Big Data,

gran aliado contra el fraude bancario

gmv
INNOVATING SOLUTIONS

Este es un documento producido por

www.ituser.es
www.itreseller.es

Accede a nuestras publicaciones digitales

CÓMO USAR ESTE DOCUMENTO

Con el fin de obtener la mejor experiencia de uso de esta revista, es **imprescindible** seguir estos sencillos pasos que te indicamos a continuación:

Paso 1. Asegúrate de disponer de las versiones más actualizadas de Adobe Reader y Flash Player. Si no las tienes instaladas, puedes descargarlas aquí:

Adobe Acrobat Reader y Adobe Flash Player

Paso 2. Accede al enlace de descarga y la publicación se abre en el visor del navegador.

Paso 3. Busca la opción guardar como que, dependiendo del navegador que utilices, podrá ser un icono o estar incluída en la barra de menú, y guarda la revista en la carpeta donde almacenes los documentos en tu equipo.

Paso 4. Accede a dicha carpeta y usa el botón derecho del ratón para hacer clic en el fichero de la revista.

Paso 5. Selecciona Adobe Reader como aplicación predeterminada para abrir este tipo de documentos.

Paso 6. Una vez abierta la revista, habilita la visualización a pantalla completa, y puedes iniciar la lectura de la revista con todas las capacidades interactivas disponibles.

GMV integra una solución que se enfrenta al fraude bancario desde todos los ángulos

Big Data, un gran aliado contra el fraude bancario

La Transformación Digital de la Banca ha generado, y seguirá generando, múltiples beneficios tanto para las entidades como para los clientes. Sin embargo, también ha provocado que estas entidades estén más expuestas a los ciberataques. De hecho, la mitad de los ataques en nuestro país afectan al sistema financiero.

Al tratarse de una temática delicada, no es fácil saber la cantidad exacta que supone el fraude en el sector, pero, según el 4º Informe sobre Fraude en Tarjetas de Crédito del BCE, que incluye cifras hasta 2013, dentro del territorio SEPA, el fraude en tarjetas fue en ese año 2013 de 1.440 millones de euros, es decir, creció un 8% frente a 2012. Por tipo de delito, descienden los fraudes en cajero y punto de venta, y aumentan por CNP (Tarjeta No Presente, Card No Present) hasta suponer un 66% del total.

Esta evolución no solo es por el incremento de volumen del comercio electrónico, sino también por el hecho de que los ciberdelincuentes usan cada vez técnicas más sofisticadas, tanto en ingeniería social (phishing)

Detección rápida y respuesta son las claves para una nueva aproximación proactiva a la seguridad, en vez de reactiva

como en tecnología. Se suma a esto que los márgenes de la Banca son cada vez más ajustados (crisis económica/financiera, competencia de las FinTech, incremento de costes regulatorios, …). La consecuencia es que los efectos económicos del fraude tienen un impacto significativo en la cuenta de resultados de un banco. Y, cómo no, también tiene un claro impacto en la imagen de la entidad y en la confianza demandada por los clientes, tanto empresariales como particulares.

Al margen de los motivos anteriormente citados, los bancos tienen que vigilar por, y cumplir, un creciente número de regulaciones y normativas, para combatir cuestiones como el blanqueo de dinero o la financiación de grupos terroristas y del crimen organizado.

En definitiva, los vectores anteriores, incremento del número de ciberataques al sector financiero, y la sofisticación de los mismos; la reducción de márgenes del negocio, haciendo que el fraude empiece a tener un impacto no despreciable en la cuenta de resultados; el impacto del fraude en la reputación de un banco y la creciente regulación (mecanismos de control) para combatir el blanqueo del dinero y financiación del terrorismo y crimen organizado, hacen que exista una creciente necesidad de combatir el fraude bancario.

Aunque, eso sí, la necesidad de inversión en seguridad no es un problema exclusivo de la Banca, y, según un informe reciente de Gartner, en el año 2020 el 60% del presupuesto de los sistemas de información de la empresa se destinará a políticas de detección rápida y respuesta ante incidentes de seguridad. En 2013, esa cifra era tan solo del 10%.

Detección rápida y respuesta son las claves para una nueva aproximación proactiva a la seguridad, en vez de reactiva (como venía siendo en el pasado). Sirva como ejemplo otro reciente estudio del Instituto de Estudios Bursátiles, donde se destaca la necesidad de un enfoque proactivo en materia de seguridad, y disponer de las alianzas estratégicas adecuadas, socios tecnológicos que proporcionen la parte de inteligencia de la seguridad.

