Términos y Condiciones HackedAlert (v1.0)

1. Objetivo y Alcance

HackedAlert es una plataforma de inteligencia técnica (OSINT), cuyo objetivo es proporcionar acceso a información (datos y metadatos) indexada y recabada desde fuentes abiertas.

HackedAlert procesa y sirve una gran cantidad de información desde fuentes de acceso público, la plataforma actúa como un motor de búsqueda agnóstico frente a las tecnologías y el mercado en general.

2. Naturaleza y Tratamiento de la Información

Toda la información contenida y servida en la plataforma, es de dominio público. Sin embargo, los datos y metadatos son procesados, categorizados, correlacionados y enriquecidos con intersecciones relevantes de la industria, para facilitar su consumo, entendimiento, y reutilización comercial o técnica.

- **Origen de los Datos**: No almacenamos, procesamos y menos aún facilitamos el acceso a información proveniente de ilícitos, fugas de información, ataques de ciberseguridad, o cualquier tipo de dato o metadato de origen delictual.
- **Metodología de Indexación**: HackedAlert se limita exclusivamente a indexar metadatos técnicos que son expuestos de forma voluntaria y abierta por los sistemas indexados hacia Internet. La plataforma no realiza intentos de autenticación, no explota vulnerabilidades ni supera mecanismos de control de acceso (tales como firewalls, sistemas de autenticación o cifrado de extremo a extremo) para obtener la información indexada.
- **Fidelidad de los Resultados**: Para garantizar el cumplimiento de las legislaciones actuales, no se realiza ningún tipo de actividad autónoma o unilateral (ni antes, ni durante ni después de almacenar y servir la información desde la plataforma), para verificar técnicamente, la fidelidad científica de los resultados que se obtienen producto de la conciliación, por lo tanto, es probable que los datos y metadatos contengan errores, imprecisiones o una desactualización temporal.

- **Identificadores CVE y Pentesting**: La plataforma no ejecuta procedimientos de pentesting o cualquier otra actividad relacionada con la reproducción de vulnerabilidades informáticas o identificadores CVE, y tampoco proporciona herramientas, códigos o programas para probar identificadores CVE ni para realizar pentesting. La clasificación y correlación de información con identificadores CVE tiene un fin exclusivamente informativo y de visibilidad de la superficie de exposición técnica. Esta funcionalidad no constituye un medio facilitador para el acceso ilícito, toda vez que no proporciona exploits ni herramientas de ejecución, limitándose a reportar información de vulnerabilidades ampliamente difundida en bases de datos públicas de seguridad.
- **Exclusión de Responsabilidad Técnica**: Dado que no comprobamos la autenticidad técnica de los datos y metadatos por diseño, la plataforma se entrega "tal cual es" (as-is).

3. Privacidad y Datos Personales

HackedAlert opera bajo un modelo de privacidad y seguridad desde el diseño, limitando su recolección de datos estrictamente a información técnica de infraestructura expuesta públicamente, excluyendo la captación de datos personales que no sean estrictamente necesarios para la identificación técnica del activo. HackedAlert implementa procedimientos técnicos destinados a la anonimización de datos personales cuando corresponda, garantizando que el almacenamiento, tratamiento y divulgación de datos y metadatos se limite estrictamente a información de infraestructura técnica pública, y no a datos personales sensibles o privados.

- **Direcciones IP**: En cumplimiento con lo dispuesto en el Artículo 11, literal j) y Artículo 27 de la Ley N° 21.663, el procesamiento de direcciones IP realizado por la plataforma se limita exclusivamente a su función técnica como identificador de red, no siendo tratadas bajo la categoría de datos personales para efectos de esta regulación.
- **Activos de dominio**: Asimismo, conforme a la naturaleza técnica y operativa de los nombres de dominio, se declara que cualquier activo registrado bajo el TLD .cl, así como aquellos vinculados a organismos públicos (.gob.cl, .gov.cl, .mil.cl) y cualquier otro TLD genérico o territorial, junto con sus subdominios asociados, constituyen activos de carácter público; dichos elementos son gestionados bajo las reglas de asignación y registro de nombres de dominio, siendo información pública por su propia naturaleza operativa. En consecuencia, el procesamiento, indexación y correlación de tales nombres de dominio y sus estructuras jerárquicas (subdominios) no constituye sujeción al tratamiento de datos personales, al no vincularse, referirse ni permitir la identificación de una persona natural, quedando excluidos del ámbito de aplicación de la Ley N° 19.628 y sus modificaciones vigentes (Ley N° 21.719).

