Tendencias en ciberseguridad

Cifrado homomórfico

El cifrado homomórfico es un mecanismo que permite **externalizar el procesado de datos sensibles** a entornos no confiables tales como la nube. Dado que los datos se encuentran cifrados, se garantiza su confidencialidad mientras se procesan y realizan cálculos sobre los mismos. Esta tendencia de cifrado permite que la información que se codifique pueda ser compartida con terceras partes y ser utilizada en cálculos y procesos computacionales sin que los sistemas implicados puedan interpretar dicha información pero sí ofrecer un resultado a esos cálculos y procesos.

ORIGEN DE LA TENDENCIA

ECONÓMICO/EMPRESARIAL | DEMANDA | NORMATIVA | TECNOLOGÍA

La criptografía y el criptoanálisis se ha convertido en una potente arma que muchos Gobiernos usan para conseguir **ventaja táctica y acceder a fuentes de información diversas**. La seguridad de la información personal y confidencial en tránsito se ha convertido en un foco de atención en numerosas empresas. Cada vez se producen más **infracciones que suponen un alto coste económico** como resultado de los fallos de seguridad en relación con la información que de forma inadvertida se revelan a través, sobretodo, de la tecnología móvil. Además, el **mayor control del cumplimiento de la legislación de protección de datos** está impulsando un significativo aumento en la adopción de soluciones de cifrado en tiempo real para garantizar la seguridad de la información que se envía a través de transacciones. Por otro lado, la técnica de cifrado homomórfico abre una puerta de actuación para la implementación de seguridad en los procesos de voto electrónico remoto

UBICACIÓN EN LA CADENA DE VALOR DE LA CIBERSEGURIDAD

Fabricación | Comercialización | **Servicios**

La oferta de servicios o aplicaciones de cifrado homomórfico se ubican entre el segundo y tercer eslabón de la cadena de valor de la ciberseguridad**. La comercialización y oferta de operaciones cifradas como parte de los servicios** basadas en la nube o como servicios de cifrado sobre Big Data serán los modelos más demandados dentro de dicha cadena.

IMPACTO EN BENEFICIARIOS

USUARIO/PARTICULAR	EMPRESAS	ADMINISTRACIÓN PÚBLICA
Impacto en usuarios ●●○	Impacto en proveedores ●●○	Impacto en gobiernos ●○○
El cifrado homomórfico, especialmente sobre entornos *cloud computing*, repercute positivamente en los usuarios aportando mayor **seguridad y privacidad** en el procesado de los datos cifrados y compartidos entre diferentes clientes para su análisis.	Las empresas proveedoras de servicios *cloud computing* cuyos datos son almacenados o tratados remotamente tienen la oportunidad de ofertar servicios de **valor añadido** cifrados. Además, las empresas especializadas pueden complementar dicho análisis sobre cifrado homomórfico.	El cifrado homomórfico aplicado a las análisis de información llevado a cabo por los diversos organismos públicos y especialmente por los **Cuerpos y Fuerzas de Seguridad del Estado**, proporcionan confidencialidad en investigaciones e información privada de ciudadanos.

CLASIFICACIÓN DE LA TENDENCIA

SOLUCIONES DE PREVENCIÓN | SOLUCIONES DE CONTROL | SOLUCIONES DE MITIGACIÓN

El cifrado en todas sus vertientes tiene carácter preventivo. El objetivo del cifrado se basa en evitar que sea pública la información, en este caso, intercambiada y procesada entre diferentes usuarios o entre usuarios y la nube. Concretamente, el cifrado homomórfico trata de facilitar que la información confidencial procesada se mantenga cifrada durante el proceso.

CICLO DE VIDA DE LA TENDENCIA

DESARROLLO | **INTRODUCCIÓN** | CRECIMIENTO | MADUREZ

Los principios en los que se fundamenta el cifrado homomórfico sirven como punto de partida para mejorar los sistemas de seguridad que almacenan y procesan datos sensibles. Esta garantía de protección deriva de la capacidad que tiene el sistema de realizar operaciones sobre datos cifrados. Desde finales de los años 70, los investigadores han defendido que el cifrado homomórfico es posible, sin embargo en la **actualidad existen pocas aplicaciones que realicen operaciones con este cifrado.**

