webdox

¿Cómo funciona la Ciberseguridad en la Nube?

Contenidos

INTRODUCCIÓN

¿Cómo funciona la Ciberseguridad en la Nube?

En los últimos años hemos sido testigos de cómo la computación en la nube y los *SaaS (Software as a Service)* han impulsado la transformación digital como ninguna otra disrupción tecnológica lo había hecho antes. De hecho, las predicciones de *Forrester*, una de las consultoras más influyentes a nivel mundial, anuncian que para este 2018 más del 50 % de las empresas globales se basarán -al menos- en una plataforma en la nube pública para impulsar su transformación digital.

Es precisamente en este escenario de grandes innovaciones tecnológicas desarrolladas en la nube en el que se inserta **Webdox**, un software diseñado para la completa gestión del ciclo de vida de los contratos de las empresas que opera bajo la modalidad *SaaS.* **Webdox** optimiza la gestión del ciclo de vida de un contrato, automatizando la gestión de solicitudes, creación, aprobación, negociación y firma de contratos, agregando además una serie de herramientas para administrar un contrato posterior a su firma.

Uno de los grandes desafíos al cual nos hemos visto enfrentados como empresa es el de romper los mitos en relación a los servicios en la nube y a la seguridad con la que operan los sistemas desarrollados en infraestructuras *cloud.*

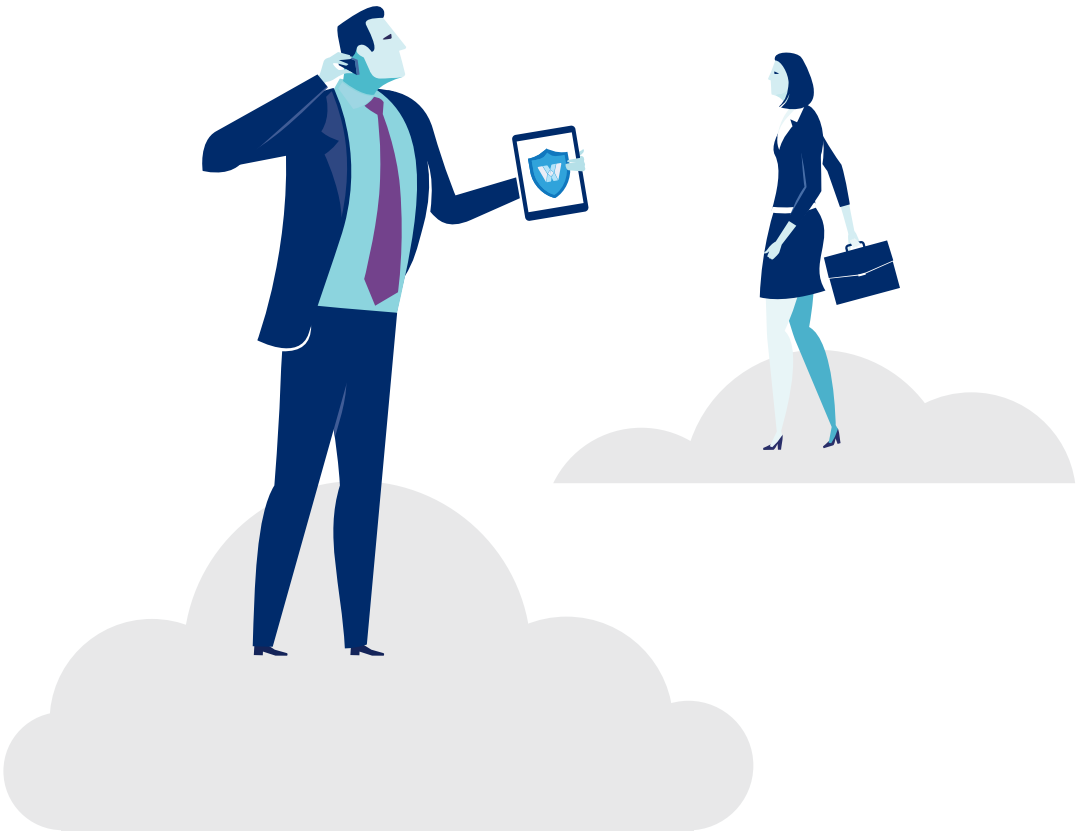
En este *ebook* exponemos algunos de los puntos más relevantes a considerar en cuanto a cómo opera la ciberseguridad en la nube. Para esto, exponemos algunas de las medidas de seguridad que *Amazon Web Services (AWS)* y *Google Cloud Platform (GCP)* - plataformas en las cuales se encuentra la infraestructura tecnológica de **Webdox** - entre otros de los principales proveedores de servicios *cloud* (como *Microsoft Azure*), han desarrollado de manera de ofrecer un servicio con estándares de seguridad de clase mundial.

