

Después de varios años de experiencia y buscar información sobre las mejores prácticas, Fabián Rodríguez y Luis Montenegro llegaron a la conclusión de que debían crear un producto como Camel. Así fue como las primeras ideas dieron vida a CVM (Camel Vulnerability Manager), un software que administraba todo el ciclo de vida de las vulnerabilidades tecnológicas, pero a medida que se sumaron clientes y de distintos rubros, comenzaron a darse cuenta de las distintas necesidades que tenía el mercado.

Poco a poco fueron adquiriendo más experiencia y se sumó un fondo de inversiones, el cual permitió el total despliegue de Camel. Hoy, el producto central es conocido como “Camel 360” y consiste en una serie de productos que colectan información del ecosistema de seguridad del cliente. Luego de esto, es posible interactuar con ella y, con una visión de negocio, hacer el cálculo de riesgo de los procesos críticos del cliente.

“Nuestro software es capaz de analizar los distintos componentes del riesgo como; exploit que buscamos en distintas bases de datos del mundo y cruzarlas con la infraestructura del cliente, con el fin de advertir sobre los riesgos presentes. Además, permitimos que el cliente interactúe con sus vulnerabilidades, eventos o riesgo de sus servicios de negocio, independiente de donde vengan, entregamos reportes, dashboard, análisis de tendencias, asignación de tareas a grupos resolutores, entre otros datos que permitan obtener el resultado de toda la gestión. El proceso que involucra es muy grande, porque es posible medir el riesgo tecnológico de la compañía”, explica su creador. Además, agrega: “Nuestra idea es proveer de la tecnología para que los clientes puedan obtener todo en una plataforma y con una visión de negocio. Esa es la magia de Camel. No buscamos reemplazar las otras plataformas, sino interactuar con ellas”.

La confianza en Camel ha ido creciendo año a año, tanto así que hoy no sólo confían en ellos el mercado chileno, sino también Europa, Estados Unidos y Latinoamérica, donde ya cuentan con clientes de distintos rubros: banca , sector automotriz, gobiernos y el área de la salud.

Para conocer más sobre Camel y sus productos puedes ingresar a **https://www.camelsecure.com**

La colaboración público-privada como pieza esencial para fortalecer la ciberseguridad nacional.

Para mantener un ciberespacio seguro es preciso apostar por el principio de responsabilidad compartida entre las Administraciones Públicas, el sector privado y la ciudadanía. Desde su creación en 2006, han sido numerosas las acciones emprendidas por el CCN-CERT, como CERT Gubernamental Nacional de España, para impulsar la coordinación, colaboración y cooperación entre el sector público y el privado, con el fin último de asegurar la protección del ciberespacio y del patrimonio tecnológico español.

Javier Candau, Jefe del Departamento de ciberseguridad del Centro Criptológico Nacional.
Los principales cometidos de su actividad son la formación del personal especialista en seguridad de la Administración, el desarrollo de normativa del CCN (elaboración de políticas, directrices y guías de seguridad de las TIC para la Administración Pública- Series CCN-STIC),- desarrollo de la herramienta de análisis de riesgos PILAR, la supervisión de acreditación de sistemas y la realización de auditorías de seguridad así como todas las acciones derivadas del ESQUEMA NACIONAL DE SEGURIDAD (ENS).
Tiene más de 18 años de experiencia en todas estas actividades.
Responsable de la Capacidad de Respuesta ante Incidentes gubernamental
(CCN-CERT. www.ccn-cert.cni.es)

No cabe duda de que la elaboración y desarrollo de las políticas relacionadas con la ciberseguridad compete en primera instancia a los Estados. No obstante, en un entorno global, como es el del ciberespacio, donde los riesgos y amenazas afectan y son responsabilidad de forma transversal de los sectores público y privado y de los ciudadanos, la coordinación y cooperación a todos los niveles resulta fundamental para adaptarse de forma óptima a este escenario.

Es preciso considerar, además, que el sector privado es gestor y propietario de una gran parte de los activos digitales de cualquier país, por lo que las capacidades de ciberseguridad de todos ellos residen, en gran medida, en sus empresas. Así lo entiende el Centro Criptológico Nacional(1), organismo adscrito al Centro Nacional de Inteligencia de España, y así se ha entendido desde el Gobierno español que, en la Estrategia Nacional de Ciberseguridad aprobada en 2019 se insta a "apoyar, promocionar e invertir en ciberseguridad para impulsar la competitividad y el crecimiento económico, a la vez que se proporciona un entorno digital seguro y confiable"(2). Este objetivo ha estado presente desde sus orígenes en 2006 en el CCN-CERT, del Centro Criptológico Nacional. Como CERT Gubernamental Nacional ha apostado por impulsar y liderar numerosas acciones destinadas a reforzar la colaboración público-privada y la seguridad y robustez de las redes, productos y servicios de las TIC empleadas en el sector público español, institucionalizando la cooperación entre los organismos públicos y la empresa privada como clave para construir comunidad.

Más de 22 soluciones de **ciberseguridad**

Fruto de esta coordinación, el CCN ha desarrollado junto con la industria española más de 22 soluciones comunes y compartidas[3] de auditoría, detección, análisis, intercambio de información y formación, que pretenden garantizar la seguridad de los sistemas y contribuir a una mejor gestión de la ciberseguridad en cualquier organización. Para ello, además, se ha contado con ayuda de la Unión Europea; a través del CEF (Connecting Europe Facility), un instrumento financiero para promover el crecimiento, el empleo y la competitividad a través de inversiones específicas en tres grandes áreas: energía, telecomunicaciones (incluida la ciberseguridad) y transporte.

Los proyectos seleccionados de entre numerosas peticiones de todos los países de la UE pretenden fomentar la tecnología europea, en este caso la española, y mejorar las capacidades nacionales de ciberseguridad e intercambio de información. En concreto, sus soluciones **Carmen** (defensa de ataques avanzados/APT), **Gloria** (gestor de logs en respuesta a incidentes/amenazas), **Marta** (análisis avanzados de ficheros), **Lucia** (sistema para la gestión de ciberincidentes) y **Reyes** (intercambio de información de ciberamenazas) contaron con estas ayudas.

Otras de las soluciones desarrolladas en colaboración con el sector privado han sido **Ana** (automatización y normalización de auditorías de seguridad), **Emma** (visibilidad y control sobre la red), **Elisa** (observatorio digital) o **Mónica**, la última solución en ser presentada que facilita la gestión de eventos de seguridad. También destacamos el esfuerzo desarrollado durante este 2020 en la herramienta Microclaudia (centro de vacunación para evitar ataques de ransomware) para proteger a las empresas y los organismos públicos frente a este tipo de ataques durante la pandemia del COVID19. Esta solución se complementa con la vigilancia de los accesos remotos en situación de teletrabajo realizadas por la solución Emma-VAR.

