LA INNOVACIÓN Y LA CIBERSEGURIDAD REVOLUCIONAN EL NEGOCIO DE LOS ABOGADOS

La Transformación Digital y sus retos en el sector legal

gmv
INNOVATING SOLUTIONS

LA TRANSFORMACIÓN DIGITAL AVANZA EN EL SEGMENTO JURÍDICO

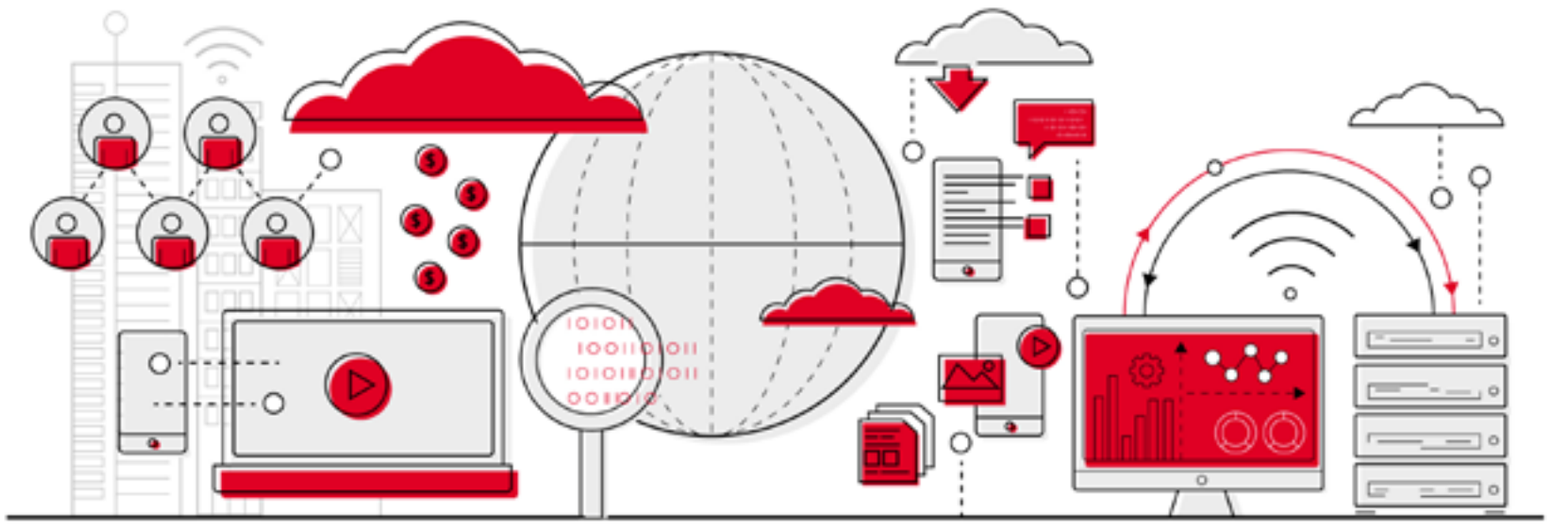
Ciberseguridad para el mundo legal

A la vez que el uso de la tecnología nos permite alcanzar nuevas cuotas de eficiencia y eficacia, se abren ante nosotros nuevos peligros derivados del propio uso de la tecnología. Por suerte, cada día somos más conscientes del riesgo al que estamos expuestos, y estamos más dispuestos a buscar soluciones que nos permitan proteger nuestros recursos. Eso sí, hay que tener en cuenta que la mejor forma de proteger nuestro negocio es asumiendo una visión global de la Ciberseguridad, que nos permita dar respuesta a todas las posibles contingencias que se sucedan.

La realidad actual es tozuda y nos obliga a asumir que, tarde o temprano, vamos a ser atacados. Por tanto, lo primero es incrementar nuestros esfuerzos para minimizar el impacto de estos ataques. Además, hay que pensar en anteponer una política de Ciberseguridad global, que nos permita identificar las posibles amenazas existentes, proteger los activos, detectar intentos de ataque y, si se llegan a producir, ser capaces de restablecer la situación lo antes posible. Sin olvidar que necesitamos que todos estos elementos estén vertebrados y coordinados por un único sistema que facilite el control y la gestión.