Finalmente, también exponemos algunas medidas de seguridad específicas que hemos desarrollado en **Webdox** para ofrecer la máxima seguridad en nuestras plataformas.

01

LA CIBERSEGURIDAD EN LA NUBE

Las plataformas en la nube han cambiado por completo la forma en que consumimos tecnologías y adoptamos sistemas de todo tipo, atrás quedó el modelo de distribución de licencias para dar paso a un enfoque mucho más orientado a los servicios. Ahora, esta tendencia está modificando las operaciones de todo tipo de compañías, sin importar tamaño, industria o geografía.



Este fenómeno trae grandes desafíos en materias de seguridad. Tanto el *cloud computing* como la ciberseguridad, se han convertido en los puntos que encabezan las listas de prioridades de las empresas con un alto componente tecnológico. Así lo evidenció el Informe *"Construyendo confianza en un cielo nublado"*, de *McAfee*, del que podemos resaltar:

Los servicios en la nube son utilizados por más del 90 % de las organizaciones de todo el mundo.

49 % de los profesionales encuestados afirmó que no habían ralentizado su adopción de la nube a causa de la falta de personal especializado en ciberseguridad.

Los profesionales que confían en nubes públicas superan en proporción de 2 a 1 a aquellos que desconfían de ellas.

Un 52 % de los encuestados aseguran haber rastreado un *malware* o infección en una aplicación *SaaS.*

Datos como estos nos permiten concluir que las empresas confían cada vez más en los servicios en la nube, pero que la seguridad es un factor al cual deben prestar especial atención.

¿Qué están haciendo las empresas líderes de servicios en la nube en materia de ciberseguridad?

Los principales proveedores de servicios en la nube como *Amazon Web Services o Google Cloud*, sobre los cuales operan gran parte de los servicios en la nube ofrecidos en el mercado, han abordado de manera proactiva sus controles de seguridad realizando verificaciones independientes de los políticas de seguridad, privacidad y cumplimiento, poniendo estos informes a disposición del público.

Las tendencias en ciberseguridad

Durante la *Cumbre de Gestión de Riesgos y Seguridad de Gartner 2017*, el analista de esta empresa de consultoria, *Earl Perkins*, presentó las que serían las tendencias de la ciberseguridad en la Nube para este año. Entre estas, habló de los crecientes volúmenes de información que tendrán que manejar los expertos en seguridad cibernética, advirtiendo que los cambios en la materia requerirán nuevos tipos de habilidades en ciencia de datos y análisis, haciendo de la inteligencia de seguridad artificial algo imprescindible.

Además, *Perkins* considera fundamental invertir en estrategias de detección y respuesta, parte del presupuesto gastado en prevención de riesgos y ataques.

No todo se puede prevenir, pero sí es posible saber cómo responder.

Impedir todos los ataques es imposible y, según el experto, es en el terreno de la detección, respuesta y solución donde debe hacer foco la ciberseguridad moderna. Por lo demás, tendremos que esperar a que tanto la nube como la ciberseguridad sigan evolucionando al ritmo que lo han hecho, porque la adopción del *cloud computing* es una realidad en la que todas las empresas del mundo habrán de sumergirse.

02

NORMAS ISO DE CIBERSEGURIDAD

A la hora de trabajar con información en la nube, las empresas que prestan este servicio deben garantizar la integridad de los datos de sus clientes. Para ello, existen las *normas ISO 27017 ,27001* y *27018*, las que apuntan a fortalecer la ciberseguridad en servicios cloud. A continuación, te contamos todo lo que necesitas saber al respecto.