En este entorno, la propuesta de GMV pasa por tecnología contra el fraude, una aproximación proactiva y reactiva (para abordar esta problemática de forma completa), y apostando por la agilidad en la respuesta. Así, a las soluciones tradicionales para hacer frente al fraude, ahora se quiere aprovechar tanto Big Data como Inteligencia Artificial, creando un repositorio de información de fraude y explotándolo, con el objetivo de reforzar la solución que permite expandir y complementar los SIEM (Security Information and Event Management) tradicionales.

Los clientes ante la problemática del fraude bancario

Ángel J. Gavín Alarcón, Project Manager de GMV Secure e-Solutions, nos explica cómo afrontan los clientes el fraude bancario y cómo les ayuda en esta tarea un socio como GMV.

Tal y como nos explica Ángel J. Gavín, "depende mucho de la realidad de cada banco, destacando los mercados en los que opera y el estado de sus sistemas de la información. Algunos optan por soluciones orientadas a tipos concretos de fraude, mientras que otros abordan el problema desde una estrategia global. Los que adoptan una estrategia global apuestan por equipos de lucha contra el fraude especializados, con perfiles multidisciplinares como ciberseguridad, analistas y científicos de datos. Disponen de un backoffice de fraude avanzado, en el que las herramientas de Business Intelligence y Big Data son clave en la lucha contra el fraude. Un datawarehouse de fraude ayuda a la consolidación y tipificación de las cifras del mismo. Esto permite a la organización conocer el impacto del fraude en el banco y las medidas que deben adoptarse, a nivel táctico y estratégico, para mitigar el fraude. Yendo a soluciones especializadas en combatir diferentes aspectos del fraude, uno de nuestros productos estrella es *checker,* que cumple ahora 10 años. *Checker* está especialmente diseñado para sistemas de autoservicio financiero, estando desplegado en más de 120.000 cajeros automáticos de todo el mundo. Asegura en el cajero un entorno de alta seguridad contra ataques software, y alerta inmediatamente de cualquier intento de fraude".

"Para detectar el fraude en tarjetas de crédito", continúa, "disponemos de herramientas de scoring del riesgo de operaciones con tarjeta. Lo mismo sucede para la detección del fraude en origen, como la solicitud de créditos bancarios: se analizan los datos del cliente y la solicitud, y se alerta en caso de que exista riesgo de fraude o impago. Todo ello cruzando información y usando una combinación de reglas de negocio y algoritmia avanzada. Tenemos una suite muy amplia de productos que incluye herramientas de gestión de vulnerabilidades de los diferentes canales (*gestvul*), la gestión del derecho de acceso a la información (*arkano*) o la cibervigilancia, buscando información sensible publicada en redes anónimas y P2P (*atalaya*)".

Estrategia de GMV en este segmento

Tal y como nos comenta nuestro interlocutor, "evidentemente la Banca (como las compañías aseguradoras) sabe de la importancia de protegerse contra el fraude. Sin embargo, esta función no siempre está clara dentro de la organización, sino que recae en varios departamentos. Y eso suele ser un problema. En GMV tene-

ÁNGEL J. GAVÍN ALARCÓN, PROJECT MANAGER DE GMV SECURE E-SOLUTIONS

CLICAR PARA VER EL VÍDEO

mos una visión holística de la lucha contra el fraude que se apoya en 4 pilares básicos: proactividad, agilidad, recursos y tecnología. Tradicionalmente, en materia de fraude, se ha adoptado una posición reactiva: respondo cuando me defraudan, intento resolver la situación y voy adaptando mis sistemas para que eso no ocurra más. Sin embargo, en GMV apostamos por la proactividad: intentamos adelantarnos al fraude, identificando una estrategia y operativa, protegiendo los activos, detectando el fraude cuando sucede, y respondiendo ante el mismo. Por último, si se ha consumado, tratar de recuperar el dinero defraudado o los sistemas y servicios afectados".

