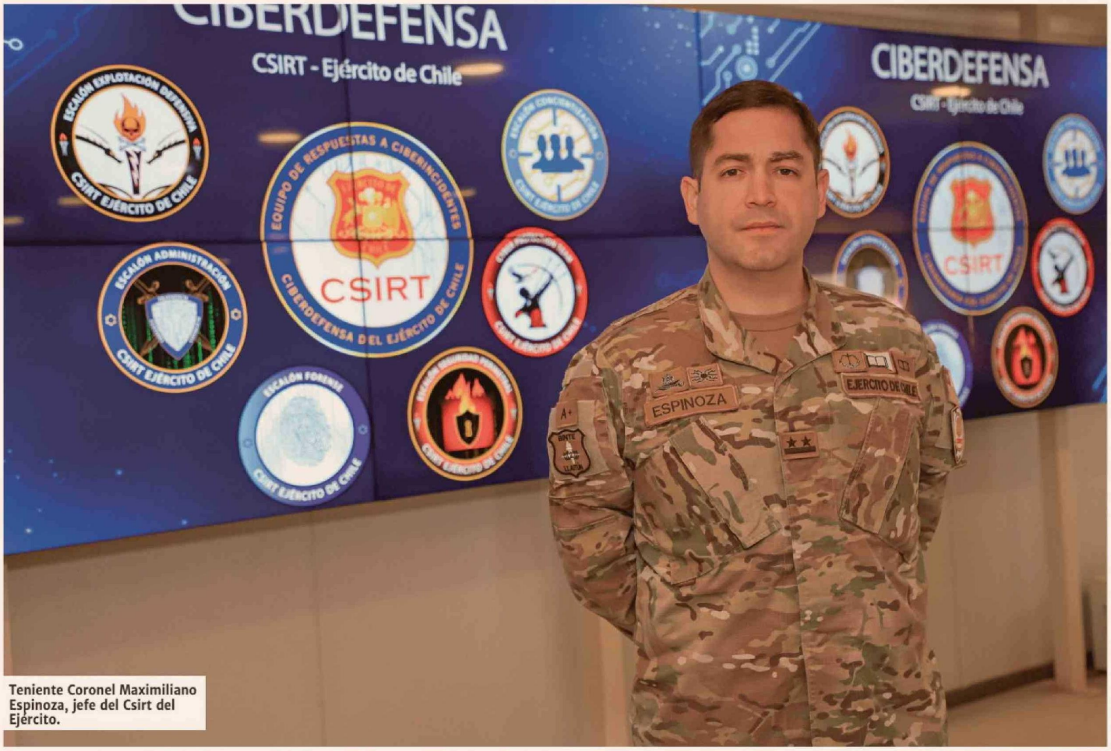
LITORALPRESS

Fecha: 02-03-2026
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: Cómo avanza el Ejército en ciberseguridad con redes seguras, sistemas de protección con IA y cifrado postcuántico

Pág. : 22
Cm2: 627,7

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

La institución trabaja en un modelo de lenguaje grande basado en código abierto para uso interno y tiene sus propios centros de datos para no depender de nubes externas.



Teniente Coronel Maximiliano Espinoza, jefe del Csirt del Ejército.

Cómo avanza el Ejército en ciberseguridad con redes seguras, sistemas de protección con IA y cifrado postcuántico

POR MARCO ZECCHETTO

El Ejército de Chile es uno de los 158 organismos del Estado designados por la Agencia Nacional de Ciberseguridad (ANCI) como Operadores de Importancia Vital (OIV) -claves para el funcionamiento del país- en un contexto de ciberamenazas cada vez más sofisticadas que incluyen, incluso, ataques a la infraestructura crítica potenciados con inteligencia artificial (IA).

Si bien la institución cuenta con una política estructurada de seguridad cibernética desde hace más de 10 años para resguardar sus sistemas críticos, las nuevas obligaciones derivadas de la Ley Marco de Ciberseguridad y del Reglamento de Ciberseguridad de la Defensa Nacional -que establecen, entre otros, deberes y plazos para reportar incidentes-, han llevado al Ejército a reforzar sus capacidades en este ámbito, con protocolos avanzados, redes seguras, tecnologías de protección de sistemas con IA y cifrado postcuántico, adelantándose a los nuevos desafíos que impone la computación cuántica.