Contar con una certificación ISO es uno de los parámetros más importantes a la hora de elegir un proveedor de servicios en la nube. Dicha certificación garantiza altos estándares en la seguridad de la información, uno de los activos más valiosos para las empresas que prestan servicios *DBaaS* (*Data Base as a Service*, o Base de Datos como Servicio), al igual que aquellas cuyo modelo es el *SaaS (Software as a Service).*

Al respecto, las normas *ISO 27017 ,27001* y *27018* constituyen algunos de los principales estándares para resguardar la ciberseguridad y garantizar la integridad de la información alojada en la nube, servicio ofrecido por empresas como *Amazon Web Services (AWS), Google Clou*d o *Microsoft Azure.*

Normas ISO para la seguridad en la nube

1. ISO 27001

A grandes rasgos, la norma *ISO 27001* es un estándar generado por la *Organización Internacional de Normalización (ISO, por sus siglas en inglés)* que describe la manera correcta de gestionar la seguridad de la información al interior de una empresa.

Se trata de la principal norma de seguridad -a nivel global- para el manejo de la información. Su eje central es el Sistema de Gestión de la Seguridad de la Información *(SGSI)*, el cual debe realizarse a través de un *«un proceso sistemático, documentado y conocido por toda la organización»*, tal como lo establece el propio organismo.

Entendiendo que es prácticamente imposible garantizar la total seguridad de la información, la norma *ISO 27001* apunta a que las organizaciones conozcan los riesgos asociados al manejo de información, asumiéndolos, minimizándolos y gestionándolos por medio de un proceso documentado, sistemático, estructurado, eficiente, repetible y adaptable a los eventuales cambios que pudieran presentar los riesgos, el entorno y la tecnología.

Para obtener una certificación *ISO 27001,* la empresa debe cumplir con ciertos pasos:

Etapa previa: Aquí, las empresas deben implementar 14 pasos básicos para iniciar su proceso hacia la certificación. Entre los principales, están la utilización de una metodología de gestión de proyectos, contar con el apoyo de toda la dirección en el proceso de implementación, definir el alcance del sistema de seguridad, determinar una política de evaluación de riesgos, implementación de controles y medidas correctivas.

Auditoría de revisión: Personal externo revisará que lo anterior se cumpla para dar curso al proceso de certificación.

Auditoría principal: Aquí, un grupo de auditores verificará que las medidas anteriores cumplan con sus objetivos. De estar todo en orden, la empresa puede ser certificada.

Revisiones periódicas: Una vez aprobada la certificación, el organismo monitoreará dicha empresa durante 3 años para garantizar que cumpla con los esfuerzos de protección de datos.

2. ISO 27017

La norma ISO 27017 es un estándar de seguridad que proporciona controles tanto para clientes como para proveedores de servicios en la nube.

Su importancia radica en la precisión con la que establece las relaciones entre clientes y proveedores de servicios en la nube, determinando qué puede exigir el cliente y qué información debe proporcionarle el proveedor.

El cumplimiento de esta guía permite fortalecer la ciberseguridad y la gestión del servicio referente a arquitectura, medidas de seguridad, funcionalidades disponibles, tecnología de cifrado y localización geográfica de los datos.

Esta norma contempla 37 controles en la nube -basados en la *ISO -27002*, junto a 7 adicionales que permiten fortalecer la seguridad de los servicios *cloud.*

3. ISO 27018

Finalmente, la norma *ISO 27018* constituye un compendio de buenas prácticas -referentes a controles de protección de datos- para servicios cloud, enfocada específicamente en los proveedores.

Su objetivo central es delimitar las normas, procedimientos y controles que los proveedores -en su calidad de **«procesadores de datos»**- deben aplicar. Además, garantiza el cumplimiento de la normativa legal en cuanto al manejo de datos personales.

Proveedores de servicios cloud que cumplen con las normas ISO

Puesto que los estándares anteriormente abordados apuntan a fortalecer la ciberseguridad en la nube, los principales proveedores del mercado deben ceñirse a ellos.

Por un lado, *Amazon Web Services (AWS)* transparenta el cumplimiento de todas las normativas anteriores, además de cumplir con leyes y regulaciones específicas de determinados países.

Por otro, *Google Cloud* también pone a disposición de los usuarios el listado de normativas, certificaciones y regulaciones con que cumple para garantizar la ciberseguridad de los datos de sus clientes. Desde luego, el servicio se cumple con los estándares anteriormente revisados.