Asimismo, añade que "la agilidad es esencial. Los defraudadores cada vez utilizan métodos más sofisticados y la respuesta debe ser lo más rápida posible. No solo en la parte de detección, sino también en las de protección, respuesta y recuperación. Lo cual nos lleva a los otros dos pilares: recursos y tecnología. La agilidad en la respuesta solo es posible con equipos multidisciplinares y la más alta tecnología. Ambos son inseparables. Si no se dispone de soluciones tecnológicas avanzadas, estamos poniendo una alfombra roja a los defraudadores. Pero las herramientas solas no sirven. Es necesario disponer de equipos que operen las herramientas, que recojan y analicen los resultados, actuando adecuadamente".

"Big Data, como herramienta contra el fraude aporta todas las ventajas del mundo: desde estratégicas a tácticas y operativas"

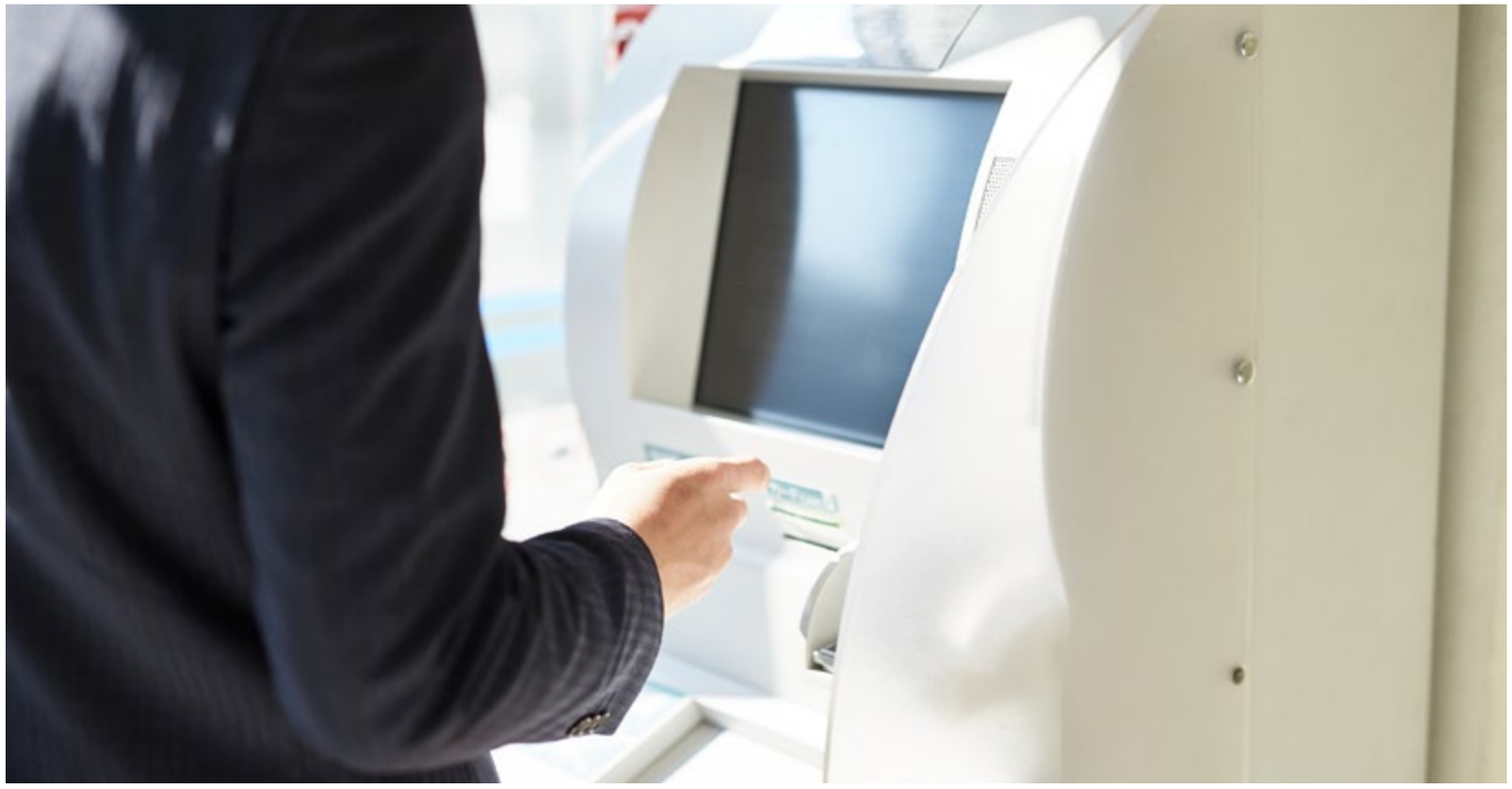
"GMV puede aportar, y aporta", finaliza, "expertos en fraude y ciberseguridad a los equipos de nuestros clientes. Con todo, nuestra oferta tecnológica es altamente diferenciadora y apuesta, como hemos visto antes, por dos grandes piezas para el puzle de la lucha contra el fraude. Por un lado, disponer de sistemas de backoffice que permitan determinar, caracterizar y combatir el fraude. Por otro, herramientas específicas para cada tipo de fraude, dentro del esquema de identificar/proteger/detectar/responder/recuperar".

