

SPD constituyó fuerza de tarea para implementación de la Ley de Seguridad Privada



A falta de poco más de un mes de la entrada en régimen de la Ley de Seguridad Privada en el país, el 29 de octubre las autoridades de la Subsecretaría de Prevención del Delito y la Subsecretaría de Seguridad Pública, lideraron la constitución de una fuerza de tarea para permitir la correcta puesta en marcha de la normativa junto a las instituciones y entidades obligadas que estarán reguladas a contar del 28 de noviembre.

En la cita participaron Carabineros de Chile, la Dirección General del Territorio Marítimo y Marina Mercante (DIRECTEMAR); la Dirección General de Aeronáutica Civil (DGAC); el Servicio de Impuestos Internos (SII); la Dirección General de Movilización Nacional (DGMN); Banco Estado, la Asociación de Empresas de Valores (ASEVA), el Hub de Líderes de Seguridad Empresarial A.G. (HUBLS), la Asociación de Bancos e Instituciones Financieras (ABIF) y la Asociación Chilena de Empresas de Seguridad Electrónica y Alarmas Monitoreadas (ACHEA), representada por nuestro presidente, Víctor Hugo Herrera Pintor.

Durante la jornada de trabajo se estableció un cronograma de presentación de los instrumentos de seguridad privada a fin de dar cumplimiento a los plazos legales de la ley, las nuevas obligaciones, y también la identificación de necesidades, brechas y propuestas del sector privado frente a la normativa.

“Esta ley representa un cambio estructural en cómo funcionan tanto las autorizaciones como el trabajo de esta industria tan importante para nuestro país. Por eso es necesario ir acompañando este proceso de seguimiento e implementación”, dijo la titular de la Subsecretaría Carolina Leitaó. Fuente: SPD



Asociación Chilena
de Empresas de Alarmas
y Seguridad A. G.

EDITORIAL

PERSONAS NATURALES QUE EJERCEN ACTIVIDADES DE SEGURIDAD PRIVADA EN SEGURIDAD ELECTRÓNICA

El Artículo 80 del Reglamento de Seguridad Privada establece que la “calificación del personal de las empresas de seguridad electrónica” recae sobre este tipo de empresas, que deberán garantizar que el personal de su dependencia cuente con los conocimientos necesarios para desempeñar las funciones para las que ha sido contratado. Lo anterior se acreditará a través de los respectivos certificados de estudios y/o de las capacitaciones que el empleador le provea en el área, sin perjuicio de las reglas generales y especiales que correspondan, dispuestas para las personas naturales que ejercen actividades de seguridad privada, de conformidad a los párrafos V y X del presente título, respectivamente.

Considerando lo anterior y probablemente el análisis previo del legislador de aquellos aspectos técnicos en la gestión de las centrales integrales de monitoreo, entre otras: Distintos sistemas de monitoreo, tipos, equipos, tecnologías de cada empresa, fabricación, características técnicas y funcionales, códigos, lecturas e interpretaciones, frecuencias radiales, canales de comunicación, protocolos de monitoreo, de comunicación, procesos de verificación de emergencias con variados canales independientes y la evolución, desarrollo e innovación que ofrece cada empresa y sus ventajas competitivas. ACHEA estima que estos, entre otros elementos, constituyen el fundamento de la decisión que adoptó el legislador para no definir un curso específico para aquellas personas naturales que ejercen actividades en seguridad electrónica como Operador de cámaras de televigilancia y alarmas e Instalador técnico, estableciendo que la calificación del personal y la certificación de sus competencias (capacitación específica, funcional e instrumental) recae sobre las empresas de seguridad electrónica y las debe proveer el empleador.

Esperamos que en la implementación de la ley así sea interpretado y establecido. De lo contrario, podría generarse una sobre-regulación y eventuales nudos críticos que se pueden evitar. En este contexto, valoramos el rol de la División de Seguridad Privada, que dirige las mesas técnicas de actores relevantes en el marco de la convocatoria del Ministerio de Seguridad Pública a través de la SPD.



Presidente Boric firmó decreto de la Política Nacional de Seguridad Pública 2023-2031

Durante la ceremonia de inauguración de un cuartel de la PDI en Limache, el Presidente Gabriel Boric firmó el decreto de la Política Nacional de Seguridad Pública (PNSP) 2025-2031, el principal instrumento de planificación en materia de seguridad para los próximos años, en el marco del nuevo Sistema de Seguridad Pública creado por la Ley N° 21.730.

