TECNOLOGÍA Y SERVICIOS
DE SEGURIDAD CIBERNÉTICA SA DE CV

Inteligencia de Amenazas

2023

AVISO DE CONFIDENCIALIDAD

ESTE MATERIAL FORMA PARTE DE LA OFERTA DE SERVICIOS DE CONSULTORIA DE SEGURIDAD DE LA INFORMACION PARA PROPORCIONAR SERVICIOS DE CONTEXTUALIZACION E INTELIGENCIA DE AMENAZAS, POR LO QUE SU CONTENIDO ES DE CARÁCTER CONFIDENCIAL Y ES PROPIEDAD DE TECNOLOGIA Y SERVICIOS DE SEGURIDAD CIBERNETICA S.A. DE C.V., EL EJERCICIO EXCLUSIVO DE LOS DERECHOS DE EXPLOTACIÓN DE LOS MISMOS EN CUALQUIER FORMA, Y EN ESPECIAL LOS DERECHOS DE REPRODUCCIÓN, DISTRIBUCIÓN, COMUNICACIÓN PÚBLICA Y TRANSFORMACIÓN. TODO ESTE MATERIAL ESTÁ PROTEGIDO POR LA LEGISLACIÓN DE LA PROPIEDAD INTELECTUAL Y SU USO INDEBIDO PUEDE SER OBJETO DE SANCIONES, INCLUSO PENALES.

AUTORIZACIONES:
EN NINGÚN CASO SE CONCEDE AUTORIZACIÓN PARA MODIFICAR EL MATERIAL QUE CONTIENE ESTE DOCUMENTO.

Contenido

Marco de Referencia

De acuerdo con la metodología de análisis y gestión de riesgos, MAGERIT V3. que define los Procesos de gestión de riesgos, se definirán en conjunto la criticidad de tópicos y hallazgos que se puedan obtener con el monitoreo objeto de la presente propuesta para

A la vista de los impactos y riesgos a que está expuesto el sistema, hay que tomar una serie de decisiones condicionadas por diversos factores:
• la gravedad del impacto y/o del riesgo
• las obligaciones a las que por ley esté sometida la Organización
• las obligaciones a las que por reglamentos sectoriales esté sometida la Organización
• las obligaciones a las que por contrato esté sometida la Organización
Dentro del margen de maniobra que permita este marco, pueden aparecer consideraciones adicionales sobre la capacidad de la Organización para aceptar ciertos impactos de naturaleza intangible tales como:
• imagen pública de cara a la Sociedad (aspectos reputacionales)
• política interna: relaciones con los propios empleados, tales como capacidad de contratar al personal idóneo, capacidad de retener a los mejores, capacidad de soportar rotaciones de personas, capacidad de ofrecer una carrera profesional atractiva, etc.
• relaciones con los proveedores, tales como capacidad de llegar a acuerdos ventajosos a corto, medio o largo plazo, capacidad de obtener trato prioritario, etc.
• relaciones con los clientes o usuarios, tales como capacidad de retención, capacidad de incrementar la oferta, capacidad de diferenciarse frente a la competencia, ...
• relaciones con otras organizaciones, tales como capacidad de alcanzar acuerdos estratégicos, alianzas, etc.
• nuevas oportunidades de negocio, tales como formas de recuperar la inversión en seguridad
• acceso a sellos o calificaciones reconocidas de seguridad
Todas las consideraciones anteriores desembocan en una calificación de cada riesgo significativo, determinándose si ...

1. es crítico en el sentido de que requiere atención urgente
2. es grave en el sentido de que requiere atención
3. es apreciable en el sentido de que pueda ser objeto de estudio para su tratamiento
4. es asumible en el sentido de que no se van a tomar acciones para atajarlo

La opción 4, aceptación del riesgo, siempre es arriesgada y hay que tomarla con prudencia y justificación. Las razones que pueden llevar a esta aceptación son:
• cuando el impacto residual es asumible
• cuando el riesgo residual es asumible
• cuando el coste de las salvaguardas oportunas es desproporcionado en comparación al impacto y riesgo residuales

La calificación de los riesgos tendrá consecuencias en las tareas subsiguientes, siendo un factor básico para establecer la prioridad relativa de las diferentes actuaciones.