Según el reglamento, el Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional (Csirt-DN), del Estado Mayor Conjunto -creado al alero de la Ley Marco de Ciberseguridad-, es el que entrega las directrices y coordina a los Csirt sectoriales, como el del Ejército. Estos últimos cumplen un rol operativo directo en la prevención, detección y respuesta de incidentes, en línea con las directrices y supervisión del Csirt-DN.

El Teniente Coronel Maximiliano Espinoza, jefe del Csirt del Ejército, dijo que para esta nueva etapa, la institución cuenta con un programa plurianual de financiamiento en ciberseguridad, que asegura recursos permanentes, para capacidades tecnológicas y continuidad operacional.

En ese contexto, destacó el proyecto "Ciberdefensa I" que contempla financiamiento a cuatro años y comenzará a ejecutarse en el segundo semestre de 2026. Esta iniciativa busca reforzar y consolidar las capacidades de ciberseguridad con la implementación de tecnologías avanzadas de monitoreo, análisis y correlación de ciberamenazas, además de protección perimetral de sistemas y redes.

"El financiamiento contempla la adquisición de hardware especializado, plataformas de seguridad, capacitación técnica y sostenimiento operacional durante el período definido", explicó el oficial.

Espinoza dijo que existe una planificación permanente y que las etapas siguientes profundizarán la "modernización tecnológica, automatización y resiliencia frente a amenazas emergentes, bajo esquemas plurianuales sucesivos".

Agregó que, a la fecha, han avanzado en diversos protocolos de comunicación y resiliencia en ciberseguridad. Esto incluye monitoreo continuo de redes y sistemas, clasificación temprana de eventos, aislamiento de activos comprometidos, y planes de recuperaciónante eventuales ciberataques. Estos se complementan con capacitación "activa" de los equipos.

Un modelo de IA propio

En enero de 2026 el Ejército comenzó a trabajar en un modelo de lenguaje grande (LLM) propio basado en modelos de código abierto de ChatGPT (OpenAI), con el objetivo de desarrollar e implementar capacidades de procesamiento local de IA. La herramienta está en fase de prueba y hace posible tareas como clasificar documentos secretos, apoyar la toma de decisiones, y analizar bases de datos, sin depender de nubes externas.

"Usamos el cerebro -los LLM- que liberan las compañías y desarrollamos el código conversacional, que permite generar el chat, la capa de personalización con el usuario (...) Al correr local, tenemos el control absoluto de las bases de datos, los *prompts* y las conversaciones que se manejan. No van a la nube externa, sino que son propiedad 100% del Ejército", explicó Espinoza.

Detalló que el proyecto "Ciberdefensa I" contempla la compra de "un pequeño data center" con unidades de procesamiento gráfico (GPU) y capacidad de procesar mayores volúmenes de datos para IA, lo que posibilitará el despliegue del modelo para uso de la institución "entre el segundo semestre de este año y principios de 2027".

El proyecto "Ciberdefensa I" comenzará a ejecutarse el segundo semestre de 2026 para desarrollar y consolidar las capacidades de ciberseguridad con la implementación de tecnologías avanzadas.

Protección con IA y redes

En la última década, el Ejército formalizó bajo estándares internacionales sus centros de operaciones de red (NOC) y centros de operaciones de seguridad (SOC) -cuyo rol es asegurar la disponibilidad de los servicios y la seguridad de sus sistemas- para fortalecer su arquitectura de supervisión y respuesta.