En este sentido, la propuesta de GMV en Ciberseguridad pasa por ofrecer una serie de servicios en los que analizan y diagnostican entornos específicos desde el punto de vista de cumplimiento de normativas o de riesgos; elaboran planes que desarrollan normas como la Protección de Infraestructuras Críticas, GDPR o los Esquemas Nacionales; incorporan soluciones tecnológicas específicas; gestionan la operación de las infraestructuras tecnológicas de Ciberseguridad; y dotan de la visibilidad necesaria para la toma de decisiones y el buen gobierno.

Así, se establecen cinco **pasos fundamentales en esta propuesta de Ciberseguridad**: identificar, proteger, detectar, responder y recuperar:



LA TRANSFORMACIÓN DIGITAL Y SUS RETOS EN EL SECTOR LEGAL

1 IDENTIFICAR.

Conseguir el conocimiento y las capacidades organizativas necesarias para poder gestionar la Ciberseguridad en la organización. Esta fase supone las bases para las demás.

- Desarrollo normativo, Plan Director y SGSI
- Definición de controles, indicadores y cuadros de mando
- Auditorías de cumplimiento (GDPR, ENS, PIC...)
- Análisis y gestión de riesgos

2 PROTEGER.

Implementar las contramedidas y salvaguardas que aseguren los servicios corporativos. Se trata de tener la capacidad de limitar o de contener el impacto de un suceso o evento de Ciberseguridad.

- Asesoramiento en la incorporación de nuevas tecnologías
- Implantación de soluciones tecnológicas de Ciberseguridad
- Fabricación de soluciones y servicios propios

3 DETECTAR.

Identificar la ocurrencia de un suceso o evento de Ciberseguridad, a tiempo.

- Diagnósticos especializados (hacking, código fuente...)
- Gestión de vulnerabilidades
- Red team
- Infraestructuras de monitorización continua
- GMV SOC

4 RESPONDER.

Medidas de actuación ante un suceso o evento de Ciberseguridad para tratar de contener el impacto.

- GMV-CERT
- SERVICIOS PROACTIVOS:
  - Assessments
  - Gestión de la configuración
  - Inteligencia
- SERVICIOS REACTIVOS:
  - Gestión de incidencias
  - Análisis forense

5 RECUPERAR.

Enfocado a la recuperación y resiliencia, minimizando el factor tiempo.

Definición y ejecución de:

- BIA
- Plan de Continuidad de Negocio
- Pruebas

Con todo, la compañía trata de acompañar a los clientes en la superación de una serie de **retos fundamentales**, desde el punto de vista de la Ciberseguridad:

- ➔ Protección de infraestructuras críticas
- ➔ Ingeniería, soluciones y servicios de seguridad de sistemas y redes de información
- ➔ Ciberseguridad en entornos industriales
- ➔ Auditorías de seguridad
- ➔ Planes de cumplimiento de los Esquemas Nacionales de Seguridad y GDPR
- ➔ Implantación de sistemas de gestión de seguridad
- ➔ Securización de plataformas, redes y servicios
- ➔ Servicios gestionados CSIRT (Computer Security Incident Response Team)
- ➔ Centros de respaldo.

La innovación tecnológica clave para impulsar el negocio jurídico

Pablo González, Responsable de Big Data & Business Analytics de Secure e-Solutions de GMV

La transformación digital es una realidad, nadie puede entender que exista un banco que no permita operar por internet, un comercio que no tenga su correspondiente tienda online o una empresa sin una base de datos de clientes. Pero tampoco nadie se extraña al ver los juzgados atestados de montañas de papeles y asumimos estoicamente que los procesos judiciales se dilaten durante años por culpa de complejos procedimientos manuales.

Si bien es cierto que el sector legal tradicionalmente ha pasado desapercibido en la aplicación de nuevas tecnologías, la realidad es que ha sido porque no ha tenido necesidad, se trata de un sector muy protegido y accesible para muy pocos donde la competencia está bastante controlada. Sin embargo, durante los últimos años, ha aparecido un nuevo movimiento conocido como "legaltech" encabezado principalmente por empresas tecnológicas que pretenden aprovechar esta oportunidad.

LEGALTECH COMO OPORTUNIDAD PROMETEDORA

Como en la mayoría de las industrias, las nuevas tecnologías no han venido a sustituir a los abogados, el objetivo es delegar las tareas más tediosas y repetitivas en una máquina para que pueda centrarse en aquellas en las que puede aportar más valor. Según un estudio de McKinsey el 23% de las tareas en un despacho de abogados son automatizables.