Cabe destacar también a *Microsoft Azure*, servicio que se ha apalancado en la basta experiencia que tiene *Microsoft* ofreciendo software empresarial para construir una infraestructura en la nube segura y confiable, que cuenta con todas las certificaciones mencionadas anteriormente.

Contar con estas certificaciones le ha permitido a *AWS, Google Cloud* y a *Microsoft Azure*, posicionarse como los mejores proveedores de servicios en la nube. Gracias a los controles implementados, tanto el modelo *DBaaS* como el *SaaS* se han vuelto más seguros, confiables, transparentes y efectivos.

03

PREVENCIÓN DE ATAQUES DDOS EN LA NUBE

También conocidos como la peor pesadilla de un administrador de sistemas, los ataques *DDoS (Distributed Denial of Service, Denegación de Servicio Distribuido)* pueden causar estragos fatales en redes corporativas y costar a las empresas importantes sumas de dinero en caso de no estar preparados. Mientras que quienes cuentan con un servidor local propio son en la mayoría de los casos los más afectados, aquellos que utilizan sistemas de cómputo en la nube, tales como *Google Cloud* , *Amazon Web Services* (*AWS*) o *Microsoft Azure*, no están exentos de tales amenazas. A continuación, revisaremos algunas de las mejores prácticas para prevenir y mitigar este tipo de ataques en configuraciones de cloud computing, pero primero, a lo básico:

¿En qué consiste un ataque DDoS?

Un ataque *DDoS (Distributed Denial of Service)* es un intento de agotar los recursos disponibles para una red, aplicación o servicio para que sus usuarios legítimos no puedan accederla.

Hace algunos años, e impulsado en gran parte por el aumento del *"hacktivismo"*, se ha visto un renacimiento en los ataques *DDoS* que ha llevado a la innovación en las áreas de herramientas, objetivos y técnicas utilizadas para ejecutarlos.

En la actualidad, la definición de **«ataque DDoS»** continúa complicandose. Los hackers utilizan una combinación de ataques de gran volumen, junto con infiltraciones más sutiles y difíciles de detectar que apuntan a las aplicaciones, así como a la infraestructura de seguridad de red existente, como *firewalls* e *IPS (sistemas de protección contra intrusiones).*

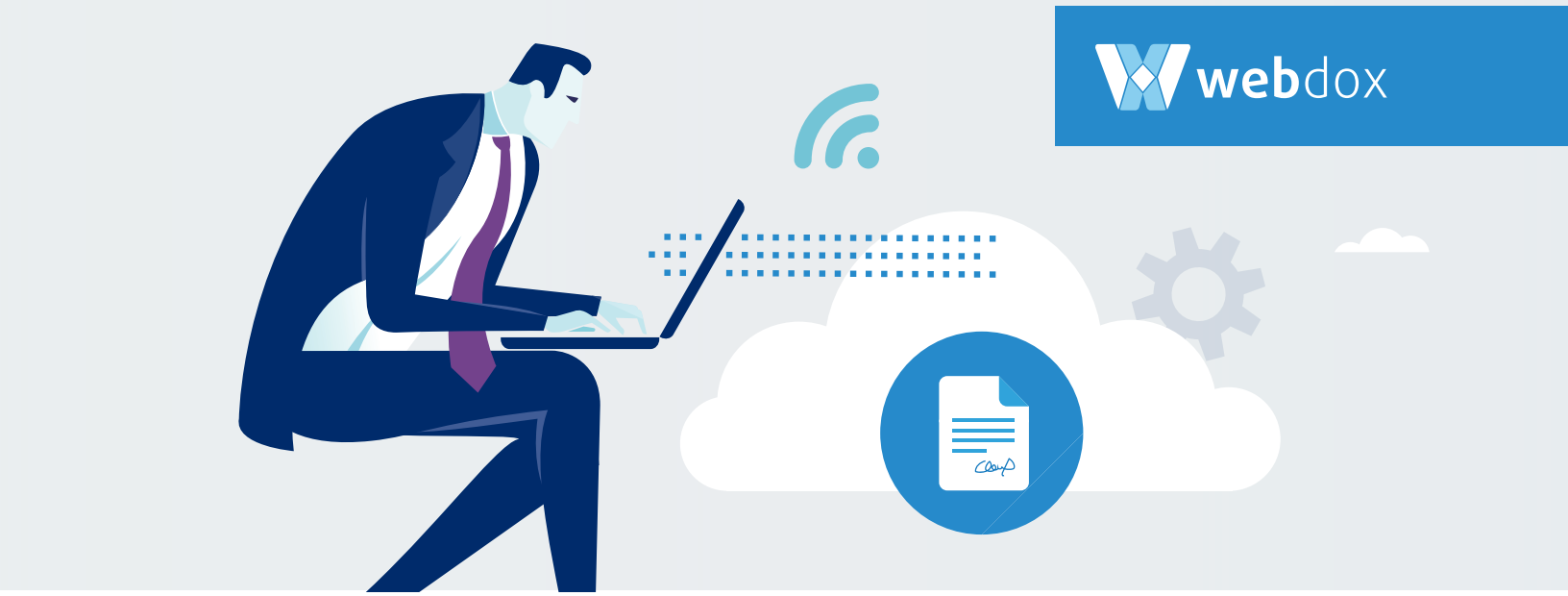
¿Cómo evitamos estos ataques al trabajar con servidores en la nube?