Big Data como mecanismo contra el fraude

Big Data, como herramienta contra el fraude aporta, según este responsable, "todas las ventajas del mundo: desde estratégicas a tácticas y operativas. Recordemos la famosa cita de Deming: 'Creemos en Dios; todos los demás, traigan datos'. Porque es el dato el que permite tomar las decisiones correctas en todos esos planos. Por ejemplo, la vigilancia de infraestructuras y empleados, para detectar actividad sospechosa, se está beneficiando del Big Data. Para uno de nuestros clientes procesamos más de 500 millones de líneas de logs diarias de diferentes elementos de seguridad para dar respuesta a diversos casos de uso. Entre ellos, la vigilancia de actividad de antiguos empleados, la caracterización de usuarios internos en función de su actividad y la navegación en redes TOR, por citar algunos ejemplos".

"Si juntamos Big Data con Inteligencia Artificial", continúa, "las posibilidades se amplían enormemente. Por ejemplo, somos capaces de detectar nuevos patrones de fraude. Actualmente, la detección del fraude se basa en reglas de negocio conocidas por los expertos. Por ejemplo, si en el intervalo de, digamos, una hora, se produce un pago con tarjeta en dos comercios físicos que se encuentran a cientos de kilómetros, resulta "sospechoso". Hay otras reglas que no lo son tanto, y para ello podemos recurrir a técnicas de Machine Learning. Afortunada y desgraciadamente los bancos son grandes generadores de datos. La diversidad y heterogeneidad de esos datos necesita de arquitecturas de Big Data eficientes y pensadas para los casos de uso que se puedan prever. Una vez hecho esto, una vez que los datos están disponibles en estas arquitecturas, la agilidad a la hora

Big Data, gran aliado contra el fraude bancario



de implantar múltiples casos de uso de caracterización, detección y prevención del fraude es una realidad".