Otro ejemplo de colaboración público-privada son nuestras Guías CCN-STIC[4] e Informes de Amenazas, Código Dañino y Buenas Prácticas en materia de ciberseguridad que elaboramos en colaboración con numerosas empresas del sector.

Si bien estos recursos están principalmente dirigidos a un sector más especializado, el CCN también tiene como una de sus principales funciones formar y promover una cultura de la ciberseguridad en todo el país. En este sentido, conviene reco-

1.-Aproximación española a la Ciberseguridad Centro Criptológico Nacional
2.-Estrategia Nacional de Ciberseguridad 2019
3.-https://www.ccn-cert.cni.es/soluciones-seguridad.html

nocer que sin el apoyo de las compañías sería muy improbable que las acciones de concienciación que desde aquí se llevan a cabo a través de eventos, jornadas y congresos, se pudieran organizar. Es el caso, por ejemplo, de las Jornadas STIC CCN-CERT[5], celebradas desde 2007 gracias al patrocino y respaldo de empresas tecnológicas que, año tras año, confían en este encuentro. Gracias a todas ellas se ha convertido en el principal evento de ciberseguridad celebrado en España.

El CCN-CERT considera que estas soluciones comunes y compartidas son la piedra angular para construir una ciberseguridad homogénea en todo el sector público y privado español permitiendo coordinar las capacidades y aprovechando todas las sinergias nacionales para una respuesta ante ciberincidentes integrada que contemple tanto la prevención (reducción de la superficie de exposición), la detección (de manera automatizada basada en reglas y anomalías aplicando inteligencia artificial) como la respuesta eficiente dotando a los centros de operaciones de ciberseguridad a nivel sectorial, autonómico y local de las capacidades adecuadas. De todas ellas se resaltan las soluciones Lucia y Reyes por su capacidad de mejorar una respuesta conjunta ante la ciberamenaza.

4.-https://www.ccn-cert.cni.es/guias.html
5.-https://www.ccn-cert.cni.es/comunicacion-eventos/jornadas-stic-ccn-cert.html

Fig. 1 Soluciones de ciberseguridad del CCN-CERT

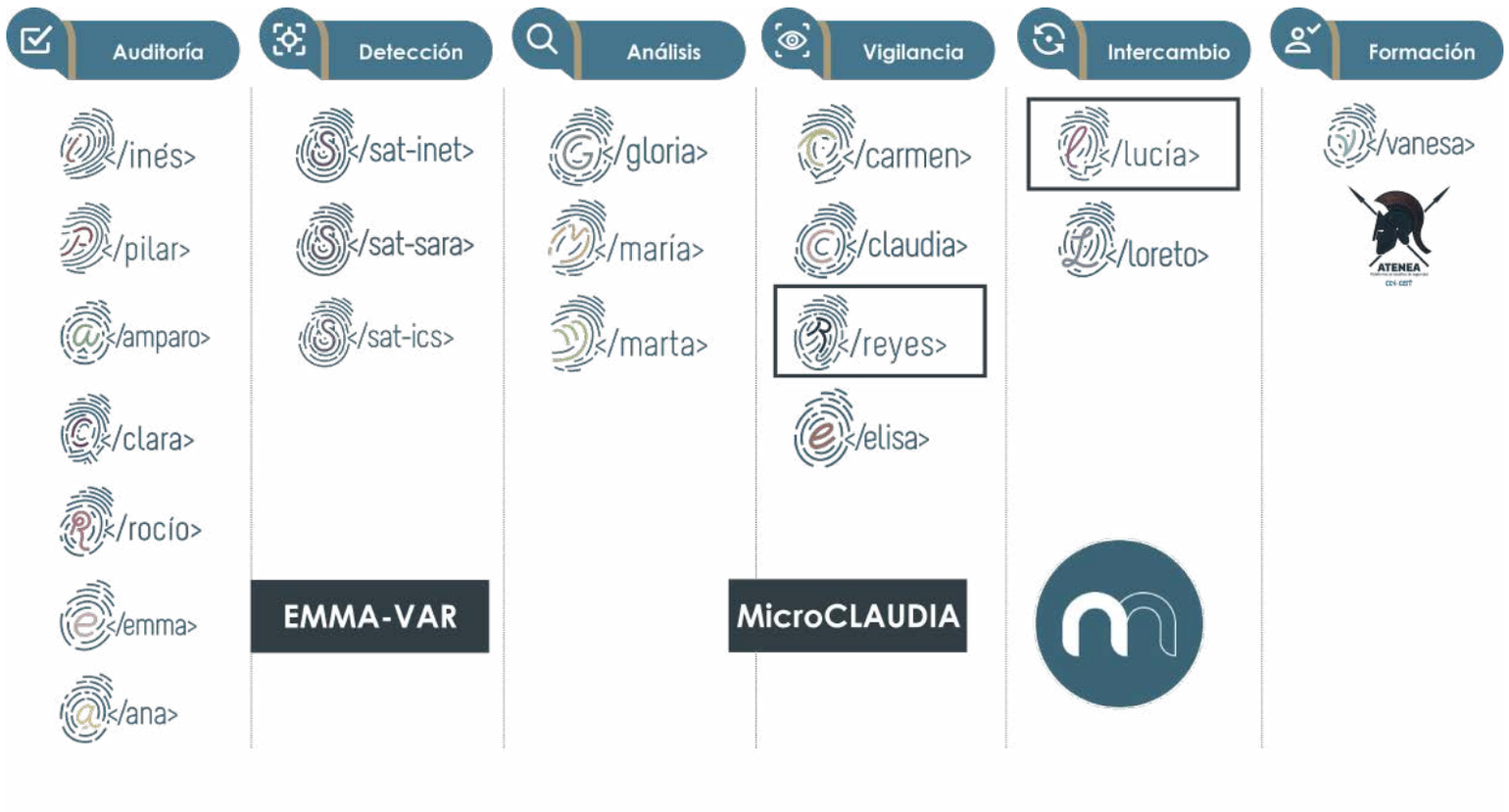
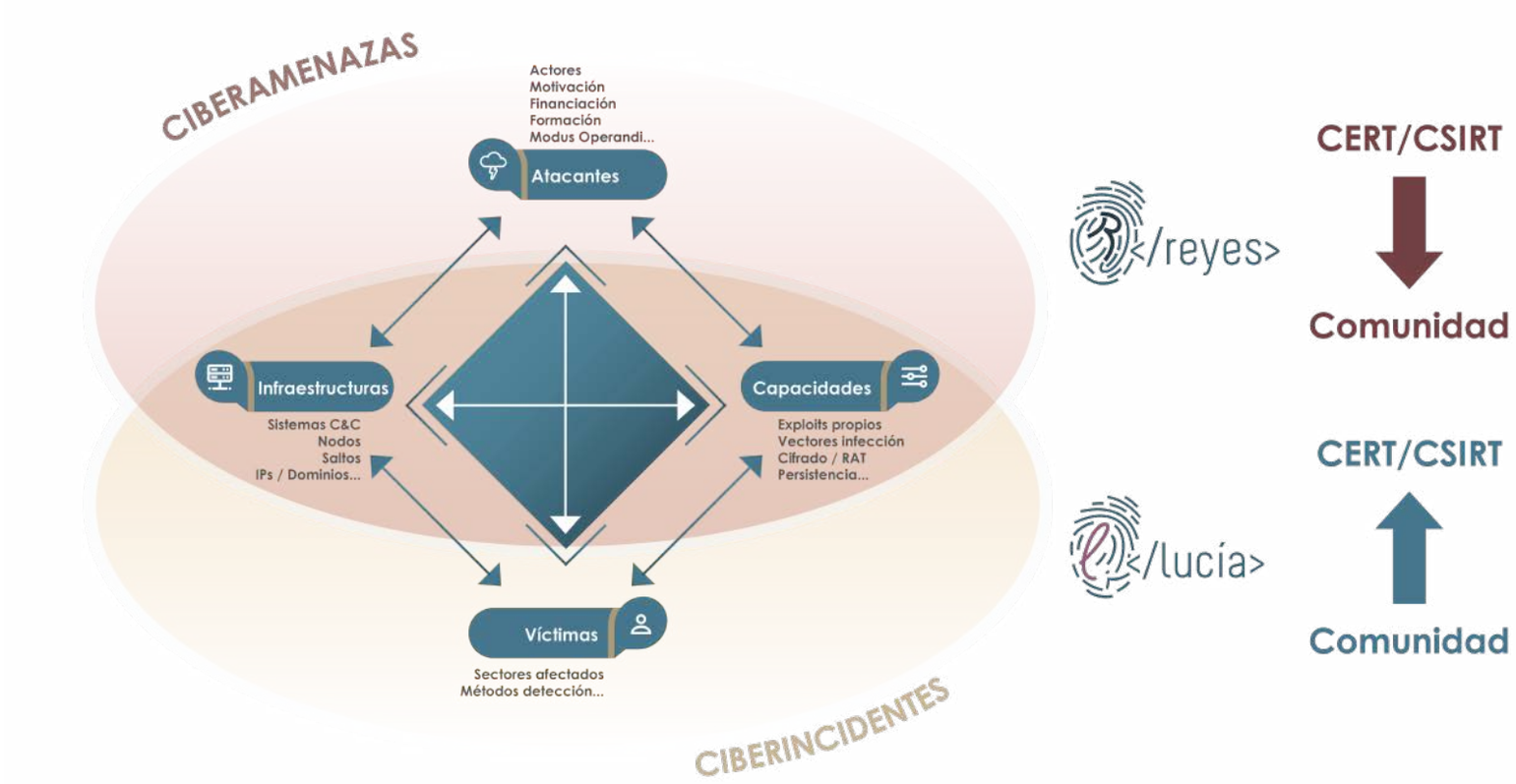