Desarrollando soluciones escalables: Una infraestructura escalable es fundamental para un sistema bien estructurado, sin embargo, también es una técnica de gran efectividad a la hora de evitar ataques *DDoS.* Escalar para cumplir con los volúmenes de tráfico adicionales, ya sean válidos o de un ataque *DDoS*, aumentará la capacidad de tus servidores para seguir funcionando.

Minimizando el área de superficie de ataque: En este caso es clave desacoplar las partes de tu infraestructura de red. Por ejemplo, al ejecutar sitios web públicos, separa la aplicación de la base de datos y, si es posible, los medios y su contenido estático también. Las aplicaciones desacopladas limitan el acceso a Internet a los componentes críticos del sistema, protegiéndose de un ataque.

¿Cómo mitigamos un ataque?

Aislando el tráfico interno de la red exterior: Implementando instancias sin IP públicas a menos que sea necesario. Por ejemplo, configurando una puerta de enlace *NAT* o un bastión *SSH* para limitar el número de instancias que están expuestas a Internet. Una vez disponible, implementamos el equilibrio interno



de carga para que las instancias internas de tus clientes accedan a los servicios implementados internamente evitando así exposición al mundo externo.

Equilibrando la carga con la ayuda de Proxys: *AWS* y *Google Cloud* poseen herramientas de balance de carga *HTTP(S)* o balance de carga *SSL proxy*, con lo cual la infraestructura de sus servidores cloud es capaz de mitigar y absorber muchos ataques de *Capa 4* y siguientes, tales como inundación *SYN*, inundación de fragmento de IP, etc. Al contar con una herramienta de balance de carga *HTTP(S)* en múltiples regiones, logran dispersar cualquier posible ataque a través de las instancias de sus servidores alrededor del globo.

En conclusión, si bien los ataques *DDoS* continúan siendo una amenaza permanente para las infraestructuras *cloud*, existen muchas maneras de estar preparados y enfrentarlos de manera exitosa para mantener tus sitios web o aplicaciones siempre disponibles en caso de recibir un intento de saturar nuestra red. Siempre es necesario tener estos datos en mente para mantener una red saludable y estable.

04

PROTECCIÓN DE DATOS

En la inminente necesidad de realizar un proceso de transformación digital, cada vez son más las organizaciones que trasladan sus datos a la nube. Al respecto, la ciberseguridad es uno de los temas que más preocupan a las entidades que quieren dar el salto, y las cifras permiten dar cuenta de ello.

La encuesta *State of Cloud 2017*, dirigida por *RightScale*, determinó que -actualmente- las empresas ejecutan 79 % de sus cargas de trabajo en la nube, evidencia de la importancia que los servicios cloud tienen para la evolución de las organizaciones, indispensable en un mercado cada vez más digitalizado y competitivo.

Por su parte, un estudio de *Forrester* arrojó que 28 % de las empresas afirman estar en proceso de implementación de *DBaaS* (*Database as a Service o Base de Datos como Servicio)* y que este número probablemente se duplicará en los próximos cuatro años.

Para las empresas, contar con un servicio de base de datos en la nube -como los que ofrece *Google Cloud, Amazon Web Services (AWS)* o *Microsoft Azure*- brinda múltiples ventajas: desde la reducción de gastos de infraestructura, pago de personal, servicio eléctrico y reducción de espacio físico, hasta aspectos como la escalabilidad, disponibilidad, automatización y aumento en la productividad.