Hay mucho trabajo ya hecho en el mundo anglosajón pero su transcripción al derecho español no siempre es inmediata y es preciso pensar en nuevas ideas y herramientas. El principal reto es adaptar las técnicas de procesado de lenguaje a la jerga legal, que tiene unas características muy especiales: ambigüedad, formalismos, estructura... y, además, hacerlo en su correspondiente idioma. No es un reto sencillo para una máquina, basta con ver la cantidad de personas dedicadas profesionalmente a interpretar los textos legales durante la historia del derecho y a pesar de ello a veces no llegan a un consenso.

Algunos casos en los que la innovación está consiguiendo algunos resultados prometedores es en la revisión automática de contratos, consultas jurídicas online, autogeneración de textos legales y por supuesto en mejorar las herramientas de gestión. En este sentido GMV está trabajando en herramientas que permitan a los abogados hacer búsquedas rápidas en la documentación en cualquier formato (texto, vídeo y audio) de sus casos para poder preparar recursos o alegaciones de una manera más eficiente.

La sensación es que esté mundo está todavía por explorar, hay muchas empresas (grandes y pequeñas) investigando e innovando, pero muchas veces del ámbito tecnológico, es necesario que los actores del sector legal tomen el protagonismo y decidan hacia dónde quiere ir su futuro.

¿QUÉ ES LEGALTECH?

Legaltech es la tecnología aplicada al mundo legal. Una tecnología que en realidad hace muchos años que existe, en Estados Unidos el sector legal lleva años de ventaja ofreciendo a sus clientes un contrato online u otras tecnologías legales como buscadores de abogados, software inteligente para búsqueda de casos y otros servicios impulsados por la aplicación de tecnologías. En resumen, son herramientas que hacen que los abogados sean más eficientes y facilite sus labores diarias, además de ofrecer un servicio más adecuado a sus clientes.

SOLUCIONES DE CIBERSEGURIDAD

GMV-CERT

GMV cuenta con un Centro de Respuesta ante Incidentes de Ciberseguridad con prestación remota 24x7, con los recursos de hardware, software y comunicaciones necesarios para dar una solución multi-tecnología acorde a la demanda heterogénea de los clientes. Proporciona cinco tipos de servicios: monitorización, vigilancia digital, gestión de vulnerabilidades, gestión de incidencias y gestión de evidencias.

ATALAYA

Solución de vigilancia digital. GMV monitoriza diversas fuentes, en modalidades de 8x5 o 24x7, 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, APT, phishing, pharming, spam, información obtenida a través de ataques contra la organización, credenciales de usuarios en los diferentes servicios de la organización, entre otros.

GESTVUL

Solución de gestión de vulnerabilidades. 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 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.

SIEM_NG

GMV ha puesto su experiencia en Big Data, Inteligencia Artificial y Ciberseguridad para desarrollar una solución que permite expandir o complementar los SIEM tradicionales integrando grandes volúmenes de información de diversa índole, y categorizando el comportamiento de usuarios y sistemas (alertando en caso de situaciones anómalas). Esta solución permite expandir la seguridad de una organización, a partir de fuentes de información diversas y heterogéneas, más allá de las posibilidades que ofrece un SIEM tradicional.

Muchos despachos de abogados han tenido que crecer y expandirse internacionalmente de manera muy rápida en los últimos años, y eso ha derivado en que sus sistemas no hayan sido diseñados para soportar estos nuevos escenarios y protegerse de las nueva ciberamenazas. GMV puede ayudar a revisar la situación actual y a crear un plan para mejorar la seguridad de dichos sistemas y activos.

SERVICIOS

La Ciberseguridad, elemento indispensable en la estrategia de los despachos de abogados

Isabel Tovar, Directora Compañías de Servicios de Secure e-Solutions de GMV

En un mundo digital donde ninguna organización es totalmente segura y los ciberataques están a la orden del día, la Ciberseguridad juega un rol trascendental para proporcionar la privacidad y protección necesaria de los datos de las organizaciones. Los despachos de abogados son uno de los sectores en los que la información constituye uno de sus activos fundamentales, ya que el valor de su actividad se encuentra en sus datos. Por lo tanto, ¿qué pasaría si estos datos son expuestos o caen en manos de terceros?