Fig. 2 Modelo de diamante. Empleo de LUCIA y REYES



Tendencia Digital

CREATIVIDAD PARA GESTIONAR **LA CIBERSEGURIDAD**

Los productos que construyen las soluciones de seguridad en el CSIRT

Andes, La Campana y Seguralia son algunos de los desarrollos propios que durante este año ha desarrolladlo el equipo del CSIRT, plataformas que buscan detectar amenazas y ayudar en la gestión de los incidentes de Ciberseguridad.

Imaginar que en el ejercicio de la función pública -abarrotada de reglas y roles definidos- haya espacio para la creatividad, es inusual. Pero siempre que las sociedades enfrentan desafíos poco convencionales, es posible encontrar el espacio para innovar y para pensar las cosas sin las ataduras propias de la burocracia.

El equipo de desarrollo del CSIRT, compuesto en su totalidad por ingenieras, encontró este espacio para crear soluciones a problemas no dimensionados. Es así como al plantearse el desafío cómo contribuir a la ciberseguridad del Estado, desarrollaron, durante este año, tres programas de monitoreos: Andes, La Campana y Seguralia.

Las amenazas, como campo de **innovación y estrategia**

Detectar amenazas y ayudar en la gestión de los incidentes. Esos son los objetivos de los desarrollos que el grupo realiza dentro del CSIRT. Este equipo se formó a finales del 2019, luego de que dos de sus integrantes participaran en un curso de capacitación en Israel, como parte del acuerdo de colaboración entre los equipos de respuesta de incidentes de ambos países. Lo aprendido en esa experiencia fue puesto en códigos para crear, a principios de este 2020, una herramienta denominada "Andes".

Andes presta una gran utilidad al monitoreo de sitios en búsqueda de posibles Defacement, un ataque que se caracteriza por la alteración en la apariencia de una página web, general

mente como consecuencia de la intrusión de un hacker o un error de programación. La herramienta funciona a partir de una carga de sitios que son revisados en forma automatizada y periódica. Si Andes detecta un error, envía una alerta y el equipo evalúa si se trata de una amenaza real o un falso positivo. Si se comprueba el incidente, CSIRT se pone en contacto con los administradores del sitio correspondiente y gestiona las respectivas mitigaciones.

El desarrollo le permitió al equipo explotar sus potencialidades, logrando así obtener un desarrollo 100% propio. Para asegurar el correcto funcionamiento y obtener un buen resultado, los programas están en permanente revisión y mejora no sólo por parte de este grupo, sino que también trabajan en conjunto con otras áreas de la División de Redes, quienes aportan con su experiencia y conocimiento para evaluar los desarrollos y proponer mejoras para pronto dejarlo disponible a la comunidad.

La Campana fue el segundo de los desarrollos del equipo. Con las estructuras de bases andando, las desarrolladoras reconocen que el trabajo fue un poco más sencillo. En ese proyecto, el objetivo fue identificar la creación de sitios que podrían ser utilizados para la suplantación de otras webs legítimas y que, eventualmente pudieran servir para campañas de phishing. La herramienta tenía que ser resuelta en poco tiempo, porque su objetivo era acotar el impacto de la eventual creación de múltiples sitios fraudulentos con el inicio de las cuarentenas. La hipótesis del CSIRT resultó ser correcta, y la herramienta, muy oportuna.