Se trata de la primera política nacional de seguridad en 21 años y busca enfrentar los desafíos actuales de criminalidad con una respuesta integral, coordinada y basada en evidencia, estableciendo los principios rectores, orientaciones estratégicas y objetivos para las estrategias, planes, programas y acciones del Sistema de Seguridad Pública hasta el año 2031.

El ministro de Seguridad Pública, Luis Cordero, destacó que “en materia de seguridad pública, lo relevante no es solo la contingencia, sino también cómo hacer sostenibles los objetivos en el largo plazo y obtener resultados. Eso implica mirar a las instituciones y al Estado como uno solo y dejar de observar cuestiones circunstanciales y sectoriales”, enfatizó.

La PNSP establece como objetivo general “reducir los delitos violentos y el temor en la ciudadanía mediante el establecimiento de lineamientos al Sistema de Seguridad Pública, orientados a fortalecer la coordinación y colaboración interinstitucional en el diseño y la ejecución de políticas públicas basadas en evidencia”. Fuente: SPD

SPD publica nueva resolución para la implementación de la Ley de Seguridad Privada

Con fecha 03 de octubre, y publicada el 9 del mismo mes en el Diario Oficial, la Subsecretaría de Prevención del Delito dio a conocer la Resolución Exenta N° 1.977, que Aprueba instrucciones generales para la actividad de seguridad privada relativa la custodia y transporte de carga sobredimensionada.

Esta normativa viene a sumarse a la RE N° 1.820, oficializada en septiembre, aprobando la matriz de factores de riesgo en seguridad privada para la clasificación de entidades en el marco de la Ley N° 21.659, sobre Seguridad Privada.

De la misma forma, se encontrarían aprobadas y prontas a ser publicadas en el Diario Oficial otras dos resoluciones, que dicen relación con el transporte de valores por vía fluvial, lacustre o marítima; y con el formulario de solicitud y acta descriptiva para la autorización de eventos masivos. Fuente: Cooperativa.cl

Contraloría determina improcedencia de contratar vigilantes privados para labores de seguridad pública comunal

Mediante el Dictamen N° E152300N25, la Contraloría General de la República estableció que no corresponde que las municipalidades contraten vigilantes privados para desempeñar funciones de seguridad pública a nivel comunal, pues estas solo pueden ejercerse dentro de recintos o áreas determinadas y no en espacios públicos de carácter indeterminado. El pronunciamiento responde a una consulta de la Municipalidad de Providencia sobre la procedencia de contratar funcionarios municipales o personal privado para labores de seguridad comunal, considerando la normativa vigente en materia de seguridad privada.

En su fundamento jurídico, la Contraloría señaló que:

- La Ley N° 18.695 faculta a las municipalidades para adoptar medidas en materia de seguridad pública comunal, pero sin invadir las atribuciones que corresponden al Ministerio de Seguridad Pública y a las Fuerzas de Orden y Seguridad.
- El Decreto Ley N° 3.607 de 1981 autoriza a los vigilantes privados exclusivamente para brindar seguridad en edificios, empresas, industrias u otros recintos determinados, quedando su función limitada a dichos espacios.
- Su reglamento (D.S. N° 1.773/1994) refuerza esta limitación, precisando que los vigilantes pueden actuar dentro de recintos o áreas específicas, y solo de manera excepcional transitar por la vía pública en labores de supervisión, cuando ello se encuentre expresamente autorizado.
- El Decreto N° 867/2017 y el reciente Decreto N° 209/2025 sobre seguridad privada confirman que la seguridad privada tiene carácter complementario y debe desarrollarse en recintos o áreas determinadas, sin sustituir las funciones propias de la seguridad pública. Fuente: DiarioConstitucional.cl

Gobierno sella importantes convenios en seguridad

La Subsecretaría de Prevención del Delito (SPD) y la Asociación Chilena de Municipalidades (ACHM) formalizaron un convenio de colaboración por \$110 millones para fortalecer las capacidades de gestión en seguridad de los municipios del país en 2025-2026. Una alianza que comenzó en 2023 y ha transferido sobre 360 millones de pesos a más de 130 comunas, para que puedan diseñar y ejecutar proyectos de prevención adaptados a sus realidades locales.