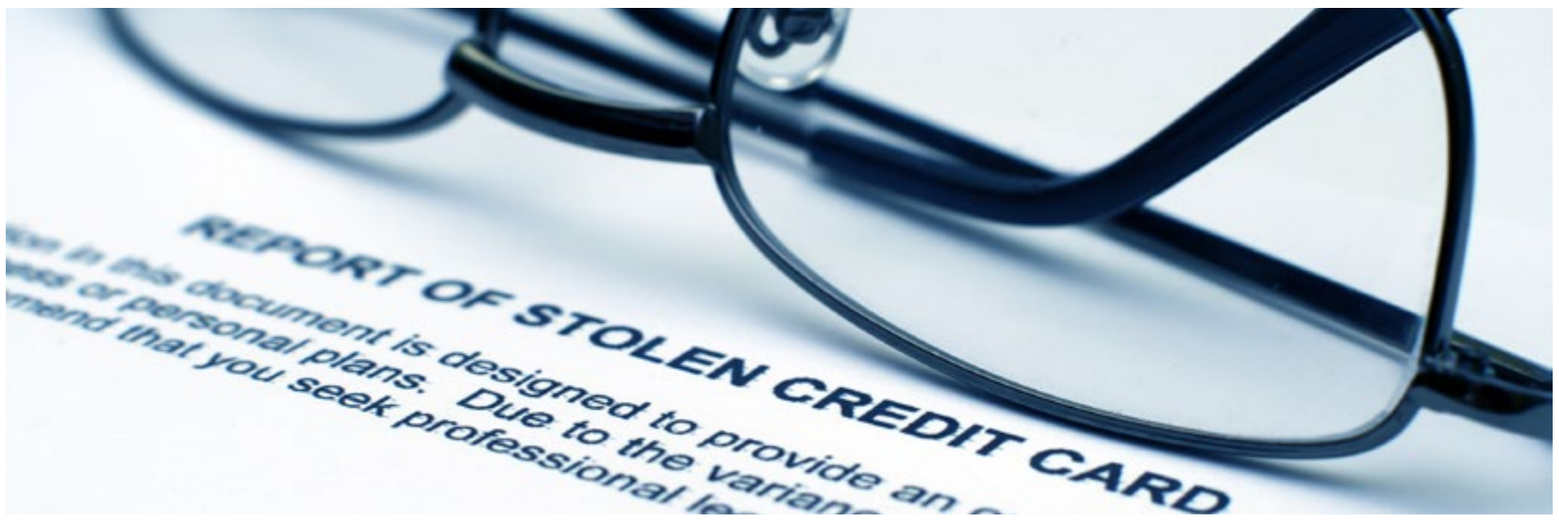
Pero, ¿y si una empresa quiere beneficiarse de esta visión? Para Ángel Gavín, "todo depende del nivel al que quiera entrar a combatir el fraude. Desde nuestra experiencia con Big Data (no solo en el sector bancario) es importante ayudar a determinar el Retorno de la Inversión (ROI) en materia de lucha contra el fraude. A partir de ahí, hay que analizar los casos de uso que se quieren resolver y las fuentes de información disponibles. Tenemos una amplia experiencia en montar arquitecturas de Big Data y en la propia recogida de datos. Pero no nos quedamos ahí. Disponemos de modelos de datos de fraude que normalizan la problemática del fraude, incluso cuando el banco opera en diferentes países. Y somos capaces de desplegar todo tipo de análisis que den respuesta a los casos propuestos".

"Un ejemplo paradigmático es el SIEM de nueva generación que hemos desplegado en uno de nuestros clientes para la monitorización de la actividad de recursos y empleados", finaliza. "Conocemos la problemática y las reglas, por lo que el despliegue es relativamente rápido, dependiendo de la disponibilidad y accesibilidad de los datos requeridos. Y, por supuesto, toda la suite de productos contra el fraude que se han mencionado anteriormente. En cualquier caso, el ROI que están observando nuestros clientes es la mejor justificación de que nuestra aproximación, trabajando codo con codo con ellos, aporta enormes beneficios".

La Banca, uno de los sectores punteros en Transformación Digital

Ciberseguridad frente al fraude financiero

La propuesta de GMV en el área de la ciberseguridad cuenta con una serie de servicios gestionados, así como una serie de productos específicos para problemas concretos. Conozcámoslos.



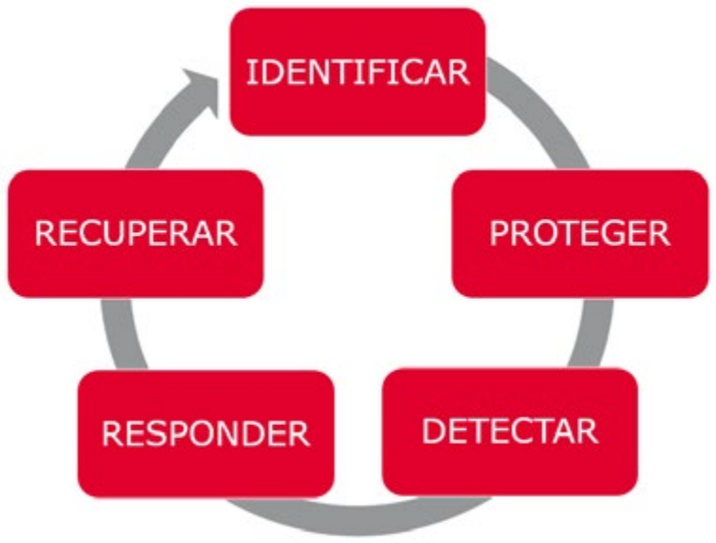
GMV cuenta con un Centro de Servicios Gestionados con prestación remota 24x7, con los recursos hardware, software y comunicaciones requeridos para dar una solución multi-tecnología, acorde con la demanda heterogénea de sus clientes, proporcionando los servicios de: Monitorización, Vigilancia Digital, Gestión de Vulnerabilidades, Gestión de Incidencias y Gestión de Evidencias.