"La Campana" es una herramienta automatizada que monitorea 24/7 la creación de nuevos dominios .CL en el portal "nic.cl". Si encuentra una coincidencia a un sitio legítimo, automáticamente se levanta una alerta para los operadores del CSIRT, quienes deben contactarse con las entidades poseedoras de la marca para dar aviso de la sospecha. En esta herramienta se utiliza un diccionario personalizado para la búsqueda de sitios creados, lo que permite un alto nivel de efectividad. Una diferencia importante con respecto de Andes, es que La Campana es parte de una estrategia mayor, porque una vez identificado el sitio fraudulento, CSIRT propone un plan de acción legal para solicitar la revocación de un dominio ante NIC Chile, lo que se apoya con asesoría legal y un manual para ese propósito.

Andes y La Campana están funcionando desde el primer semestre y sus resultados son muy positivos, pues han robustecido la infraestructura de seguridad de los sitios web del sistema público y han incapacitado la acción criminal en el ciberespacio al advertir potenciales sitios para fraudes.

Conscientes de los resultados, las profesionales están cada día más motivadas para continuar desarrollando nuevos programas que permitan contribuir a detectar nuevas amenazas y detener las acciones de los criminales. Por esto, para cerrar este año y complementar el trabajo realizado, se encuentran desarrollando una plataforma e-learning, llamado Seguralia, para la concientización y educación de usuarios sobre las amenazas de ingeniería social y phishing. El objetivo es enseñar a identificar, proteger y fomentar la seguridad de la información.

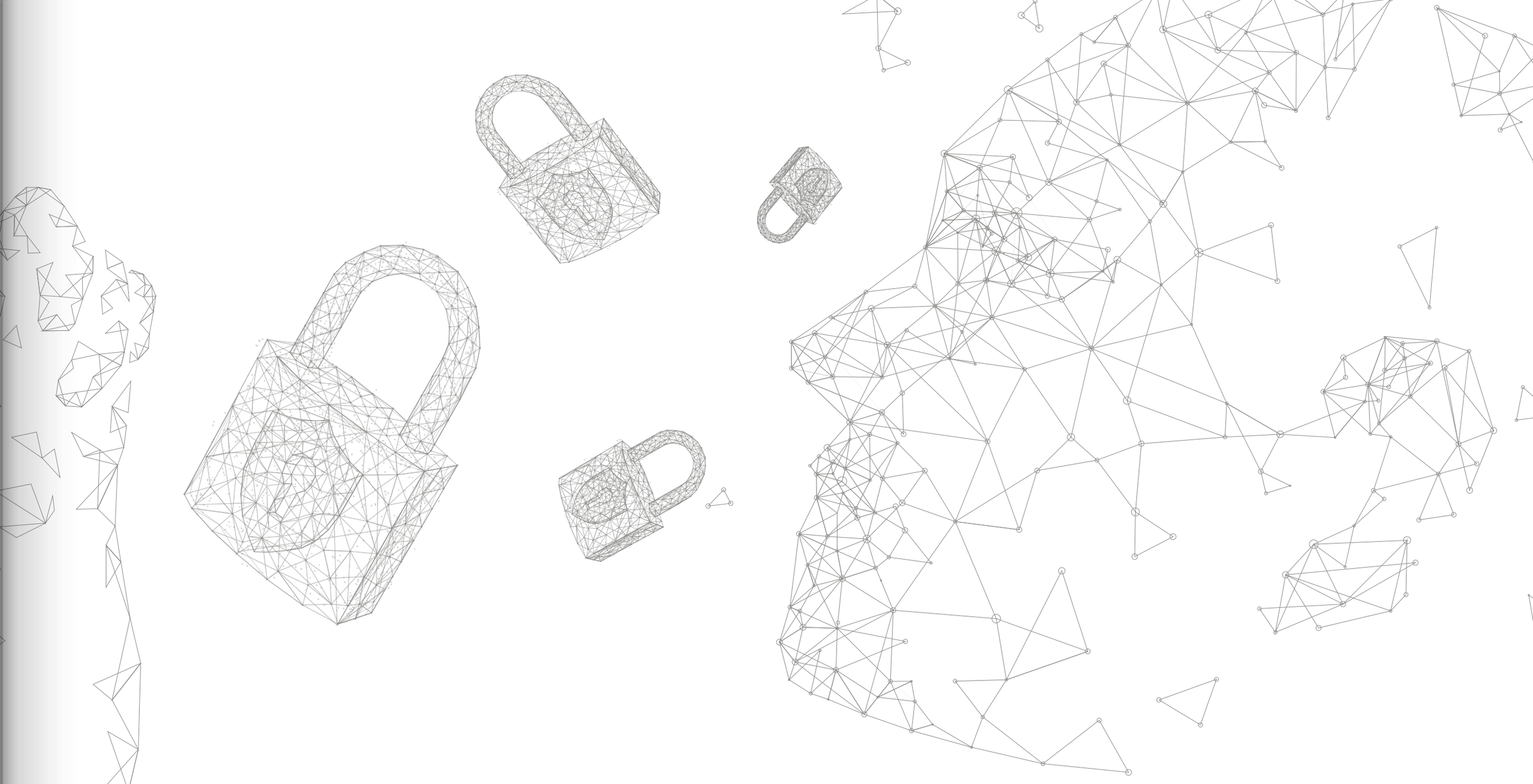
CIBERSEGURIDAD Y CRIPTOGRAFÍA DESDE LA UNIVERSIDAD DE CHILE

El CLCERT de la Universidad de Chile y su rol en el Fortalecimiento de la Ciberseguridad del País

clcert
Lab. de Criptografía Aplicada y Ciberseguridad

Vivimos tiempos complejos. La pandemia que azota al mundo nos ha obligado a revalorar nuestras redes y sistemas informáticos, de momento que tales sistemas tienen el potencial de permitirnos disminuir el riesgo de contagio, por ejemplo, con el trabajo remoto. Sin embargo, las amenazas y ataques informáticos reportados recientemente – desde vulnerabilidades en sistemas de videoconferencia y fraudes online en la devolución del 10%, hasta debilidades en los sistemas de salvoconductos ciudadanos – dan cuenta que nuestra súbita dependencia en esta infraestructura tecnológica no necesariamente viene con garantías de seguridad. Si bien Chile cuenta con una amplia oferta comercial para proteger nuestras redes actuales, nuestra seguridad en el mediano y largo plazo depende crucialmente de la existencia de centros de investigación científica. Ellos deben ser capaces de construir el conocimiento experto para mejorar la ciberseguridad de un ecosistema tecnológico inherentemente cambiante. Desde el 2001, el Laboratorio de Criptografía Aplicada y Ciberseguridad de la Universidad de Chile (CLCERT) ha buscado aportar en ese rol. La creación de capital humano especializado en ciberseguridad, la generación de información precisa y relevante para la generación de políticas públicas tecnológicas, y el desarrollo de sistemas innovadores cada vez más seguros han sido las líneas de desarrollo del CLCERT. Ellas han sido llevadas a cabo tanto desde proyectos académicos como vía directa colaboración con organizaciones públicas y privadas en nuestro país.