Tendencias en ciberseguridad

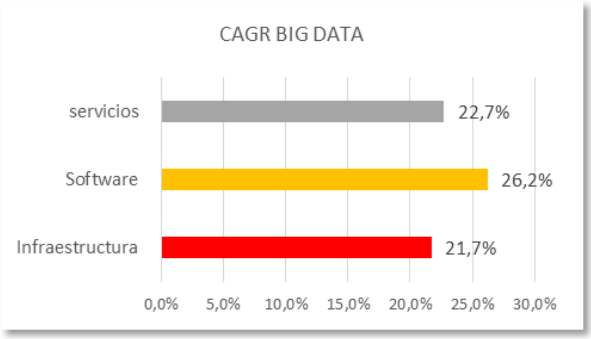
Cifrado homomórfico

ÁMBITO DE APLICACION

El cifrado homomórfico tiene aplicación en prácticamente todos los ámbitos digitales actuales (banca móvil, eHealth, Smart Grids, Smart Cities…) pero concretamente, adquiere especial relevancia como aplicación en el **cloud computing** como modelo que permite el acceso ubicuo, adaptado y bajo demanda en red, y en aplicaciones de **Big Data**, en referencia al procesado masivo de datos para descubrir patrones ocultos o correlaciones desconocidas manteniendo el anonimato de los datos.

CARACTERIZACIÓN DEL SECTOR

- Según las previsiones de la **Comisión Europea** el fomento del *cloud computing* crearía 2,5 millones de nuevos puestos de trabajo en Europa, y se traduciría en un incremento anual del PIB en la Unión igual a **160.000 millones** de euros, entre **2012 y 2020**. Un motivo suficiente como para buscar una especialización en este área para los profesionales TIC.
- Según IDC, **España** es el país europeo que mayor proporción de **ahorro de costes** ha experimentado en sus implementaciones *cloud computing*. De media, en 2015 las organizaciones españolas ahorraron en torno a un **15%**, aunque algunas empresas consiguieron superar el 50%.



- Según International Data Corporation (IDC), el mercado **Big Data llegará a generar un negocio** (gasto) de casi **50.000 millones de dólares para 2019**, con una **tasa de crecimiento medio anual compuesto (CAGR) del sector de hasta el 23,1%.**
- Concretamente, el **software de Big Data** será lo que más haga crecer el mercado en su conjunto, con un crecimiento medio anual del **26,2% entre 2014 y 2019**.
- Los dos sub-mercados restantes (Infraestructura y Servicios) se espera que crezcan durante el periodo 2015-2019 un 21,7% y 22,7%, respectivamente.

PREVISIONES DE DEMANDA

CRECIMIENTO

- Un estudio copatrocinado por Thales y publicado durante la conferencia de seguridad RSA 2016 revela que el **84 %** de los encuestados espera **transferir datos sensibles a la nube** en el año **2018**. Además, sólo el 15 % de los encuestados aseguraron no tener planes de cifrado.
- Se espera un crecimiento aproximado del **50% anual** en los **próximos cinco años** en el mercado de software de seguridad en la nube, según ReportsnReports.com.

CLIENTES

- Empresas con grandes sistemas de información y de gestión de datos.
- Empresas de seguridad y de oferta de servicios *cloud computing*.
- Empresas proveedoras de servicios de Internet.
- Organismos y universidades dedicadas a la investigación.
- Gobierno y Administraciones Públicas.

MODELOS DE NEGOCIO

DIFERENCIACIÓN EN COSTE | **DIFERENCIACIÓN EN PRESTACION DE SERVICIOS** | **DIFERENCIACIACIÓN EN VALOR AÑADIDO**

CASO DE ÉXITO

mit media lab

enigma

- **Enigma es una plataforma en la nube descentralizada con garantía de confidencialidad. Los datos privados se almacenan, comparten y se analizan sin ser revelados a cualquiera de las partes.** En la plataforma está involucrada la cadena de bloques además de una serie de técnicas que permiten proporcionar cifrado homomórfico.
- Una característica importante e innovadora del sistema Enigma es que permite el análisis de los datos almacenados por el sistema con aplicaciones externas, manteniendo los datos en sí de manera privada y bajo el control total de sus propietarios.
- Al igual que en Bitcoin, Enigma elimina la necesidad de una tercera parte de confianza, lo que permite un control autónomo de los datos personales.