Lo anterior se explica, entre otras cosas, porque el modelo de base de datos en la nube se adapta a las necesidades de cada empresa. Así, mientras el proveedor ofrece la infraestructura física y almacenamiento de los datos, el cliente se encarga de su administración y operación.

Sin embargo, al momento de migrar y almacenar información en un servicio *cloud*, es común que surjan algunas inquietudes sobre la protección de datos. A continuación, responderemos los cuestionamientos más comunes al respecto:

¿Qué garantía de protección de datos existe en la nube?

Las empresas que ofrece servicios de *DBaaS* deben implementar estrictas medidas de seguridad para no comprometer la información de sus clientes. Por ejemplo, en el caso de *Google Cloud*, la compañía cuenta con más de 750 expertos encargados de mantener los sistemas de defensa, crear la infraestructura y políticas de seguridad.

Es importante destacar que la seguridad del almacenamiento de datos en la nube depende de dos factores: cliente y proveedor.

Mientras que al proveedor le compete la seguridad de la nube, es responsabilidad del cliente la seguridad en la nube. **¿A qué se refiere esto?** a que es un modelo de responsabilidad compartida: Mientras que el primero protege los componentes del sistema operativo, alojamiento y las instalaciones físicas; el cliente debe vigilar sus plataformas, sistemas, aplicaciones, configuración y redes, además de prestar especial atención a los permisos y la privacidad con la que los usuarios acceden a sus plataformas en la nube. Siendo así, es el cliente quien controla la arquitectura de seguridad, la fuerza de sus contraseñas, permisos de acceso, etcétera.

¿Dónde se almacenan los datos en la nube?

Para tranquilidad de los usuarios, los datos son almacenados y resguardados con estrictos controles de seguridad en los servidores de los centros de datos del proveedor, con una protección mayor a la que tendrían dentro del área de IT de una empresa. Estos centros están ubicados en diversas localizaciones y cada cliente determina la región y el servidor donde desea alojar sus datos.

Por ejemplo, *AWS* cuenta con diversas capas de protección de sus *data centers,* para asegurar al máximo la integridad de los datos aquí alojados.

¿Quién puede acceder al contenido?

Solo los clientes pueden manejar el formato, estructura y claves de cifrado de los datos, y son ellos los únicos que deciden a quiénes facultan para acceder a determinada información.

Los principales proveedores de *DBaaS* -como *Google Cloud* , *Microsoft Azure* y *AWS*- ofrecen ciberseguridad, privacidad, transparencia y cumplimiento de las normas internacionales, garantizado a través de auditorías y certificaciones. Por ello, mantener una base de datos en la nube suele ser más seguro que administrarla en un servidor y redes privadas.

05

INTELIGENCIA ARTIFICIAL PARA LA PROTECCIÓN DE DATOS

La *Inteligencia Artificial* (*AI*) está cambiando nuestra manera de pensar y abordar los problemas. Cada vez se abren más puertas en esta nueva simulación de procesos de inteligencia humana a través de sistemas informáticos, procesos de aprendizaje, de razonamiento y de autocorrección.

Entre las aplicaciones de la *AI* actual, se encuentran sistemas expertos, reconocimiento de voz y visión artificial. No obstante, los principales proveedores de servicios *cloud*, como *Google Cloud Platform* o las herramientas de *Amazon Web Services*, están utilizando inteligencia artificial para la protección de los datos almacenados en sus servidores.

¿Por qué debería interesarnos?

En vista de los constantes ataques por parte de la delincuencia informática, es cada vez más necesario robustecer los servidores de una manera automatizada y confiable, por lo que muchas organizaciones se ven obligadas a mejorar su ciberseguridad. Analizar cómo se está aplicando la Inteligencia Artificial en este importante campo, nos ayudará a percibir nuevas soluciones en la protección de datos e información confidencial.

¿Quiénes son pioneros en seguridad AI y cómo se está utilizando?

Uno de los principales ejemplos es *Amazon.* Tras la adquisición de la importante startup de seguridad cibernética *"Harvest.ai",* creó un nuevo servicio de almacenamiento denominado *Amazon Macie*, admitido actualmente en el Norte de Virginia y Oregón.