Desde la perspectiva formativa, el CLCERT ha participado en la organización o ejecución de programas académicos y cursos en temas tan variados como criptografía aplicada, criptomonedas, votación electrónica, y ciberseguridad, y el desarrollo de competencias de tipo capture the flag, dirigidos a sus estudiantes universitarios. Es justamente en estas últimas instancias donde hemos visto un creciente interés en la forma de nuevos y nuevas participantes de diverso perfil, en una afortunada consecuencia del incremento reciente en el número de estudiantes en carreras de computación e informática. Nuestro país – y no sólo la U. de Chile – tiene la enorme oportunidad de crear una nueva generación de profesionales de ciberseguridad, la cual no debe dejar pasar. Por esto, las iniciativas donde los estudiantes tengan el espacio y el apoyo para desarrollar sus conocimientos y habilidades en el área debieran ser prioritarias. Nuestra experiencia en el CLCERT dice que, usualmente motivados por un sentido de comunidad y con motivación de sobra, los jóvenes sólo buscan la oportunidad del conocimiento. De hecho, nuestro laboratorio, en cierto sentido, sólo ha tenido la suerte de estar en el lugar correcto, en el momento adecuado, lo cual le permitido transformar ese entusiasmo en proyectos innovadores para el país. El grupo de investigación del CLCERT se desenvuelve en dos líneas de trabajo principales: búsqueda y notificación de vulnerabilidades, y desarrollo de nuevas tecnologías en ciberseguridad. A continuación, mencionaremos brevemente algunas de las experiencias recientes dentro de estos ámbitos.



La búsqueda y notificación de vulnerabilidades es una de las formas en la cual la participación, aprendizaje y motivación de los y las estudiantes se convierte en un mecanismo de mejora de la ciberseguridad de nuestros sistemas informáticos. El empuje de una mente curiosa puede transformarse en la detección de una vulnerabilidad de seguridad multimillonaria. Para el CLCERT, un caso destacable en este sentido fue la experiencia con el Banco de Chile durante los años 2017 y 2018. Gracias a la investigación de un estudiante de pregrado, se pudo identificar y luego reportar una vulnerabilidad que permitía a cualquier persona endosar una compra a un cliente del banco, contando solamente con el RUT del cliente. Si bien el proceso de notificación no estuvo exento de dificultades – luego de casi un año de interacción entre investigadores del CLCERT y la entidad financiera, sólo una divulgación pública de la falla gatilló el arreglo del problema – la experiencia permitió evidenciar carencias subyacentes en la industria (en particular, la falta de canales de reporte de vulnerabilidades) incluso antes que la seguridad bancaria estuviera cuestionada por bullados robos por parte de grupos internacionales.

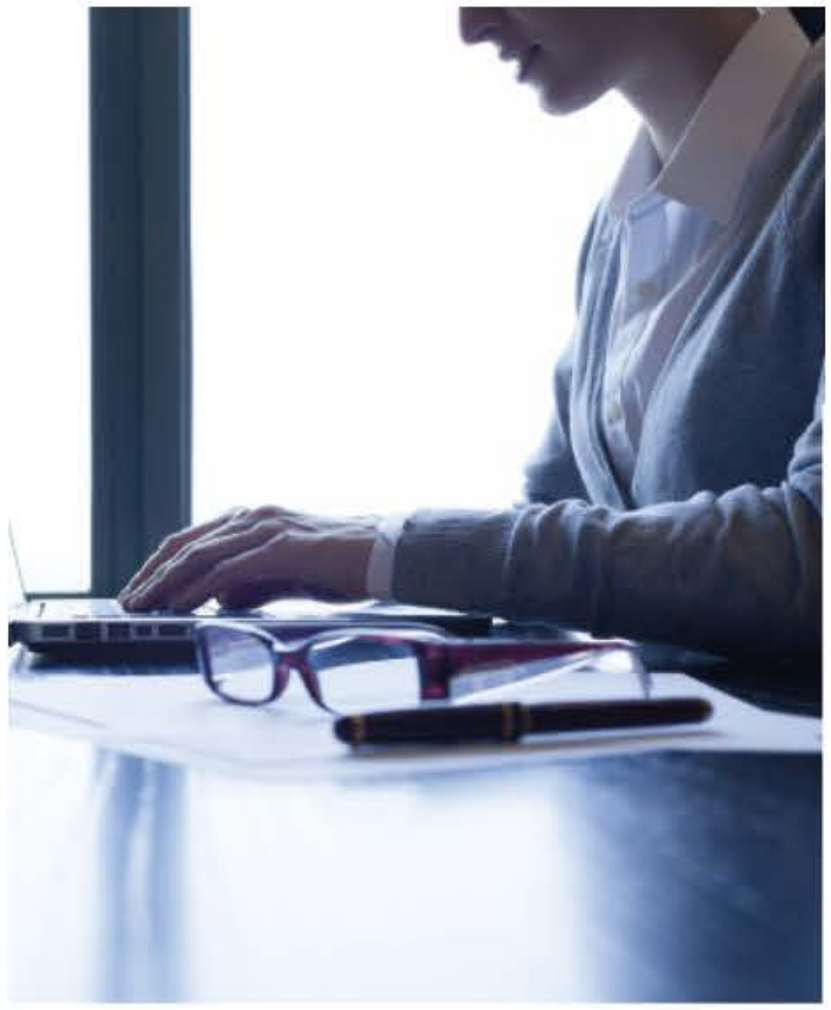
No todos los casos de reporte de vulnerabilidades han sido así de difíciles para el CLCERT. Hace tan solo unos meses, investigadores del laboratorio detectaron la exposición pública de datos personales como nombre, RUT y dirección de pacientes y sospechosos de COVID-19 reales. Los datos estaban asociados a una plataforma de desarrollo privado utilizada por un organismo de salud de gobierno. Afortunadamente y en contraposición al caso anteriormente descrito, una diligente y certera respuesta del grupo de desarrollo involucrado al recibir el reporte permitió corregir el problema en muy poco tiempo. La relación de confianza y valoración mutua construida tras este proceso llevó a investigadores del CLCERT a colaborar activamente en mejorar esta plataforma para su uso en Chile.