Dentro de un despacho de abogados se tratan diariamente datos sensibles que suponen bienes tangibles de gran valor, tanto para los despachos como para sus clientes. En caso de pérdida, sustracción o acceso no consentido por parte de terceros, la información puede ser usada para comercializarla u otros fines indeseados. La situación puede llegar a ser alarmante para el sector legal, ya que sus clientes ven amenazada la confianza que han depositado en estos profesionales ante la posible fuga de información u otras vulnerabilidades. Como consecuencia de esta problemática, los despachos de abogados deben de llevar a cabo una estrategia de Ciberseguridad para dar valor a sus clientes, evitando las filtraciones de información, repercusiones legales, sanciones y la posterior pérdida de imagen del despacho.

La Ciberseguridad debe ser un elemento indispensable en las inversiones de los despachos de abogados para hacer frente a las ciberamenazas (malware, daños informáticos, fraude y suplantación de identidad, destrucción de información...) y fomentar las medidas necesarias de sensibilización, prevención, detección y reacción ante incidentes.

Las causas principales de las fugas de información se enmarcan en el ámbito organizativo (falta de clasificación, delimitación del ámbito de difusión, falta de conocimiento y formación, ausencia de procedimientos o inexistencia de acuerdos de confidencialidad) o en el ámbito técnico (código malicioso o malware, acceso no autorizado a sistemas e infraestructuras, generalización del uso de servicios en la nube o el uso de las tecnologías móviles para el trabajo diario).

En la mayoría de los casos, las fugas de información implican la ausencia o ineficiencia de algún tipo de medida o de procedimiento de Ciberseguridad. Esta carencia de medidas conlleva un inadecuado control sobre la información que se maneja, lo que hace aumentar de forma significativa la probabilidad de que se produzca un incidente que lleve consigo una fuga de información.

Desde GMV, destacamos que las principales preocupaciones para los despachos de abogados es la seguridad perimetral, protegerse ante cualquier tipo de ataque y controlar el intercambio de información con sus clientes.

MAYO DE 2018…

Una fecha marcada en el calendario y que inevitablemente está suponiendo un punto de inflexión en el sector de la Ciberseguridad en España y en la actividad de los profesionales. En primer lugar, una Directiva Europea, la 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como Directiva NIS, que ha desembarcado en nuestro país el 9 de mayo de 2018. El pasado 25 de mayo también se estableció el Reglamento Europeo de protección de datos, conocido como GDPR (o RGPD en español).

El cumplimiento de la legislación vigente que incluye aspectos de Ciberseguridad es uno de los retos actuales de las organizaciones. Otro de los retos es el del retorno de la inversión en servicios y soluciones tecnológicas de Ciberseguridad, donde se ha impuesto una percepción de puro gasto que es muy difícil de revertir. Lo cierto es que todos los ciberincidentes, en especial los ataques intencionados, se aprovechan de una vulnerabilidad no resuelta de nuestros sistemas. Por lo tanto, mejor que intentar paliar los efectos adversos de un ciberincidente una vez que se produce, tiene más sentido ir

Continúa ➜

LA TRANSFORMACIÓN DIGITAL Y SUS RETOS EN EL SECTOR LEGAL

➜ *Viene de la pág. anterior*

al origen del problema y solucionar la vulnerabilidad de manera preventiva, antes de que se produzca el ataque. En GMV apostamos por ofrecer una mayor seguridad y control a las empresas con sistemas de gestión muy exigentes, permitiendo la protección adecuada de la información de los clientes y asegurando la continuidad del negocio ante un desastre. El objetivo de GMV es identificar las amenazas existentes, proteger los activos, detectar intentos de ataque y, si es necesario, restablecer la situación lo antes posible.

"Así como el departamento de seguridad del Banco de España tiene que poner todas las medidas para proteger el tesoro del país (millones de toneladas de oro), los departamentos de seguridad de los despachos tienen que proteger su tesoro más preciado que son los documentos."

De esta manera, GMV proporciona al sector legal una solución de Ciberseguridad que protege la información y garantiza la privacidad de los datos, además de ser un perfecto socio para el cumplimiento de las normas legislativas de sus clientes. ■

MÁS INFORMACIÓN

- Ciberseguridad
- Ciberseguridad
- checker ATM Security
- atalaya
- gestvul
- GMV-CERT

"GDPR VA A PRODUCIR EN EL SECTOR LEGAL UNOS EFECTOS DESCONOCIDOS"