Este servicio de seguridad emplea el aprendizaje automático para descubrir, clasificar y proteger datos confidenciales, utilizando al mismo tiempo su plataforma de servicios *cloud*: *Amazon Web Services* o *AWS*.

Amazon ha ofrecido a múltiples empresas de diferentes niveles de madurez, los servicios de *Amazon S3*, basados en la nube y con una funcionalidad práctica y sencilla. Los clientes solo deben crear cubos o contenedores lógicos de información, parametrizado según el nivel de permisología y los accesos basados en roles y perfiles de cargo.

Por su parte, *Google* ha desarrollado el servicio *Data Loss Prevention (DLP)* que, bajo la misma premisa, busca enriquecer los niveles de seguridad y privacidad del contenido almacenado en la nube.

¿Cómo funcionan?

Amazon Macie y *Google DLP* son capaces de reconocer información sensible o de propiedad intelectual. Las aplicaciones de estos servicios pueden ser muy bien aprovechadas por las instituciones financieras y otras empresas tecnológicas, pues les proporciona una mejor visión de toda la información que entra o sale de los servidores.

El objetivo de este servicio es garantizar la ciberseguridad, identificando y creando alertas ante cualquier dato confidencial que se encuentre almacenado en la nube y que no esté del todo seguro.

Las herramientas de *Google* y *Amazon* analizan patrones de uso, acceso y descarga. Nada se escapa de su inteligencia artificial. Con *Google DLP*, se puede configurar para todas las plataformas de *G Suite*, protegiendo así correo electrónico o archivos de *Drive*, siendo altamente personalizable.

Por supuesto, la implantación de un sistema de seguridad en la nube basado en inteligencia artificial debe estar levantado por una consultoría y entrenamiento especializado que permita una correcta alineación entre el nuevo servicio y los responsables de la plataforma tecnológica y de seguridad.

¿Qué tipo de información detectan y protegen estas plataformas?

Tanto *Amazon Macie* como *Google DLP*, pueden detectar y clasificar información almacenada en documentos bajo diversos formatos como *MS Word*, *MS Excel* y notas de texto. También pueden contemplar la extensión del documento o archivo, evaluando la sensibilidad de la información, los metadatos del documento y, a través de otros servicios de seguimiento de auditoría, puede extraer la información relacionada con los usuarios que solicitan o utilizan la información y sus roles.

Para una mayor eficiencia, en los documentos más confidenciales podría requerirse de la configuración de los metadatos y palabras clave de la empresa, garantizando que la información sensible cuente con la mejor protección.

Google DLP mantiene una base con más de 50 referencias y detectores, donde se incluyen datos bancarios u otro tipo de clasificación de información sensible. Por su parte, *Macie* puede admitir 20 categorías de alertas, entre las cuales se encuentran los eventos de datos de alto riesgo, credenciales almacenadas en código fuente, backups no cifradas que contienen credenciales, entre otros.

¿Qué hay del mantenimiento y actualización?

Google DLP no mantiene planes mensuales, sino que funciona en base a la cantidad de datos procesados en el servicio, entregando una atención más personalizada.

Por su parte, *Amazon* cuenta con una plataforma que contempla un conjunto de planes que se adaptan a las necesidades de cada organización.

Hoy es posible contratar servicios especializados en la gestión de contratos online y administración de documentos sensibles, los cuales utilizan servicios de manejo de datos en la nube para asegurar la confidencialidad de sus clientes, ofreciendo plataformas optimizadas para usuarios no especializados en tecnologías de la información.

Los servicios de Seguridad en la nube que estos gigantes de la tecnología han venido desarrollando y profesionalizando son solamente el inicio de nuevas aplicaciones que en poco tiempo podremos aprovechar para blindar la ciberseguridad de nuestra organización.

06

CIBERSEGURIDAD EN UNA PLATAFORMA SAAS PARA LA GESTIÓN DE CONTRATOS

Cada vez más empresas se suman a la tendencia de automatizar sus procedimientos, con el fin de optimizar la gestión de los recursos y generar ventajas competitivas. Claramente, lo anterior incentiva la necesidad de automatizar la gestión de contratos, dados los múltipls beneficios. Así, el uso del *Cloud Computing* ha logrado convertirse en uno de los sistemas más utilizados para mejorar la colaboración, la agilidad de los procesos y la disponibilidad de la información.