Descripción de las soluciones que componen el servicio

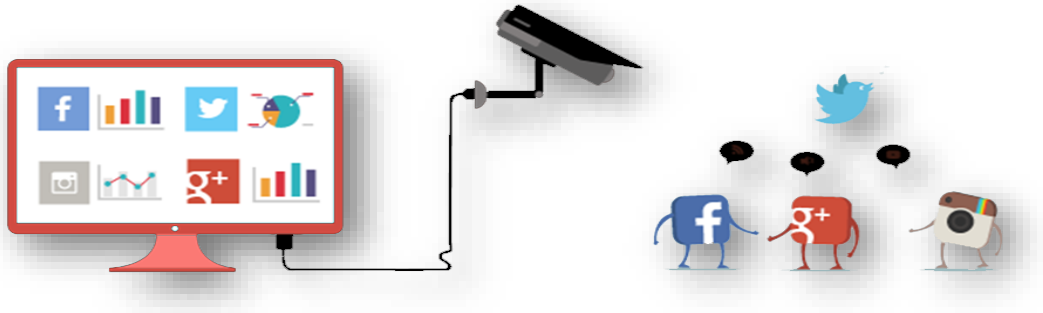
1. Public Intelligence (Plataforma de Ciber Patrullaje de Clear web)

Contamos con una de las soluciones más completa del mercado para minería de datos basada en OSINT (Open Source Intelligence) con acceso desde una plataforma web, para medir el comportamiento de millones de ciber-usuarios que habitan en internet, los cuales integran un sistema social conductivo que opina, piensa y desea.

La importancia del funcionamiento de la solución radica en la capacidad de visualizar desde Internet, la pluralidad de opiniones, gustos, geografías, géneros, sentimientos, y comportamiento de los individuos, permitiéndonos tener la capacidad de vincular, analizar conceptos y segmentar criterios creando universos específicos de investigación y monitoreo continuo, los cuales pueden ser utilizados para distintos fines, que van desde una aplicación Mercadológica hasta llegar a investigaciones de inteligencia.

Gracias a estas propiedades de la solución, podemos tomar medidas de estrategia en función a los siguientes principios:

- ✓ Prevención
- ✓ Acción
- ✓ Corrección



En Public Intelligence es posible desarrollar estrategias de forma precisa, de acuerdo con la información que se determine o a través de diversas fuentes de extracción, que incluyen:

- Redes sociales
- Foros
- Noticias
- Fuentes con acceso controlado

MONITOREO ONLINE

- ✓ Seguimiento a tiempo real de imagen y reputación.
- ✓ Prevención y detección temprana de crisis de reputación.
- ✓ Análisis de la polaridad de las conversaciones, sentimiento (positivo, negativo neutral).
- ✓ Comparativa de la Reputación Online propia frente a la competencia

SOCIAL LISTENING

- ✓ Escucha activa en Social Media de marcas, tópicos, campañas, acciones y más.
- ✓ Social Analytics: Métricas de perfiles propios y de la competencia.
- ✓ Hashtags Tracking: Seguimiento y medición de Hashtags.
- ✓ Detección de tendencias e identificación de "Influencers".

Esto se logra con potentes motores de búsqueda rastrean la información en millones de sitios web de todo el mundo, como Redes Sociales (Facebook, Twitter, Instagram, YouTube, etc.), prensa online, blogs, foros y más.

Seguimiento a incidencias

- ✓ Análisis semántico de la pluralidad de menciones encontradas
- ✓ Obtención de Insights relacionados con motivaciones, ocasiones atípicas, factores de inhibición, etc.
- ✓ Estudio de las tendencias por cadenas de búsqueda a partir de las coincidencias encontradas.
- ✓ Análisis agrupados por filtros o reglas específicas.

A. Funcionalidades y características gráficas del tablero de monitoreo de Public Intelligence.

- Alertas

  Genera alertas en tiempo real de acuerdo con los criterios de búsqueda.

- Flexibilidad

  Utiliza potentes filtros o crea reglas y etiquetas automáticas para segmentar y clasificar la información en base a distintos parámetros.

- Alcance

  Rastreamos información en más de 70 millones de fuentes en 25 idiomas.