Además, ofrece otra serie de servicios, análisis y diagnósticos, despliegue e integración de soluciones tecnológicas, y mantenimiento y mejora de los niveles de servicio, dentro de lo que podríamos denominar, segu-

MISIÓN DE GMV EN LA LUCHA CONTRA EL FRAUDE

- **Ponemos a disposición de nuestros clientes la más alta y avanzada tecnología contra el fraude, siempre dirigida por nuestros conocimientos del negocio bancario y su contexto.**
- **Apostamos por una aproximación proactiva y reactiva, abordando el fraude bancario en todas sus formas.**
- **Consideramos la agilidad en los procesos una pieza fundamental de nuestra oferta: capacidad rápida de respuesta, pero también de adaptación a un medio en constante cambio, con nuevas formas de fraude, actores y tecnologías.**

Big Data, gran aliado contra el fraude bancario



GMV ha desarrollado el SIEM de Nueva Generación SIEM_NG, aprovechando la enorme experiencia acumulada en materia de ciberseguridad y know-how en proyectos Big Data. Dicho SIEM dota a la empresa de una capacidad predictiva de eventos que pueden comprometer la seguridad de una organización. No excluyen ni reemplazan los SIEM actualmente en el mercado (ArcSight SIEM de HP, QRadar, Splunk, LogRhythm...), los complementa con capacidades predictivas y analíticas avanzadas. Puedes leer más aquí

ridad operativa. Si hablamos de seguridad de la información, los servicios ofrecidos serían sobre gestión de riesgos, cumplimiento de las normativas, y planificación y gestión de la seguridad.

Soluciones tecnológicas

Las principales soluciones de GMV son:

- *Checker* es un producto de seguridad para sistemas de autoservicio financiero. Protege desde hace ya 10 años más de 120.000 cajeros en cerca de 35 países de todo el mundo. *Checker* ofrece protección sin consumir recursos, sin afectar a su disponibilidad y siendo completamente independiente del fabricante del equipo en el que se instale.
- *Atalaya.* GMV monitoriza diversas fuentes, en modalidades de 8x5 o 7x24, con el objetivo de identificar información que permita detectar publicaciones accidentales o premeditadas que puedan suponer un riesgo a la Organización o un perjuicio a su imagen. Actividades como fuga de información, suplantación de identidad, ataques organizados, constatación de actividades fraudulentas, espionaje industrial, ATP, phishing, pharming, spam, información obtenida a través de ataques contra la organización, credenciales de usuarios en los diferentes servicios de la Organización... son detectadas por este servicio.
- *Gestvul.* La detección y posterior gestión de las vulnerabilidades tecnológicas se ha convertido en uno de los procedimientos de seguridad más efectivos en la lucha contra los incidentes de seguridad. En este sentido, cualquier entidad que realiza análisis de vulnerabilidades se encuentra

CLICAR PARA CONOCER LA PROPUESTA DE GMV EN CADA UNA DE ESTAS ÁREAS

Big Data, gran aliado contra el fraude bancario

NECESIDAD DE COMBATIR EL FRAUDE

- **Incremento del número de ciberataques al sector financiero y la sofisticación de los mismos.**
- **La reducción de márgenes del negocio, haciendo que el fraude empiece a tener un impacto no despreciable en la cuenta de resultados.**
- **El impacto del fraude en la reputación de un banco.**
- **La creciente regulación (mecanismos de control) para combatir el blanqueo del dinero y financiación del terrorismo y crimen organizado.**

con que una vez obtenidos los resultados, hay que realizar tareas adicionales como distribución de resultados, descarte de falsos positivos, soporte y verificación de la resolución y evolución del estado de seguridad.

- *Arkano*. Solución que gestiona el derecho de acceso a la información almacenada en formato digital, incluyendo cifrado de correo electrónico, protección de documentos (Office y PDF), protección de páginas Web y protección de almacenamiento (cualquier formato almacenado en la nube). Revolucionaria frente a productos presentes en el mercado por su simplicidad, no requiere instalación de certificados, ni software específico de descifrado, ni es necesario pre-registro de usuarios. El cifrado se realiza "extremo a extremo", sin que ningún intermediario o administrador de sistemas pueda acceder a los datos.

Enlaces relacionados

- Soluciones de Ciberseguridad de GMV
- Checker
- Gestvul
- Arkano
- Atalaya