Este cambio implica que los equipos de TI tienen que actualizar sus competencias y establecer diversos protocolos, con medidas de seguridad para controlar y resguardar el acceso a la información.

¿Qué factores hay que considerar?

Una plataforma *SaaS* para la gestión de contratos, tiene que cumplir una serie de estándares de ciberseguridad; tomando como base los principales desafíos que un ambiente cloud representa. Entre los principales encontramos:

• Proteger el acceso no autorizado a los datos y las credenciales de los usuarios.
• Evitar la pérdida de información y generar respaldos en la nube.
• Construir interfaces y APIs de gestión seguras.
• Implementar barreras para impedir la denegación de los servicios, por ejemplo, por los llamados ataques «DoS/DDoS» y otros similares.
• Definir protocolos ante el robo o pérdida de dispositivos.

¿Qué requerimientos necesita una plataforma SaaS para gestionar contratos de manera segura?

Los documentos que vas a almacenar y gestionar contienen información sensible de tu empresa, por lo que una solución de este tipo debe contar con distintas características enfocadas a mantener la seguridad e integridad de todos los archivos que se alojen en ella:

Navegación segura: En todo momento se debe navegar un sitio con certificado *SSL (Secure Sockets Layer),* lo que indica que se ha verificado la identidad de sus propietarios y se codifica con tecnología *SSL* toda la información que se envía al servidor.

Almacenamientos de datos: Al existir múltiples usuarios, la plataforma tiene que ser capaz de aislar de manera individual la información de cada uno de ellos.

Además, requiere utilizar cifrado de datos -para protegerlos ante una eventual pérdida- de tal forma que no puedan ser leídos por usuarios no autorizados.

Control de acceso: La aplicación debe permitir a los administradores tener un control exhaustivo sobre quienes pueden acceder a los datos.

Esto se logra mediante una autorización en distintos niveles, para que un usuario pueda colaborar específicamente en los documentos que se le han compartido.

Además, el administrador requiere herramientas para gestionar las distintas cuentas y acceso a los registros de las acciones que han sido realizadas, con las que podrá efectuar (y enfrentar) una auditoría.

Finalmente, si un usuario se equivoca un número determinado de veces al ingresar, su cuenta y dirección IP deben bloquearse, a la espera de verificar la situación.

Seguridad en contraseñas y sesiones

Cada cierto tiempo es recomendable que los usuarios renueven sus contraseñas y que sus sesiones se cierren automáticamente. Estas son dos opciones que el administrador debe poder configurar en la plataforma.

Adicionalmente, el sistema tiene que tener la capacidad de solicitar a los usuarios que creen contraseñas seguras. Este formato usualmente exige una longitud de 8 caracteres, el uso de mayúsculas, minúsculas y de un número.

Copias de seguridad y medidas para recuperar datos

Una plataforma *SaaS* de este tipo tiene que generar respaldos de seguridad diarios e incrementales en la nube:

Que permitan recuperar los datos rápidamente en caso de pérdidas o daños. Que utilicen la última tecnología, por ejemplo, *Amazon AWS S3 Versioning.*

Protección de los datos

El sistema debe cuidar la totalidad de la información en todas sus etapas.

Desde la protección contra la modificación o eliminación de documentos por intrusos -a través de un acceso no autorizado- hasta garantizar la transmisión efectiva de los datos desde su origen hasta el destino correspondiente.

Transferencia de datos

Como dijimos, cuando la información **«viaja»** de un lugar a otro, una plataforma de esta naturaleza tiene que asegurar que los documentos no sean modificados ni eliminados por un tercero.

Es imprescindible que exista una verificación de identidad tanto en la parte emisora como en la receptora, buscando prevenir eventuales ataques *DNS*, *MITM (Man In The Middle)* o suplantación de IP.

Como los contratos de tu negocio contienen información valiosa para su desarrollo, la ciberseguridad no puede ser un tema dejado al azar. Por eso, es clave elegir una plataforma que cuente con estándares de seguridad de clase mundial, para así aprovechar todos los beneficios que entrega utilizar una plataforma de gestión de contratos en la nube.

webdox

¿Cómo funciona la Ciberseguridad en la Nube?

www.webdox.cl

La Concepción 266, Piso 5.
Oficinas 504/503 Santiago, Chile