4. Derechos ARCOP y Transparencia

En cumplimiento de la Ley N° 21.719, HackedAlert reconoce el derecho de los titulares a ejercer las facultades de Acceso, Rectificación, Cancelación, Oposición y Portabilidad (ARCOP). Los usuarios o titulares cuyos datos personales (identificables) pudiesen estar indexados y disponibles para consulta en los resultados de búsqueda de HackedAlert, pueden ejercer estos derechos enviando una solicitud a contacto@wl-inc.cl, conforme al procedimiento establecido en el Artículo 11 de la Ley N° 19.628 (modificada).

5. Uso Responsable y Obligaciones del Usuario

El uso de la plataforma y su información para fines que contravengan las leyes N° 21.459, N° 21.663, N° 21.719, y N° 19.628, o cualquier legislación o normativa vigente de Chile, responsabiliza exclusivamente al usuario final por el uso que le dé a la inteligencia obtenida a través de HackedAlert.

- **Infraestructura Crítica**: Está estrictamente prohibido el uso de HackedAlert con el fin de identificar, enumerar y analizar infraestructura de servicios de utilidad pública o activos críticos definidos bajo la Ley Marco de Ciberseguridad (Ley N° 21.663) para la ejecución de ataques o interrupciones. HackedAlert declina toda responsabilidad sobre el uso no autorizado de su información para la afectación de dichos servicios estratégicos. HackedAlert no está diseñado, exclusivamente, para el monitoreo ni la vigilancia de infraestructuras críticas o servicios esenciales definidos en la Ley N° 21.663, y cualquier consulta realizada sobre dichos activos deberá ser ejecutada en cumplimiento estricto con las obligaciones de ciberseguridad sectoriales que correspondan al usuario.
- **Finalidad del Tratamiento**: El tratamiento realizado por HackedAlert tiene como finalidad exclusiva el análisis técnico de activos y la investigación de seguridad (OSINT), en el marco de un interés legítimo por dotar de visibilidad a la superficie de ataque pública, no siendo utilizados dichos datos para fines de mercadotecnia, perfilamiento de personas naturales o elaboración de perfiles.

6. Colaboración con la Autoridad y Protocolos

- **Cooperación Lega**l: HackedAlert colaborará, siempre, con las autoridades y la policía, frente a casos de delitos informáticos relacionados con el abuso o la mala utilización de la plataforma y su contenido.
- **Respuesta ante Vulnerabilidades**: En caso de que usuarios o terceros informen a HackedAlert sobre la detección de vulnerabilidades, HackedAlert se reserva el derecho de actuar conforme a los principios de respuesta responsable, pudiendo, a su discreción, canalizar dicha información a los dueños o responsables de los sistemas afectados, así como a las instituciones del Estado según corresponda, sin que esto constituya una asunción de responsabilidad sobre la veracidad del hallazgo.
- **Posicionamiento Legal**: HackedAlert no actúa bajo el régimen de "comunicación responsable de vulnerabilidades" previsto en el artículo 2° de la Ley N° 21.459, ya que no realiza actividades de escaneo intrusivo ni pruebas de vulnerabilidad. Consecuentemente, HackedAlert no se posiciona como una entidad de investigación de seguridad sujeta a las obligaciones de dicho cuerpo legal, sino como un servicio de indexación de información pública.
- **Gestión de Exclusiones**: HackedAlert actúa como un motor o buscador de datos de acceso público. Dada la naturaleza dinámica y constante de la indexación de fuentes abiertas, la plataforma no garantiza la eliminación permanente de activos, ya que estos pueden ser re-indexados automáticamente en procesos futuros. No obstante, HackedAlert respeta los protocolos técnicos estándar de la industria (tales como archivos robots.txt o meta-etiquetas noindex), los cuales son el mecanismo técnico reconocido para que los administradores de sistemas expresen su voluntad de no ser indexados por crawlers o bots. La implementación y el mantenimiento de dichas medidas técnicas son responsabilidad exclusiva del administrador del sistema. HackedAlert no ofrece servicios de gestión, limpieza o auditoría de activos a terceros, ni presta servicios de consultoría técnica para la exclusión de datos.

7. Planes de Suscripción

- **Planes de consumo**: HackedAlert proporciona planes de suscripción, los cuales podrán ser pagados mediante transferencia bancaria, depósito, y vía web con cargo automático a tarjetas de crédito y débito.
- **Características de los planes**: HackedAlert se reserva el derecho de agregar, eliminar y modificar los planes de suscripción, las características de los planes y sus alcances de servicio en la plataforma, de manera unilateral y sin aviso previo.
- **Pasarela de pago externa**: HackedAlert utiliza el servicio payment gateway de la empresa Mercadopago, sin embargo, este proveedor podrá ser reemplazado en cualquier momento y sin previo aviso.

8. Contacto

Frente a cualquier duda o requerimiento, puede tomar contacto con nuestro equipo utilizando el siguiente correo electrónico: contacto@wl-inc.cl.

Santiago de Chile, 26 de Mayo de 2026.