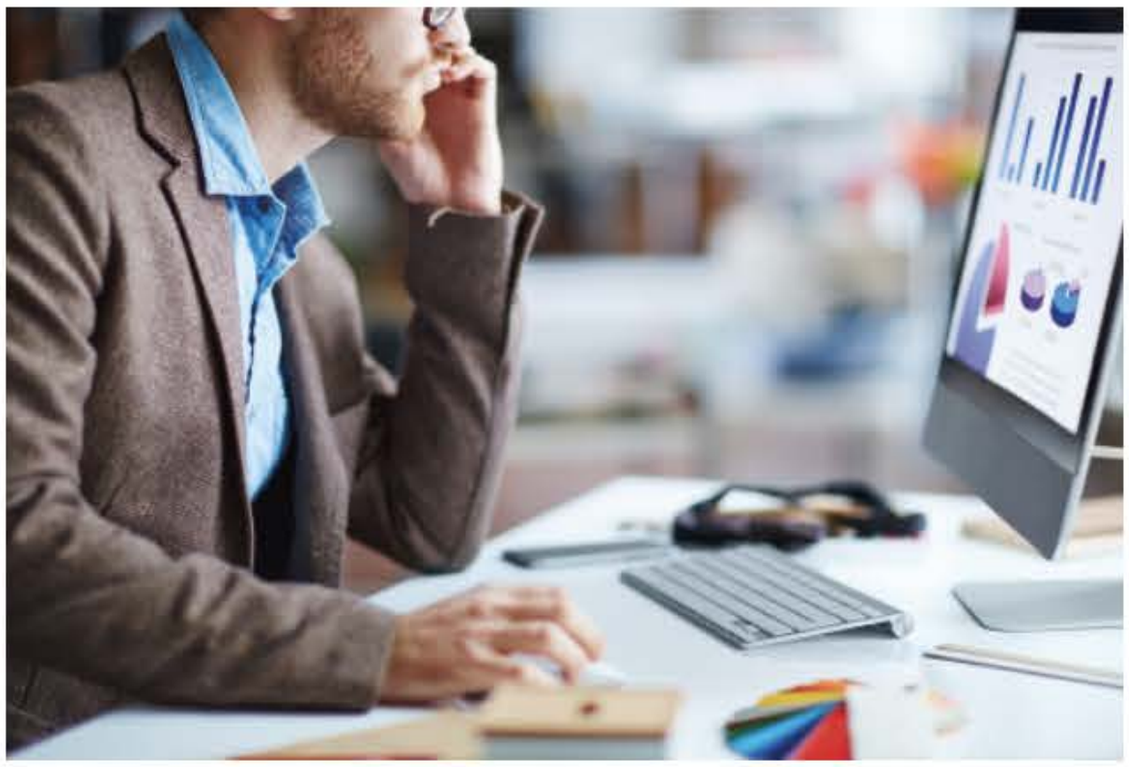
Con respecto a la investigación y desarrollo de nuevas tecnologías en ciberseguridad, el CLCERT pone su creación científica a disposición de la comunidad chilena a través del desarrollo de plataformas con sistemas de código abierto, utilizables (y replicables) por toda la comunidad chilena. Dos servicios actualmente entregados por el CLCERT son muestra de esto: el faro de aleatoriedad verificable (o Random UChile, random.uchile.cl) y el sistema de monitoreo activo de la red chilena (Observatorio de Seguridad de la Red). El primero, el sistema Random UChile, permite generar números aleatorios confiables en forma pública: en cada minuto, el sistema produce una semilla aleatoria, pública y verificable generada a partir de datos aleatorios entregada por fuentes públicas tales como el Centro Sismológico Nacional, radios, mensajes en Twitter, e incluso blockchains. Esta semilla puede ser incorporada en procesos (algoritmos) del sector público que utilicen el azar y así entregarles transparencia a procesos que de otra manera serían opacos (¿cómo saber, por ejemplo, si mi selección como vocal fue efectivamente aleatoria?). Un ejemplo de ellos es el prototipo desarrollado en la Contraloría General de la República, el cual utiliza Random UChile para sustentar una elección imparcial de funcionarios y autoridades a auditar. Llendo un poco más lejos, Random UChile es parte de La Liga de la Entropía, una iniciativa internacional aún mayor, donde participan entidades públicas y privadas de todo el mundo, con el objetivo de crear un faro de aleatoriedad distribuido y estandarizado.

El segundo servicio del CLCERT es un sistema de monitoreo activo de sistemas en la red chilena. A través de escaneos periódicos a dispositivos en la red chilena (esto es, ubicados en territorio nacional, incluyendo aquellos asociados a infraestructura crítica), el sistema identifica vulnerabilidades en ellos, permitiendo reportarlos antes de ser descubiertos y explotados por criminales. Actualmente un portal especializado con visualizaciones automáticas y periódicas de dichos reportes se encuentra en desarrollo.

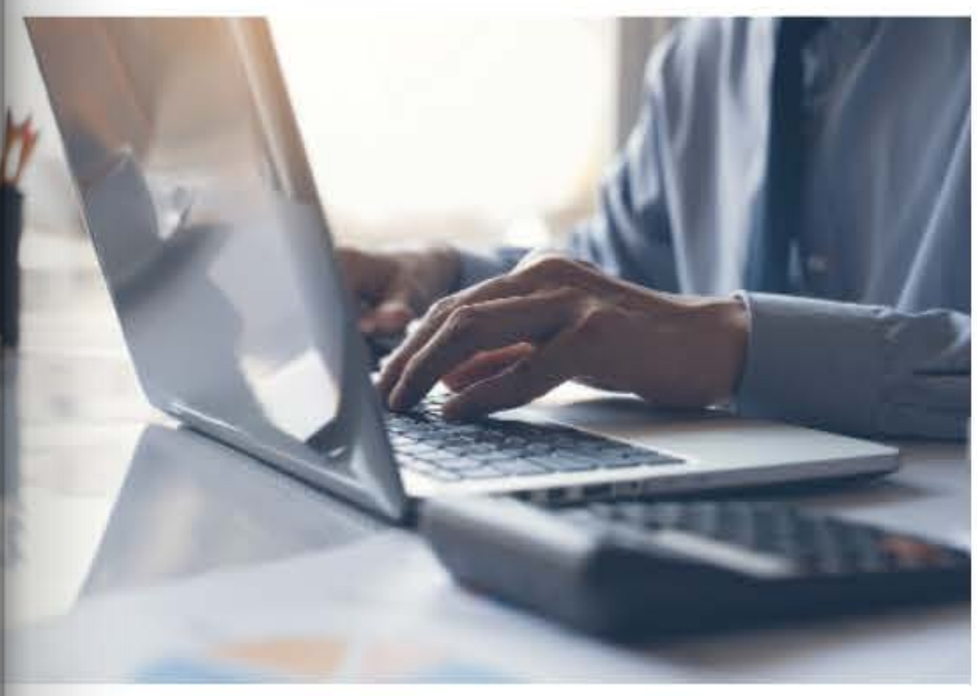
En el futuro, el CLCERT planea extender las líneas de trabajo actuales, incluyendo la formación de redes de trabajo con otras instituciones tanto públicas (CSIRT Gob) como privadas (Alianza Chilena de Ciberseguridad). Facilitar el intercambio de información, lograr la formación de un recurso humano experto, y concebir iniciativas tecnológicamente innovadoras en ciberseguridad serán siempre objetivos de este grupo.

