CNR refuerza su seguridad de TI con Kaspersky

CNR
Ministerio de Agricultura
Gobierno de Chile

CNR

kaspersky BRING ON THE FUTURE

La Comisión Nacional de Riego (CNR) de Chile se ha asociado con Kaspersky para mejorar la visibilidad del estado de sus equipos de TIC y reforzar su ciberseguridad interna.

La CNR promueve el desarrollo agropecuario de los agricultores, cultivadores y productores de Chile mediante financiamiento, desarrollo y transformación.

Servicio Público – Gobierno

- Chile, Sudamérica
- Uso de Kaspersky Endpoint Security Cloud Pro
- Atender una importante brecha de vulnerabilidad que amenazaba tanto al servicio como al Estado

220
usuarios en todo Chile

110.000m
de pesos en financiamiento anual

48
años de experiencia en la industria

- **Facilidad de uso**, excelente manejo de activos y soporte de proveedores
- **Gestión en la nube**, así que se centra en las directivas y es fácil de implementar
- La protección esperada **se cumplió al 100%** en todas las plataformas
- **Precios competitivos** y todos los ciberataques/incidentes bloqueados

"Confiamos en Kaspersky como socio directo por toda la protección y visibilidad que nos ha dado. Podemos dar seguimiento a los ataques, incidentes, la aplicación de parches y el bloqueo manual."

Sebastian Casabonne Vilches
Coordinador de la Unidad de Tecnología y Transformación Digital de la CNR

Acerca del cliente

Desde 1986, la CNR contribuye a la política nacional de riego de Chile y mejora la eficiencia de sus sistemas de riego, con especial atención a los productores en situación de vulnerabilidad, así como al continuo desarrollo de las regiones extremas del país. Lo hace a través de proyectos de desarrollo y transformación productiva, y promoviendo de la inversión privada en obras de riego y drenaje.

Desafíos

La CNR ha detectado una laguna de vulnerabilidad en sus sistemas que, a su juicio, debía atenderse con carácter urgente.

La brecha en cuestión se hallaba entre sus activos de TIC y la educación de sus empleados, lo que significaba que los informes diarios, las notificaciones y la ejecución de las actividades de actualizaciones se estaban parcheando para protegerse contra los ataques.

Antes de acercarse a Kaspersky, la CNR estaba empleando otra solución. La propuesta de renovación para esto era extremadamente alta y requeriría la adquisición de módulos de seguridad separados. El equipo optó por realizar un ejercicio de prueba de concepto con Kaspersky para ganar visibilidad y destacar el número de ataques contra la organización.

La CNR también quería visibilizar el estado de sus equipos TIC, así como reforzar su seguridad interna mediante la sensibilización, respaldada por políticas, decretos, instrucciones y buenas prácticas de ciberseguridad.

En concreto, quería que esto incluyera el control del acceso, la protección de datos, la respuesta a incidentes y la detección temprana de monitoreo. Necesitaba que todo fuera fácil de entender, tanto para el operador de las TIC como para el usuario final, todo ello con un alto nivel de soporte del socio en caso de que surgiera alguna duda, y todo ello a un coste razonable. La solución debía ser eficaz y fácil de entender, con apoyo complementario a lo largo de las fases de configuración y familiarización, y en adelante.

En última instancia, la CNR quería mejorar sus capacidades de inteligencia contra amenazas y, a través de un socio de ciberseguridad fiable, tener plena confianza tanto en su sistema como en la respuesta de sus empleados ante amenazas cibernéticas actuales y emergentes.

99% de tiempo de actividad
de la plataforma

24%
de ahorro de costos

0% de eventos materializados
ide ciberseguridad a través de EDR y Zero Trust

“Con la solución de Kaspersky Endpoint Security Cloud, hemos logrado gestionar la seguridad y vulnerabilidades de manera oportuna, enfocándonos en esta actividad relevante en la institución, lo que nos ha permitido mantener un total control de las actividades que suceden en la CNR.”

Nicolás Ignacio Cares Toro,
Infraestructura y Gerente de Operaciones de la Unidad de Tecnología y Transformación Digital, CNR

La solución de Kaspersky

Kaspersky le ofreció a la CNR una solución de ciberseguridad integrada de extremo a extremo. Implementó la solución de nivel empresarial Kaspersky Endpoint Security Cloud Pro en estaciones de trabajo, servidores y dispositivos móviles, cubriendo aproximadamente 300 licencias en total.

Kaspersky Endpoint Security Cloud Pro se eligió por su facilidad de uso y sus excelentes capacidades de administración de activos, lo que hizo que la experiencia del usuario fuera sencilla. Además, la CNR podía tener acceso al soporte técnico las 24 horas del día, los 7 días de la semana, gestionar todo desde la nube y operar dentro de su presupuesto.

- La CNR pudo sentar una base sólida para el futuro, con una continua ruta de actualización a EDR, protección de puertas de enlace y seguridad en la nube.
- Al reunir diferentes herramientas de seguridad en una sola solución, la CNR pudo maximizar tanto la eficiencia como la comodidad.
- Kaspersky Endpoint Security permitió que la CNR pudiera implementar un enfoque de protección de varias capas, basado en la tecnología de aprendizaje automático, y una excelente inteligencia de amenazas que cubría amenazas sin archivos, exploits, rootkits, por nombrar solo tres.

Protección
La CNR ahora puede detener amenazas que incluyen (pero no se limitan a) ransomware, ataques sin archivos, exploits, rootkits, virus y troyanos.

Eficiencia
El trabajo ahora se optimiza en una sola plataforma, utilizando herramientas automatizadas.

Flexibilidad
La CNR ahora tiene capacidades de seguridad de extremo a extremo que se implementan rápidamente y se pueden usar en cualquier plataforma, con toda su infraestructura existente.

Transparencia
La visibilidad que la CNR requería como prioridad es ahora una realidad. Puede acceder a revisiones del código del producto, actualizaciones y reglas de detección de amenazas, y monitorear las amenazas en tiempo real.

La implementación de Endpoint Security de Kaspersky le dio a la CNR una base segura para permitir y respaldar su transformación digital de una manera sólida y sencilla.

Habiendo implementado el bloqueo de unidades extraíbles de Kaspersky, Zero Trust, recomendaciones de panel, notificaciones, EDR, navegación segura para Windows, MAC y dispositivos móviles, la protección requerida se ha cumplido al 100%. La asociación en curso entre la Comisión Nacional de Riego de Chile y Kaspersky es de absoluta confianza.

Cyber Threats News: securelist.lat
IT Security News: business.kaspersky.com
IT Security for Enterprise: latam.kaspersky.com/enterprise

latam.kaspersky.com

kaspersky BRING ON THE FUTURE