El nuevo convenio contempla la elaboración y ejecución de un Plan de Asistencia Técnica y Aprendizaje Colaborativo Intermunicipal, estructurado en tres líneas de trabajo fundamentales: Asistencia técnica especializada, Formación y aprendizaje colectivo, y Difusión y materiales de apoyo.

En la misma línea y en el marco del tercer año de implementación del Plan Calles Sin Violencia, el Ministerio de Seguridad Pública y Carabineros de Chile firmaron un convenio de transferencia de recursos por \$4.868.332.370 que permitirán fortalecer las capacidades operativas y de investigación para contribuir a la prevención, control y persecución del delito. Fuente: SPD/Minseg



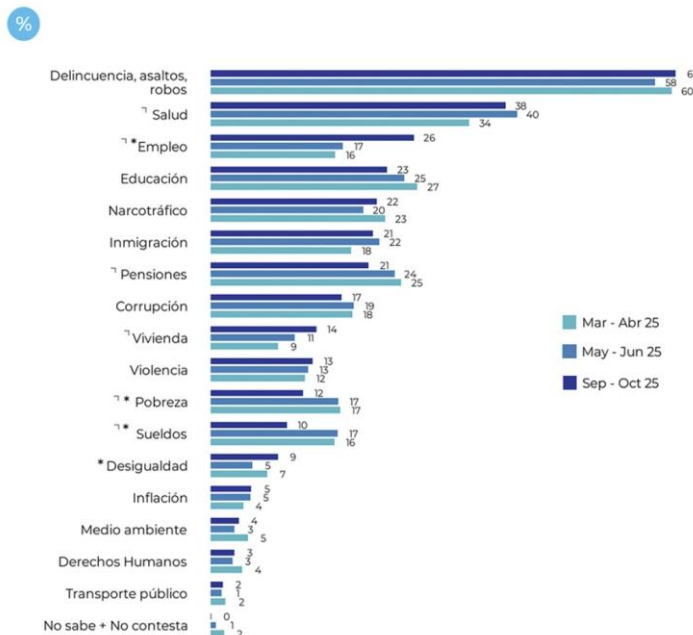
Boletín Informativo ACHEA

Encuesta CEP: Delincuencia es el problema al que el Gobierno debería prestar más atención

La 95ª edición de la Encuesta Nacional de Opinión Pública, que realiza el Centro de Estudios Públicos (CEP), reveló que la delincuencia es el problema en que el Gobierno debiera poner su principal esfuerzo para solucionar. Realizado entre septiembre y octubre de este año, el estudio mostró que la criminalidad se mantiene en el primer lugar del listado, con un aumento de tres puntos en comparación con la medición de los meses de mayo y junio. En segundo lugar, se ubicó salud, seguido de empleo, educación, narcotráfico e inmigración. En contraste, los temas que registraron menores niveles de preocupación fueron el transporte público, derechos humanos y medioambiente.

La encuesta también evidenció que la Policía de Investigaciones (PDI) mantiene el primer lugar en confianza ciudadana, pasando de 60% a 59%. Le siguen Carabineros (56%) y las universidades (54%). Las Fuerzas Armadas suben de 51% a 53%, mientras que las radios y diarios registran 43% y 29%. El Gobierno marca 20%, el Ministerio Público (los fiscales) 17%, los tribunales de Justicia (16%). El Sistema de Pensiones (15%), la televisión (14%) y las redes sociales se mantienen entre las menos confiables. En último lugar están el Congreso (8%) y los partidos políticos (4%).

¿Cuáles son los 3 problemas a los que debería dedicar el mayor esfuerzo en solucionar el Gobierno?



¿Cuánta confianza tiene usted en cada una de estas instituciones?

(% Mucha + Bastante confianza) (Evolución)



Delincuencia adolescente: 45% vivió con persona con antecedentes

Unicef Chile publicó el estudio titulado "Adolescentes en conflicto con la ley pena", que muestra que el 45% de los adolescentes infractores vivió con una persona que estuvo privada de libertad o que el 70% sufrió ausencia o separación de padre o madre. En tanto, el 56% presenció violencia en su comunidad, el 48% fue víctima de violencia intrafamiliar, abuso emocional (25%), abuso físico (17%).

También expone dos perfiles de adolescentes que cometen delitos. Uno vinculado a "carencias" materiales y con inicio a temprana edad en el mundo delictual, principalmente con hurtos y robos por sorpresa. El otro, en cambio, comienza a delinquir para "lograr una capacidad económica que permita conseguir un determinado nivel de acceso al consumo, puntualmente de ropa y accesorios". Fuente: Emol

RM: Violencia en los delitos sube 14 puntos

Un sondeo realizado en la Región Metropolitana por CORPA Estudios de Mercado reveló que, si bien las víctimas de robo bajaron de 27% a 21% respecto de mayo-junio, la violencia en los delitos se mantiene en 49%, lo que significa 14 puntos más que en igual fecha de 2024. La vía pública sigue siendo el principal lugar de ocurrencia de los robos, con un 60% de los casos. Le siguen el transporte público, con 28%, y los hogares, que llegan a un 8%, ambos en alza en relación con mayo-junio. Fuente: TVN



Proyecto Red Azul: Colaboración de la Policía Nacional con la Seguridad Privada en España



En España, los profesionales de la seguridad pueden acceder ahora a la plataforma Red Azul de la Policía Nacional usando su Documento Nacional de Identidad. Este nuevo método de acceso, que busca modernizar la gestión y reforzar la seguridad, se está implementando gradualmente para todos los integrantes del plan de colaboración, permitiendo a los profesionales de la seguridad privada un acceso más directo a información y servicios.

La iniciativa, que se enmarca Proyecto Red Azul de digitalización de la Policía Nacional para modernizar los sistemas de acceso, introduce un formato de colaboración profesional de complementariedad y corresponsabilidad, mediante un escenario de puesta en común o alianza de recursos.

En este caso, los vigilantes podrán acceder a herramientas y servicios como información administrativa, acreditaciones de centros de formación y otras funcionalidades relevantes para su labor. Fuente: Seguritecnia.es



Policía Federal de Brasil ha clausurado más de mil empresas clandestinas de seguridad privada

En solo siete años, la Policía Federal (PF) de Brasil ha ordenado el cierre de al menos 1.176 empresas clandestinas de seguridad privada. La ofensiva contra empresas no autorizadas también resultó en 26 arrestos y la incautación de 46 armas de diversos calibres.

La información solicitada por Agência Brasil indica que, entre 2017 y 2024, 3.358 empresas de seguridad privada fueron blanco de la Policía Federal, solo en el ámbito de la legalidad, con lo que aproximadamente el 35 % de las empresas visitadas no estaban autorizadas para operar.

Las cifras serían aún mayores si, en 2020, la pandemia de Covid-19 no hubiera impedido a la Policía Federal llevar a cabo el operativo, que se realiza en todo el país desde 2017.

En Brasil, solo las empresas de seguridad privada autorizadas por la Policía Federal (PF) pueden prestar servicios y contratar guardias de seguridad. Desde la institución, advierten que la contratación de servicios clandestinos supone un riesgo para la seguridad física de las personas y la propiedad de los contratistas. Además, sus empleados no están sujetos a la verificación de antecedentes penales ni se ha acreditado su formación, aptitud física y psicológica. Fuente: ICNdiario



Gremio pide aprobar nueva Ley General de Seguridad Privada en México

En una asamblea celebrada en Playa del Carmen, Daniel Espinosa Ávila, presidente de la Asociación Mexicana de Seguridad Privada (AMESP), manifestó que el rezago legislativo que ha frenado la aprobación de la nueva Ley General de Seguridad Privada limita el potencial del sector como coadyuvante de la autoridad y obstaculiza su desarrollo.

"Seguimos luchando por una legislación justa, adecuada y acorde a nuestras necesidades. A pesar de los desafíos, hoy renovamos nuestro compromiso con las autoridades federales, estatales y municipales porque somos coadyuvantes de la seguridad pública", comentó el directivo.

Espinosa Ávila agregó que "es importante que las autoridades vean la fuerza que representa AMESP y el esfuerzo que hacen sus integrantes todos los días". Y destacó que el sector genera más de 700.000 empleos formales y representa casi el 2% del Producto Interno Bruto (PIB) nacional. "Estamos en un proceso de modernización y transición, adaptándonos a nuevas regulaciones para mejorar las condiciones laborales y profesionales de nuestros elementos", señaló.

Fuente: Segurilatam

En España, ingresos de las compañías de seguridad crecieron 7,6% en 2024

En 2024, el sector de las empresas de seguridad en España alcanzó un negocio de 6.440 millones de euros, lo que supone un crecimiento del 7,6% en comparación con el año anterior, de acuerdo con la información proporcionada por el Observatorio Sectorial DBK de Informa.

Este crecimiento se apoya en la «favorable evolución» de la demanda de servicios de vigilancia y transporte de fondos, así como en el «dinamismo» de los sistemas de seguridad, en un contexto de «continua innovación tecnológica» y «mejora de productos y servicios».

En el ámbito de la vigilancia, los ingresos se incrementaron un 5,5%, alcanzando los 3.260 millones de euros, representando el 50,6% del total del sector.

Por otro lado, el mercado relacionado con la instalación, mantenimiento y conexión a Centros de Recepción de Alarmas (CRA) de sistemas electrónicos aumentó un 9,6%, llegando a los 2.795 millones de euros y constituyendo el 43,4% del total.

El observatorio destaca el desarrollo de proyectos de integración tecnológica y servicios avanzados de monitorización remota, que han impulsado notablemente este sector. Para 2025 se espeta que el mercado crezca un 5%. Fuente: Democra.es



Boletín Informativo ACHEA

Ciberseguridad en la nube: cinco pasos para reducir riesgos empresariales

En el mes de la concientización en Ciberseguridad, la empresa Axity ofrece los siguientes consejos y buenas prácticas para la protección de los entornos cloud, con el propósito de que las empresas fortalezcan su infraestructura tecnológica y reduzcan los riesgos asociados a ciberataques.

Fomentar una cultura de seguridad desde el inicio

La base de toda estrategia de ciberseguridad está en las personas. Promover una cultura organizacional orientada a la protección digital permite que todos los colaboradores comprendan los riesgos, adopten buenas prácticas y respondan con rapidez ante posibles incidentes. La capacitación en temas como phishing, ingeniería social y ransomware es clave para reducir vulnerabilidades internas y fortalecer la primera línea de defensa.

Implementar soluciones de auditoría y control en la nube

Los servicios nativos de las nubes y las soluciones de terceros deben tener la capacidad de generar información que permita monitorear actividades en los entornos cloud, detectar cambios no autorizados y anticipar amenazas. Supervisar el acceso a datos sensibles, permisos administrativos y movimientos de usuarios contribuye a una visibilidad integral del sistema y a la mejora continua de los procesos de seguridad basados en las recomendaciones y buenas prácticas del proveedor de nube.

Adoptar sistemas de cifrado avanzados

El cifrado de datos en tránsito y reposo sigue siendo uno de los pilares más sólidos contra las ciberamenazas. Este mecanismo protege la información en caso de ser comprometida, reduciendo los riesgos de exposición incluso ante una brecha de seguridad. Seleccionar proveedores que ofrezcan cifrado de alta calidad y compatibilidad con entornos locales o cloud es fundamental para garantizar la integridad de los datos corporativos.

Gestionar identidades y accesos

El control de identidades y permisos de mínimos privilegios, junto con la autenticación multifactor (MFA), es vital para limitar accesos no autorizados y proteger recursos críticos en la nube. La mayoría de los incidentes empieza por el compromiso de una cuenta de accesos.

Mantener actualizados los parches de seguridad

Las vulnerabilidades en las piezas de software, sistemas desactualizados y nuevas vulnerabilidades son una de las puertas más comunes para los ciberdelincuentes. Las herramientas de gestión de parches permiten identificar, priorizar y aplicar actualizaciones de seguridad de manera oportuna, reduciendo significativamente los riesgos de infecciones de malware o interrupciones no planificadas.



Boletín Informativo ACHEA

América Latina: Déficit de 329.000 profesionales de ciberseguridad

A pesar de los avances tecnológicos, la falta de concienciación y formación en ciberseguridad sigue siendo la principal causa de las brechas de seguridad. Además, aunque la ciberseguridad se ha convertido en una prioridad estratégica dentro de las organizaciones, muchas juntas directivas aún carecen del conocimiento necesario para abordar adecuadamente estos desafíos, lo que limita la capacidad de las empresas para gestionar los riesgos de manera efectiva. La escasez de habilidades como factor clave detrás de estas vulneraciones: más del 60% de los encuestados en la región (63%) identificaron la falta de capacitación en seguridad informática como una de las principales causas de intrusiones. Respecto de las consecuencias, 35% de los encuestados latinoamericanos mencionaron que los ciberincidentes les costaron más de un millón de dólares en 2024. En tanto, 98% de las organizaciones en la región ya utilizan o planean implementar tecnologías de Inteligencia Artificial en sus estrategias de seguridad. Fuente: ItSitio.com

Ciberseguridad en crisis: 76% de los especialistas sufre Burnout

El sector de la ciberseguridad enfrenta una crisis sin precedentes: 76% de los especialistas sufrió burnout durante el último año, según un informe de Sophos. Este agotamiento no es solo un problema de salud individual, sino un riesgo crítico de negocio, ya que reduce la productividad en 39% y eleva la probabilidad de errores humanos. La fatiga de los equipos puede costar a las grandes empresas hasta 5 millones de dólares anuales en pérdidas operativas y rotación de personal. Para mitigar este impacto, las organizaciones están recurriendo a soluciones de Detección y Respuesta Gestionada (MDR), las cuales permiten externalizar la supervisión 24/7 y aliviar la carga de trabajo. El 92% de quienes utilizan servicios MDR reportan una reducción en sus niveles de estrés. Fuente: ItSitio.com

Aumenta el crimen organizado en Chile: más de 86 mil delitos en 2024

De acuerdo con la segunda versión del Indicador Nacional de Crimen Organizado, elaborado por el Centro de Estudios en Crimen Organizado (CESCRO) de la Universidad San Sebastián, el Ministerio Público recibió 86.323 denuncias por ilícitos vinculados a estas redes durante 2024. Esto significa que en solo dos años se ingresaron 20.825 mil casos adicionales, consolidando un alza de 31,8% y una tendencia que golpea especialmente a las zonas extremas del país. Aunque el narcotráfico y los delitos relacionados con armas siguen siendo los más comunes, la corrupción y la ciberdelincuencia fueron las categorías que más crecieron en los últimos años. Un 61,8% fue el porcentaje de alza de la frecuencia ponderada de delitos asociados al crimen organizado en Los Ríos, entre el 2023 y 2024, siendo la región con el mayor incremento. Al mismo tiempo, el Informe de Crimen Organizado en Chile elaborado por la Unidad Especializada en Crimen Organizado y Drogas (UCOD) de la Fiscalía Nacional reveló un incremento sostenido de los delitos predatorios



-como los secuestros y las extorsiones-, una mayor sofisticación tecnológica de las organizaciones criminales y una creciente infiltración en economías locales y mercados ilícitos, especialmente en las macrozonas norte y centro.

Así las cosas –añade-, resulta impostergable fortalecer la coordinación interinstitucional dentro de Chile: que policías, aduanas, fiscalías, jueces y en general, los actores vinculados al enforcement actúen en concierto, compartiendo datos y estrategias. La persecución efectiva al crimen organizado demanda una estrategia integral: combinar el control territorial (recuperar espacios pretendidamente capturados por las organizaciones criminales) con la persecución financiera (hacer quebrar las organizaciones criminales) y reforzar la gestión penitenciaria para impedir que las cárceles sigan sirviendo como casa matriz de las organizaciones.

Fuente: Emol y Fiscalía Nacional



Google intensifica ciberseguridad con Inteligencia Artificial: Lanza un agente autónomo contra vulnerabilidades

Google ha presentado nuevas iniciativas de ciberseguridad diseñadas para fortalecer la defensa digital global, ante el uso acelerado de la inteligencia artificial (IA) por parte de ciberdelincuentes y estafadores, con el propósito de cambiar el equilibrio en favor de los defensores, utilizando el poder de la IA de manera responsable.

La división DeepMind de la compañía presentó un agente de IA diseñado para revolucionar la seguridad del código. Lo nombraron CodeMender, capaz de detectar y corregir vulnerabilidades de software de forma autónoma antes de que puedan ser explotadas.

El sistema aprovecha las capacidades de razonamiento de Gemini para identificar fallas, generar parches y validar automáticamente las soluciones antes de una revisión humana final. El objetivo es acelerar los tiempos de respuesta en el ecosistema de código abierto y promover una defensa proactiva contra amenazas. Su enfoque de seguridad es reactivo al corregir vulnerabilidades nuevas de forma instantánea, y proactivo al reescribir y asegurar el código existente para eliminar clases completas de fallos.

En solo seis meses de desarrollo, CodeMender ha implementado 72 correcciones de seguridad en proyectos de código abierto. Fuente: Wired.com