Legal





EMPRENDEDORES, **OJO CON SU PROPIEDAD INTELECTUAL**



Todos sabemos que emprender es una tarea difícil, desafiante y a veces bastante frustrante, tarea que es el resultado de un proceso creativo en la que se buscan maneras de resolver o satisfacer necesidades no resueltas. Los últimos años han estado marcados por una explosión de nuevos emprendimientos, explosión que la pandemia ha llevado a niveles nunca antes vistos, ya que producto de la misma, muchas personas, se han visto obligadas a reinventarse, dando espacio a la creatividad e ingenio para generar todo tipo de negocios y nuevas invenciones.

En ese camino, el emprendedor generalmente focaliza toda su atención y energía en lograr que su negocio sea rentable en el menor tiempo posible, dejando muchas veces de lado la protección de su propiedad intelectual. En ese sentido, una de las primeras cosas que se debiera proteger, es el nombre de su negocio, su marca, esto porque ella es la cara visible de la empresa, siendo uno de los casos más polémicos del último tiempo el de la marca de miel "Gibson".

¿Qué es una marca?

Una marca comercial es todo signo que sea susceptible de representación gráfica capaz de distinguir en el mercado productos o servicios. Ellas pueden consistir en palabras, elementos figurativos, así como también, cualquier combinación de estos signos, pero lo más importante es que estas tienen que tener un carácter distintivo, deben ser capaces de distinguirse de otras que existan en el mercado. ¡Ojo que la marca no es lo mismo que la razón social de la empresa!

¿Por qué registrar mi marca?

Porque ofrece varias ventajas, como otorgar el derecho exclusivo a utilizarla por un periodo de 10 años renovables indefinidamente, el poder licenciarla y sobre todo el poder evitar que otros utilicen signos similares a la marca registrada a través de acciones tanto penales como civiles.

¿Cómo registro una marca?

En primer lugar, debemos analizar si la marca que queremos registrar reúne los 3 requisitos esenciales para su registro, esto es: signo, representación gráfica y distintividad. Para el caso de que concluyamos que la marca cumple con ellos, hay que determinar si la marca que queremos registrar está constituida por una palabra, en cuyo caso sería una marca denominativa, o si consiste en una imagen grafico o símbolo, en cuyo caso sería una marca figurativa o podría ser que la marca que se quiera registrar reúna todos los elementos anteriores, en cuyo caso estaríamos frente a una marca mixta.

En segundo lugar, debemos tener presente que para solicitar una marca comercial en Chile es necesario clasificar los bienes o servicios comprendidos por ella en alguna de las 45 clases de productos y servicios que comprende la clasificación de Niza. Por ello, antes de presentar la solicitud de registro debemos tener claridad de cuál o cuáles serán los productos o servicios comprendidos por la marca en base dicha clasificación, la cual podemos encontrar en https://www.wipo.int/classifications/nice/nclpub/en/fr/ .
Una vez efectuado todo lo anterior estamos en condiciones de presentar una solicitud de registro ante el Instituto Nacional de Propiedad Intelectual (INAPI).
Para ello, debemos dirigirnos al sitio https://www.inapi.cl/marcas/tramites/solicitud-nueva y seleccionar la opción "solicitud nueva y pago electrónico" y rellenar el formulario que se presenta en base a la información que levantamos previamente.
El procedimiento de registro es eminentemente online y si no existen observaciones u oposiciones al registro este tarda aproximadamente 5 meses en total.

EL PASO A PASO **DEL REGISTRO**

1. Presentación de la solicitud.
2. El examen formal de la misma por parte del INAPI, en el cual se determina que la solicitud cumple todos los requisitos formales.
3. Efectuado el examen formal sin observaciones, en un plazo de 20 días hábiles desde la aceptación del trámite, se debe efectuar su publicación en el diario oficial. Ello para dar a conocer la solicitud de registro y darle la oportunidad a terceros para que puedan oponerse al registro de la misma. En caso de que el INAPI haya efectuado observaciones en la forma, estas deben ser contestadas dentro de un plazo de 30 días hábiles desde la notificación de las mismas.
4. El examen de fondo de la misma por parte del INAPI, en el que este determina si la solicitud de registro cae en algunas de las causales de rechazo contempladas en la ley. En caso de que existan observaciones en el fondo u oposiciones por parte de terceros, éstas deben ser contestadas dentro de un plazo de 30 días contados desde su notificación.
5. La resolución definitiva de concesión.
6. Registro de marca.

PROTEGIENDO **EL DISEÑO**

Registrada la marca, lo que debiéramos proteger ahora es el diseño de nuestros productos, su diseño industrial, entendiéndose por tal toda forma tridimensional asociada o no con colores, y cualquier artículo industrial o artesanal que sirva de patrón para la fabricación de otras unidades y que se distinga de sus similares, sea por su forma o configuración de tal manera que resulte en una apariencia nueva.
Para ello, deberemos presentar ante el INAPI una solicitud de patente de diseño industrial, la que una vez concedida otorga una protección por 10 años no renovables.
El único requisito para proceder a proteger un diseño industrial, es que el diseño debe ser "nuevo". Considerándose nuevo un diseño que no se ha hecho público, ni ningún otro idéntico o similar antes de la fecha de presentación de la solicitud de registro. Esto es, en la medida en que el diseño por el cual se solicita protección difiera de manera significativa de diseños industriales conocidos o de combinaciones de características de diseños industriales conocidos.
Una vez determinado que el diseño industrial a registrar cuenta con el nivel de novedad suficiente, debemos dirigirnos a la página web del INAPI: https://www.inapi.cl/patentes/tramites/-tramitacion-de-patentes y seleccionar "solicitud y pago en línea". Una vez seleccionado dicho trámite accederemos a la hoja de solicitud, donde deberás describir detalladamente el diseño y acompañar dibujos e imágenes del mismo.
El procedimiento para efectuar el registro es el mismo señalado para las patentes de invención.

TEN **PRESENTE**

1. Para saber si la marca que quieres registrar ya se encuentra registrada o se asimila a una que ya lo esté, puedes salir de esa duda haciendo una búsqueda en el siguiente link: https://ion.inapi.cl/Marca/BuscarMarca.aspx.