Entre las tecnologías de punta que ya han implementado, Espinoza destacó los "agentes de protección" de *endpoints* con IA que se despliegan en los computadores

LITORALPRESS

Fecha: 02-03-2026
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: **Cómo avanza el Ejército en ciberseguridad con redes seguras, sistemas de protección con IA y cifrado postcuántico**

Pág. : 23
Cm2: 281,5

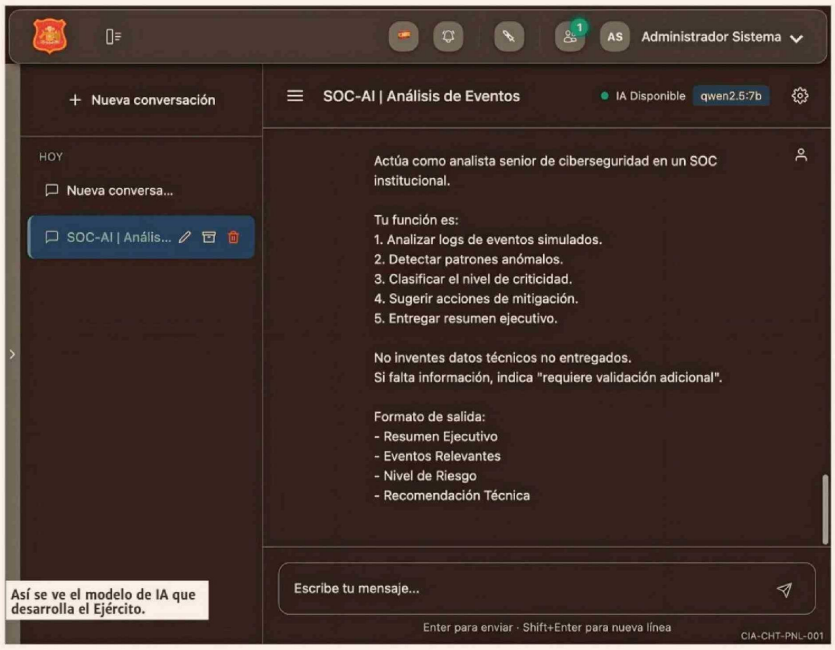
Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

con acceso a la red. Estos pueden ejecutar tareas preconfiguradas de forma automática, desde monitorear en tiempo real la actividad de los sistemas, detectar comportamientos anómalos y generar alertas.

"Por ejemplo, establecemos ciertos parámetros para que aprenda el comportamiento del usuario. Cuando detecta algo que no es normal actúa en forma autónoma para bloquear y proteger", dijo.

En conectividad, el Ejército opera con una Intranet propia a nivel nacional, para comunicarse de forma segura con todas las unidades a lo largo del territorio, y se apoya en "enlaces de microondas punto a punto y en comunicaciones satelitales" para asegurar la conectividad en zonas alejadas o de difícil acceso.

También trabaja con servicios externos para enlaces de internet y redes privadas, las que son administradas por la plataforma tecnológica SD-WAN que selecciona automáticamente "la mejor ruta disponible", según latencia, estabilidad y disponibilidad, "lo que permite mantener la continuidad y eficiencia del servicio", dijo Espinoza.



Así se ve el modelo de IA que desarrolla el Ejército.

Para proteger sus redes, además de cortafuegos, incorporaron equipos de cifrado que resguardan la información frente a accesos no autorizados, y utilizan tecnologías como ZTNA (Acceso a Red de Confianza Cero, en español), que integran controles de identidad y validación continua de usuarios y dispositivos.

El Ejército tiene su propia infraestructura de centros de datos.

Espinoza dijo que, para complementar los esquemas de criptografía tradicionales, desde hace "más de cinco años", trabajan en la anticipación de los futuros ataques de computadores cuánticos e integraron una capa de cifrado "de nivel estratégico" con tecnología postcuántica -basada en algoritmos complejos diseñados para resistir las amenazas de estos computadores-, la que se implementa en los enlaces troncales que interconectan los data centers de la institución.

Para las unidades desplegadas en el territorio nacional, la protección contempla "túneles seguros" -canales protegidos con cifrado avanzado- para asegurar la integridad y confidencialidad de las comunicaciones entre los usuarios finales y la red institucional.

"De esta forma, existe una capa de máxima seguridad entre los centros de datos y otra capa robusta de protección para las unidades operativas, lo que garantiza el resguardo de la información en todos los niveles", afirmó el Teniente Coronel Espinoza.