- Facilidad

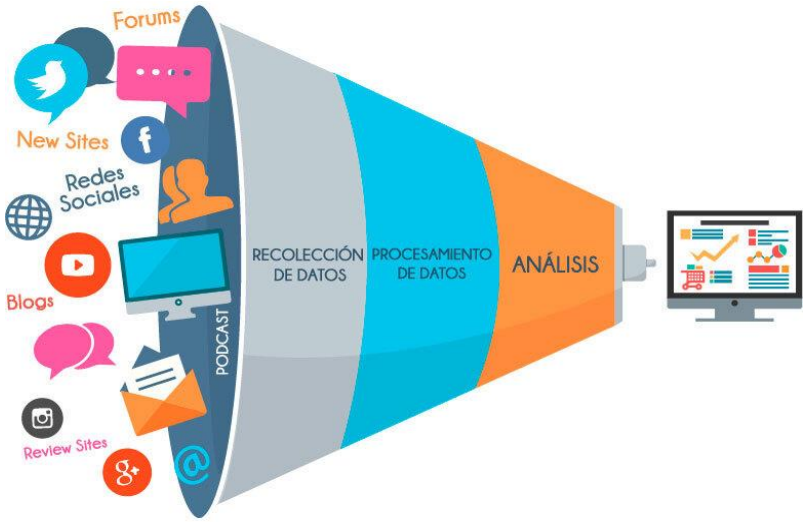
  A diferencia de otras herramientas, está diseñada para ser totalmente intuitiva y fácil de usar.

- Visual

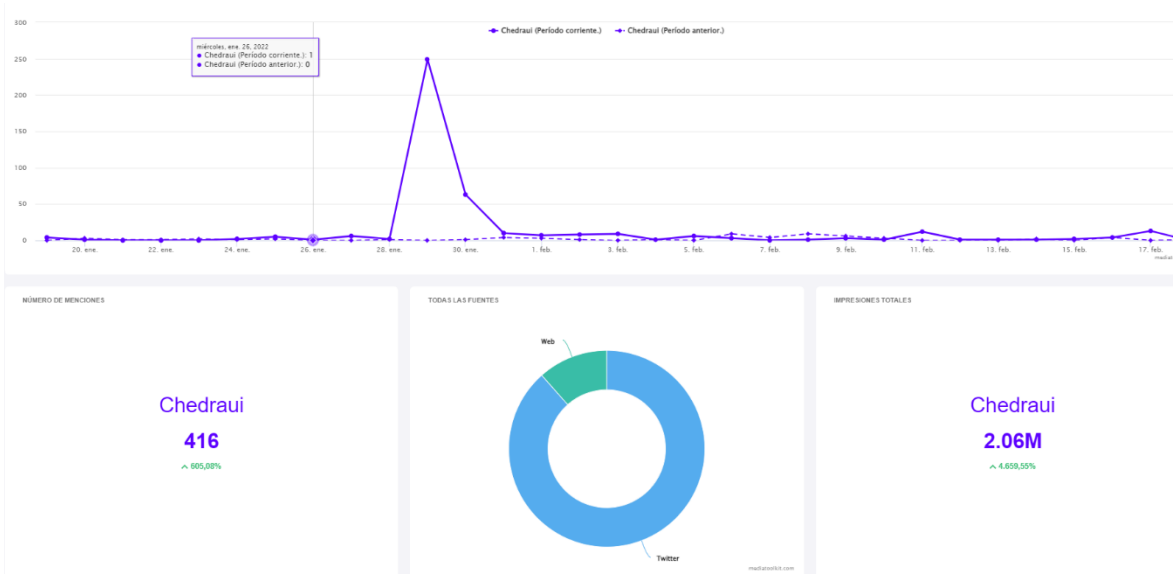
  Crea y descarga tableros de control personalizados con el resto del equipo.

- Versatilidad

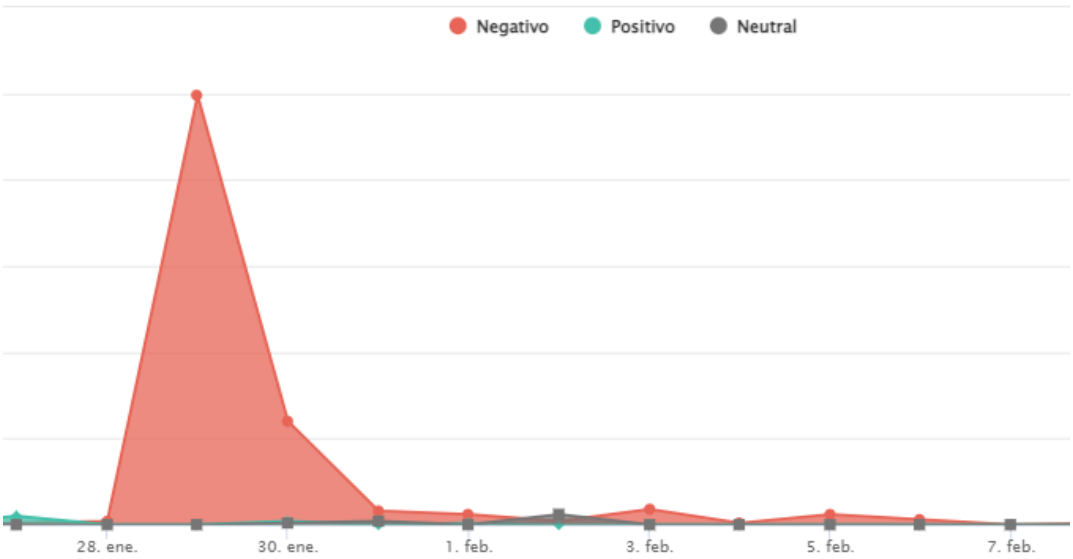
  Obtén métricas avanzadas de la presencia y actividad de cualquier palabra o tópico en internet.



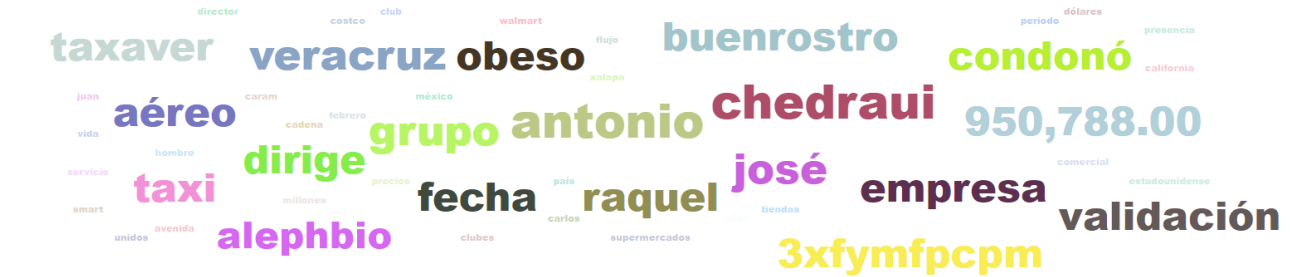
- Visualización de volumetría en el tiempo.



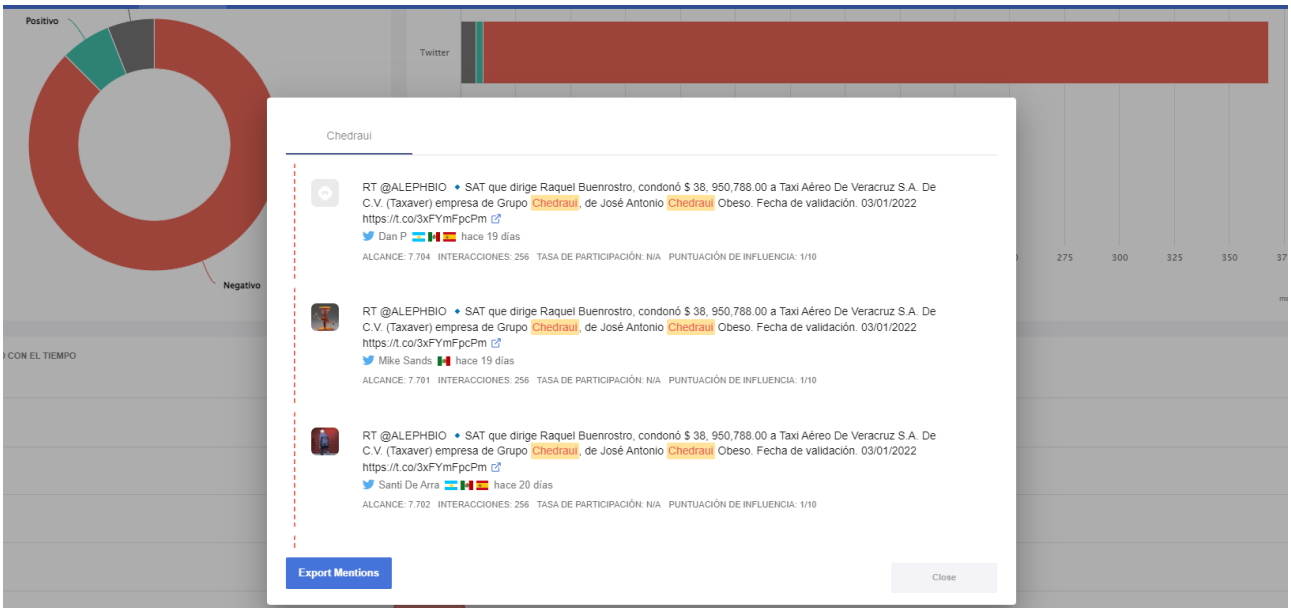
- Visualización de sentimiento en la volumetría.



- Nubes de tópicos



- Detalle de las publicaciones.



2. Site Takedown

La velocidad es esencial en cada caso, se debe bajar rápidamente el contenido robado o doloso.
Cuanto menos tiempo pase dicho contenido en un sitio de robo, mejor.
Por muchas razones. sabemos que eliminar rápidamente este contenido es relevante y de vital importancia. Todos nuestros casos de eliminación utilizan códigos de fecha y hora para el seguimiento del proceso.
Con la experiencia viene el conocimiento. La experiencia de eliminación de casos significa que nuestro equipo conoce el camino más rápido para eliminar el contenido robado y dejar antecedente con las instituciones especializadas en la procuración de justicia o regulación de contenido facilita la acción en futuras reincidencias.

Contamos con la definición de procesos y procedimientos de manejo de casos y hemos creado un sistema de manejo de solicitudes de eliminación con los canales oficiales e instancias reguladoras que aceleran el proceso de eliminación de contenido más eficiente, rápido y efectivo.

Entre otras cosas se busca evitar:

- Uso ilegitimo de marcas registradas
- Difamación o perjuicio a la marca o imagen corporativa
- Contrademandas pendientes
- Difusión de información falsa o de uso exclusivo interno.
- Difusión de información confidencial corporativa

Requisitos por solicitud.

- Se debe definir la proporción de la información de la que se solicita la baja. (URLs, Contenido de reportajes, descripciones dolosas, imágenes o audios)

- La información a bajar debe tener sustento legal de acuerdo a las leyes mexicanas o marcos de referencia internacionales (leyes de Propiedad intelectual, propiedad industrial, Ley federal de protección de datos personales en posesión de particulares, ley federal de protección de datos personales en posesión de obligados solidarios, derecho ARCO, misoginia, racismo, violencia, odio)

- Dependiendo del país en que se encuentre hospedada la información, podrán variar los periodos de tiempo de respuesta a las solicitudes y las leyes que aplican a dicha información.

- La información que no reúna estas características legales, no podrá ser bajada o "desplublicada" de no llegar a acuerdo consensual con el autor.

- Los acuerdos consensuales con los autores pudieran incurrir en costos adicionales a los descritos en esta propuesta.

3. Monitoreo de Exposición en Deep Web y Dark Web

Parte importante del servicio es el monitoreo de exposición de las personas de interés, mediante el cual se verifica la exposición al público de información personal de empleados, VIPs, PoI´s (Person of Interest) y cuentas de correo del dominio del cliente.

Este monitoreo permite verificar si su información personal, como direcciones de correo electrónico o contraseñas, ha sido comprometida en violaciones de datos conocidas además de realizar un seguimiento a la exposición de cuentas individuales, contraseñas con alto impacto al negocio y daño a la marca por mal uso de recursos de la empresa.

NOTA IMPORTANTE: El servicio solo muestra información sobre violaciones de datos conocidas y divulgadas públicamente. Es posible que existan otras violaciones de datos que aún no se hayan descubierto o revelado

Niveles de Servicio de detección y recuperación de menciones y publicaciones.

- Recuperación de las menciones 30 días previos al inicio del servicio y publicaciones de hasta 5 tópicos con retención de hallazgos por hasta 6 meses de antigüedad.

- Presentación de las menciones y publicaciones de los tópicos de interés de hasta 1 mes de antigüedad en tablero operativo con recuperación de menciones y publicaciones inmediata.

- Detección de las menciones recientes en menos de 1 hora posteriores a la publicación en redes sociales y fuentes abiertas.

Sitios WEB	SLA
Zona México o Estados Unidos	72 horas
Resto del Mundo	5 a 15 días hábiles
Reportajes en medios	**SLA**
México y Estados Unidos (Sujeto a sustento legal)	3 a 15 días hábiles
Resto del mundo	5 a 15 días hábiles
Redes Sociales	**SLA**
Publicaciones en Redes sociales (Sujeto a sustento legal): -Twitter -Facebook -TikTok -Instagram	5 a 8 días hábiles