2. Si bien las marcas y los nombres de dominio no son lo mismo, este último ha pasado a ser una expresión de las primeras en internet, por lo que siempre que registres una marca, registra también el nombre de dominio asociado a ella y viceversa.

¿Y QUÉ SUCEDE SI LO QUE QUIERO PROTEGER **ES UN PROGRAMA DE COMPUTACIÓN?**

En ese caso, debemos tener presente que, en nuestro país, los programas de computación (Software) están protegidos por la ley de derechos de autor, la que asimila éstos a una obra literaria, tal y como si de un libro se tratase. La importancia de esta ley, es que otorga una protección automática a los derechos que, por el solo hecho de la creación de la obra, adquieren los autores de la misma.
Esto quiere decir que no es necesario hacer ninguna gestión para adquirir la protección que otorga la ley, el programa que has creado o encargado su creación, está protegido automáticamente.
Sin perjuicio de ello, el registro es sumamente útil, toda vez que sirve como medio de prueba y además deja claramente establecido quién es el titular de los derechos.
Un programa de computación, al igual que toda obra, debe cumplir con 3 requisitos fundamentales para ser objeto de protección, debiendo ser:

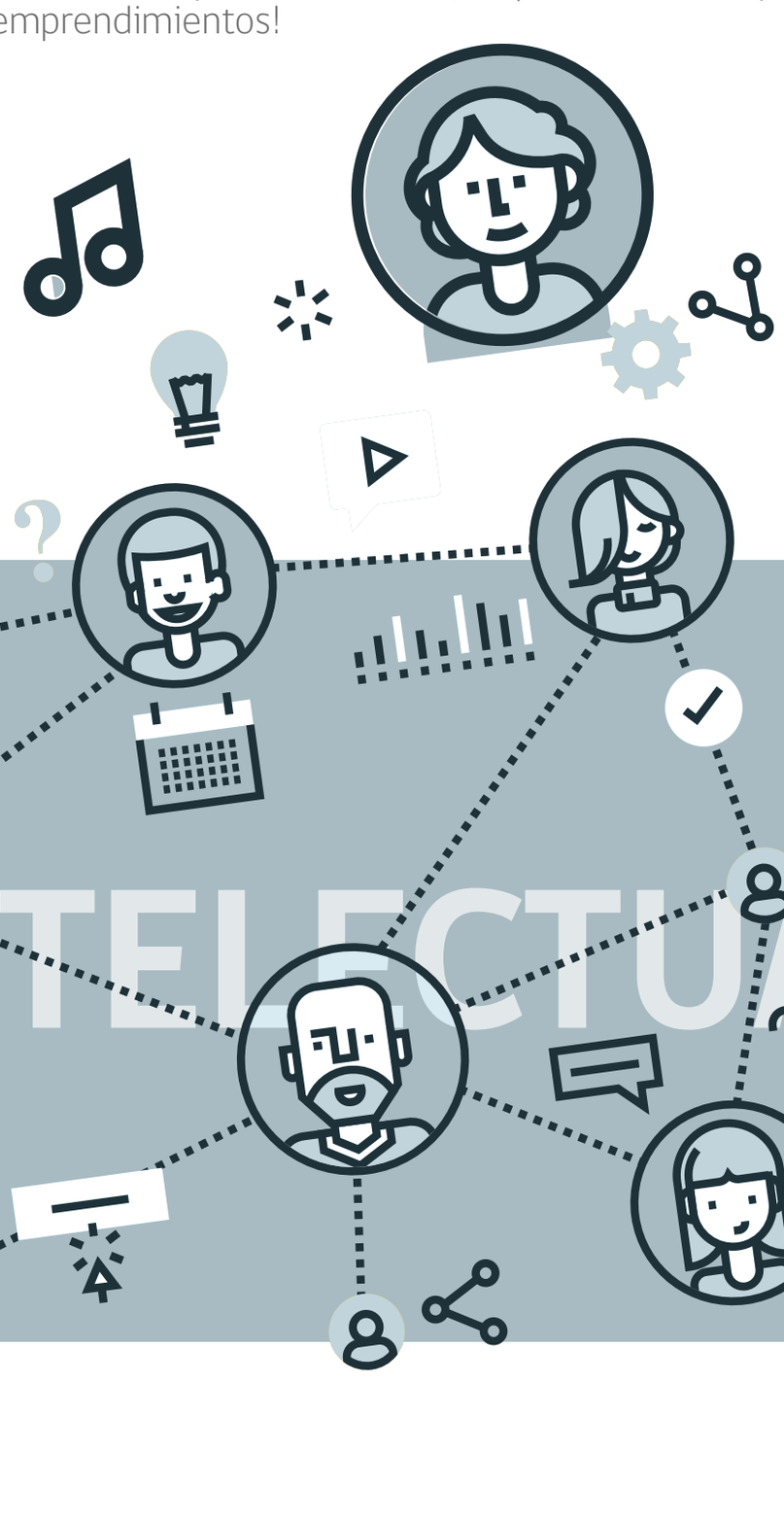
Novedoso: que no haya sido producida anteriormente por un tercero.

Original: la obra tiene que manifestar la personalidad de su autor.

Lícito: que no sea contraria a la ley, al orden público y a las buenas costumbres.

Cumpliendo con esos requisitos, ya estarías condiciones de presentar una solicitud de registro ante el departamento de derechos intelectuales del Servicio Nacional del Patrimonio Cultural en el siguiente link:
https://www.propiedadintelectual.gob.cl/sitio/Contenido/Instucional/29209:Inscripcion-de-Obra-Intelectual

Una vez ahí debes seleccionar la opción "solicitar un nuevo registro" y completar el formulario. Ojo, que esta sección puede ser un poco confusa, por lo que para registrar un programa computacional, en la sección "género de obra" selecciona "literaria" y en el tipo de obra, "programa computacional".
Luego de esto, el proceso de registro de software es bastante sencillo debiendo depositar en el Servicio Nacional del Patrimonio Cultural una copia del código fuente, un manual de uso, una declaración jurada de que se es el titular del software y copias de las licencias de los programas que se utilizaron para programar.
Con estos importantes consejos, ¡te invitamos a proteger tus emprendimientos!



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile

CONTÁCTANOS

+(562) 2486 3850

r e g i s t r a u n i n c i d e n t e

Síguenos

Twitter de CSIRT
https://twitter.com/csirtgob/

LinkedIn
https://www.linkedin.com/company/csirt-gob/

Youtube
https://www.youtube.com/channel/UCua0E5Jz9V1Rn-VtLHPP4Nw/

Instagram
https://www.instagram.com/csirtgobcl

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl