Mes de la Ciberseguridad
Octubre 2021

EL IMPACTO DE LA MIGRACIÓN A LA NUBE EN LA CIBERSEGURIDAD Y LA TRANSFORMACIÓN DIGITAL

Encuentre su Punto Ciego

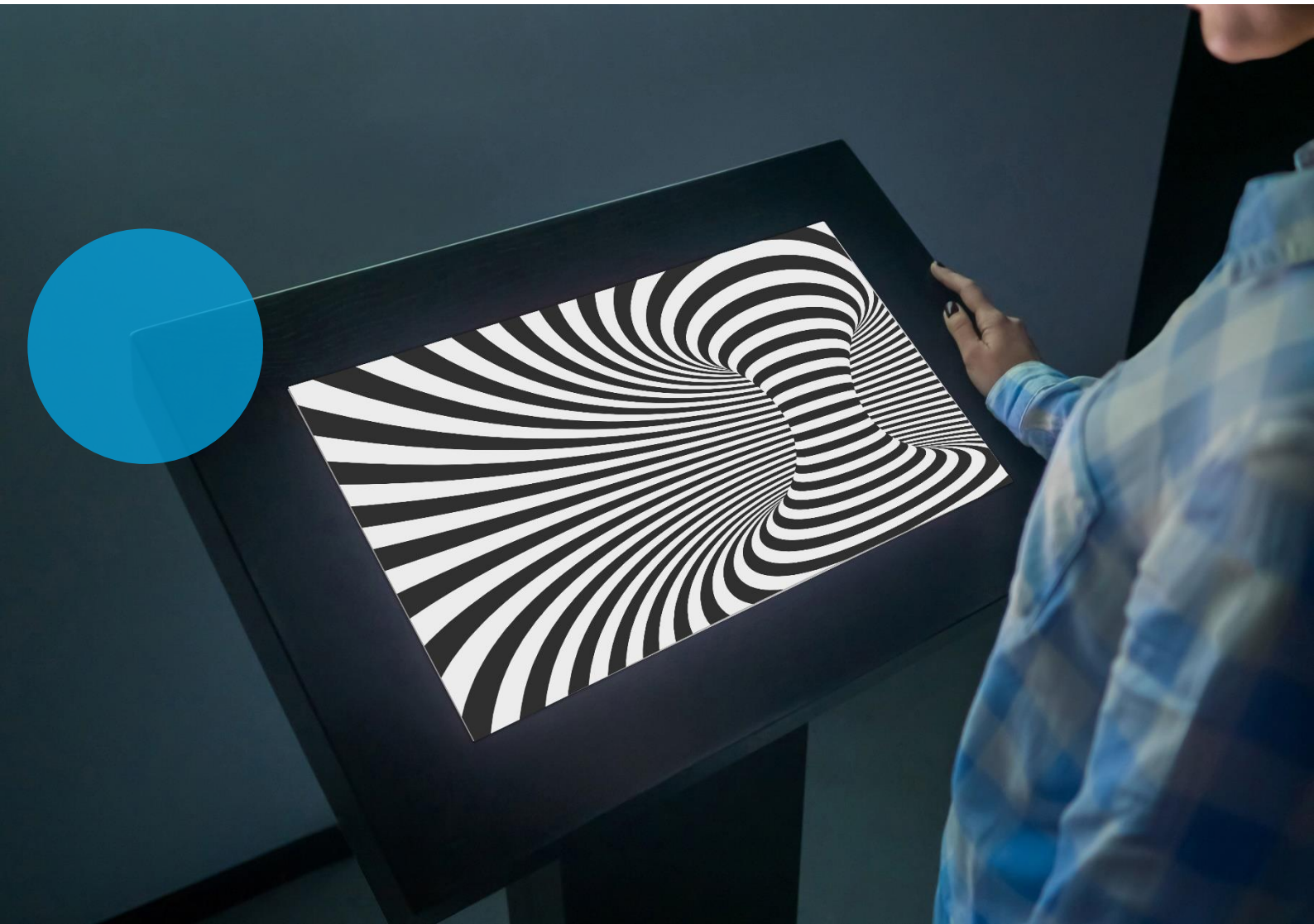
BDO

RESUMEN

La nube es uno de los principales factores que contribuyen a la transformación digital. La pandemia de COVID-19 y la consiguiente recesión económica han acelerado aún más el cambio a la computación en la nube en muchas organizaciones, mientras que los servicios modernos requieren continuamente la adquisición y el análisis de enormes volúmenes de datos y su traducción en información procesable. La computación en nube es una parte crucial de la ecuación que permite dar servicio y proteger dichos datos, lo que podría ser desafiante.

Hace tan sólo unos años, los clientes se veían obligados a implicarse a fondo en el desarrollo de aplicaciones internas y en la integración de las distintas plataformas que se niegan a comunicarse entre sí. En las últimas décadas se han desarrollado numerosos estándares con el objetivo de definir un "lenguaje de seguridad común" que permita una fácil integración de los distintos servicios. Esto incluye protocolos en ámbitos como el control de acceso, la autenticación y la autorización, la auditoría de seguridad centralizada y muchos más.

El auge de la computación en la nube ha permitido un cambio de paradigma en la forma de aplicar estos protocolos. Varios servicios basados en la nube pueden "hablar" entre sí utilizando estos protocolos estándar. Además, estos protocolos permiten a los principales proveedores ofrecer capacidades centrales de seguridad como un servicio, eliminando la necesidad de desarrollar dichas capacidades por separado. Este desarrollo reduce el tiempo y el esfuerzo necesarios para desarrollar, implementar y mantener nuevos servicios funcionales, garantizando al mismo tiempo una postura de seguridad mejorada.



PARTE 1: LA TRANSFORMACIÓN DIGITAL COMO ACELERADOR DEL CRECIMIENTO EN LA NUBE

VENTAJAS DE LA NUBE COMO INFRAESTRUCTURA PARA LA TRANSFORMACIÓN DIGITAL

La transformación digital se define como un "proceso que pretende mejorar una entidad desencadenando cambios significativos en sus propiedades mediante combinaciones de tecnologías de la información, la informática, la comunicación y la conectividad". [1]

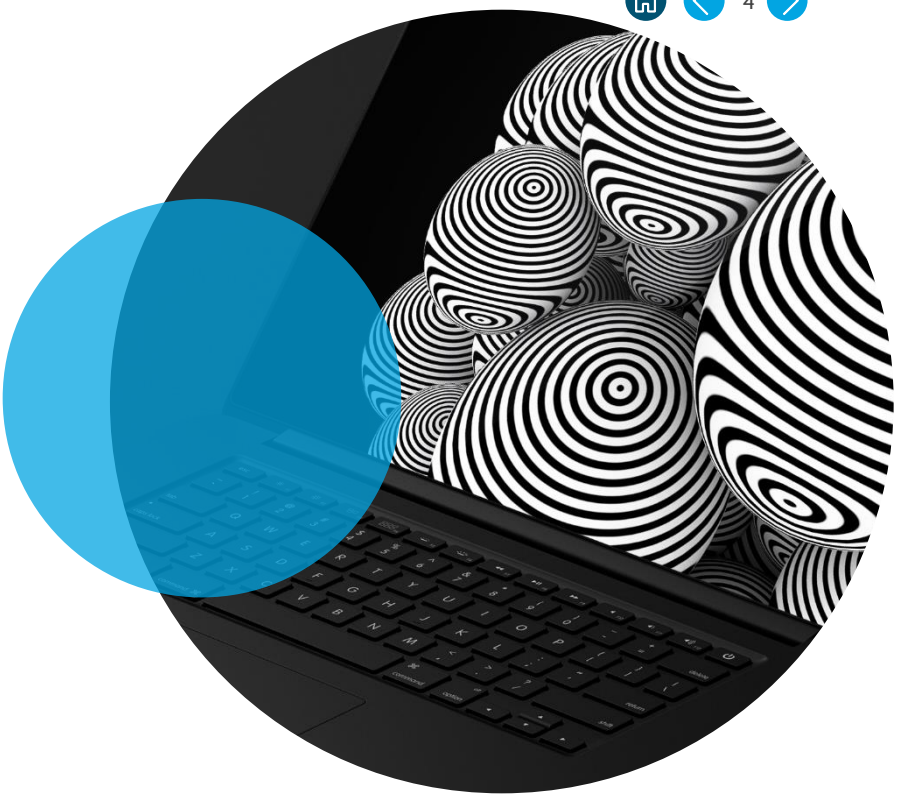
La transformación digital está afectando a muchos ámbitos de nuestras vidas, por ejemplo, la interacción con el gobierno ha cambiado drásticamente al dejar de utilizar el papel; las industrias de la música y las artes visuales han cambiado, ya que los artistas publican ahora sus creaciones directamente a través de las redes sociales y los servicios de streaming, la atención sanitaria ofrece ahora aplicaciones de "conversación con un médico" y el diagnóstico inicial del paciente puede hacerse a distancia, mientras que la investigación científica realiza simulaciones increíblemente complejas en un esfuerzo por evaluar los posibles tratamientos COVID-19[2] combinando los recursos de millones de ordenadores domésticos en la mayor avidez informática civil existente.

La computación en la nube contribuye en gran medida a la transformación digital. Permite la automatización de los procesos empresariales que hacen posible dichas transformaciones. En lugar de mantener sus propios y engorrosos centros de datos y su costosa infraestructura, una empresa puede aprovechar los recursos de la computación en la nube para acceder a una enorme potencia de cálculo, análisis de datos y otras capacidades a la carta, con un coste total de propiedad inferior al de las arquitecturas informáticas tradicionales. Esto no quiere decir que la nube sea necesariamente más barata, sino que el coste total de propiedad es amplio y debe tener en cuenta las actividades de I+D, el soporte técnico, la gestión de proyectos, el ciclo de vida del software y muchas más, además de los costes del hardware y del centro de datos (dependiendo de la estrategia de la nube que se utilice, que se explica más adelante).

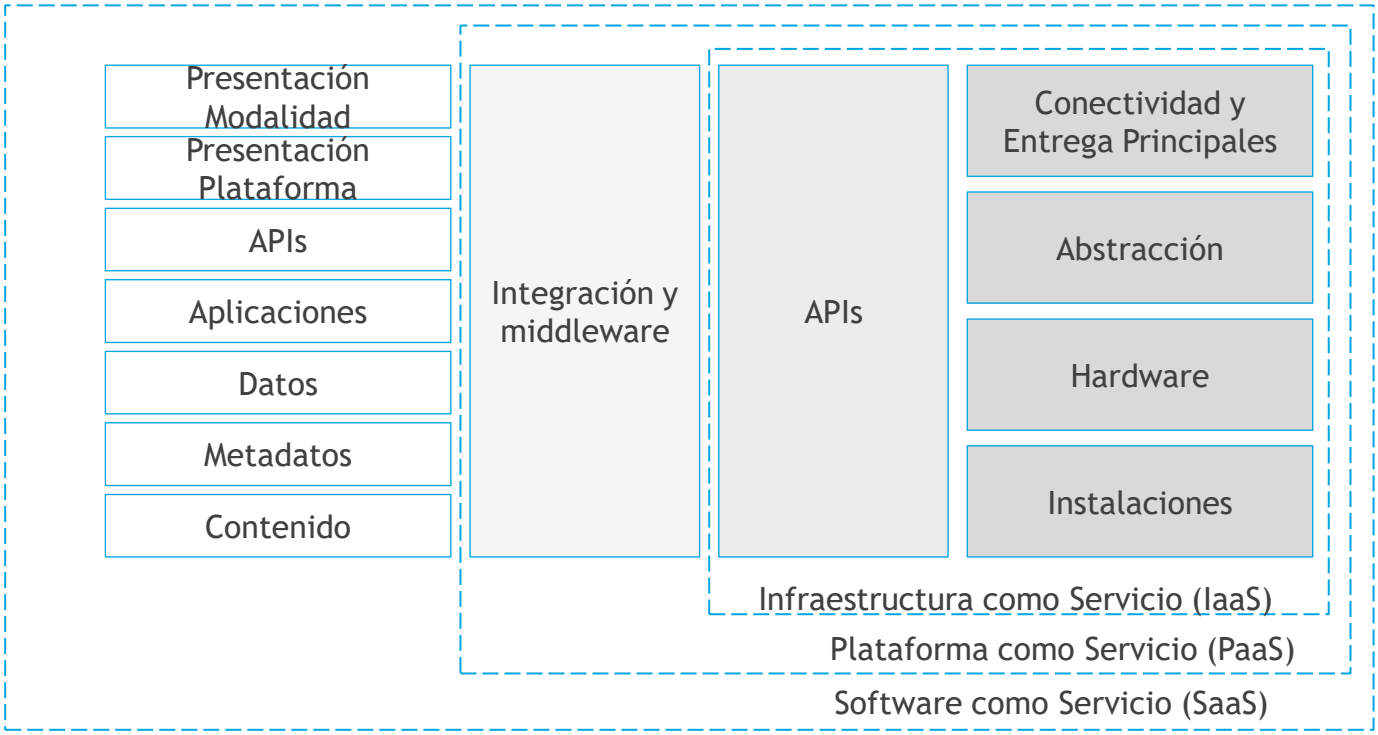
La computación en la nube es la base de empresas bien establecidas como Amazon, Uber, Spotify, Airbnb y Netflix. Estas organizaciones han utilizado la nube para crear modelos de negocio disruptivos, aprovechando su flexibilidad, escalabilidad y asequibilidad. Al mismo tiempo, las pequeñas empresas emergentes, creadas por emprendedores en el garaje de su casa, pueden poner en marcha rápidamente sus empresas utilizando las capacidades que ofrece la nube.

La computación en nube ofrece varias ventajas con las que las redes tradicionales tienen dificultades para competir, que van desde el mantenimiento mínimo o nulo de los servidores in situ, tiempos de despliegue más rápidos y menor sobrecarga y complejidad de la infraestructura.

1 Wolfswinkel, J. F., Furtmueller, E., and Wilderom, C. P. 2013. "Using grounded theory as a method for rigorously reviewing literature," European Journal of Information Systems (22:1), pp. 45-55.
2 Folding@Home project: https://foldingathome.org/



Una forma de ver la computación en nube es como una pila en la que el software como servicio (SaaS) se construye sobre la plataforma como servicio (PaaS), que a su vez se construye sobre la infraestructura como servicio (IaaS).[3]



3 Cloud Security Alliance Guidance - https://github.com/cloudsecurityalliance/CSA-Guidance/blob/master/Domain%201-%20Cloud%20Computing%20Concepts%20and%20Architectures.md

A continuación se presenta una breve descripción de cada capa, según la definición de la Cloud Security Alliance:

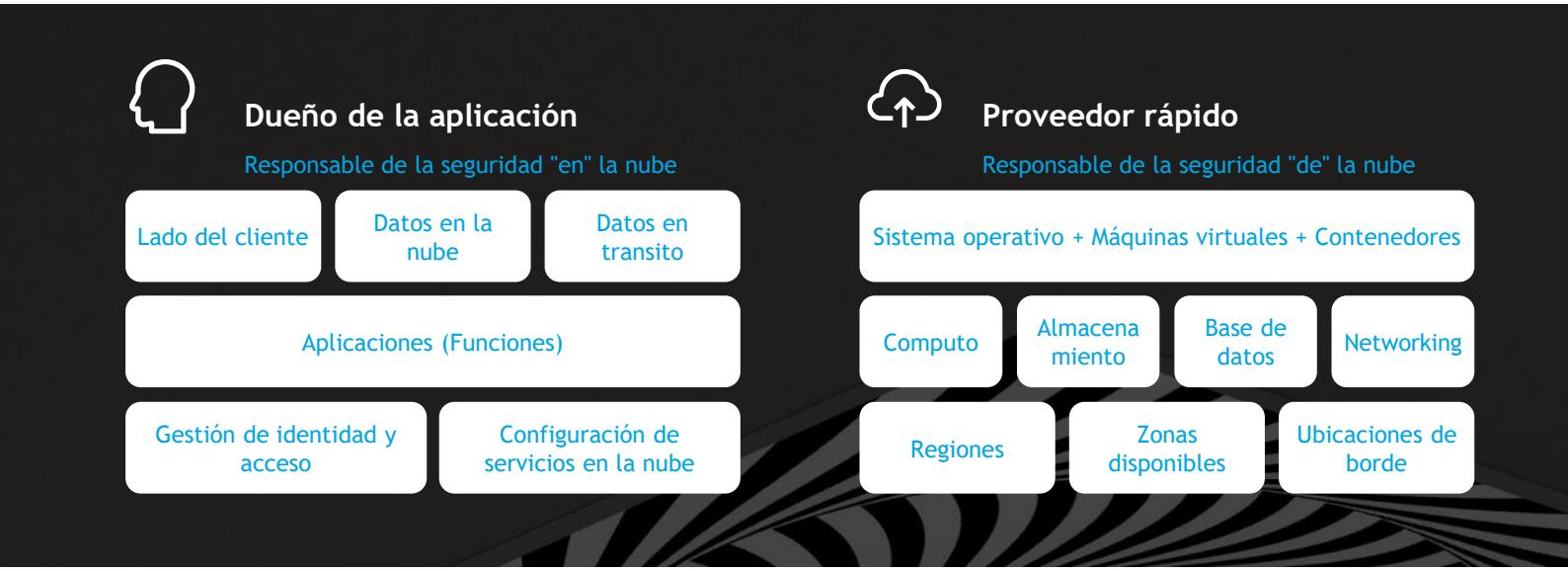
Infraestructura como servicio (IaaS): Con la computación en nube, abstraemos y ponemos en común estos recursos pero, en el nivel más básico, siempre necesitamos hardware físico, redes y almacenamiento para construir. Estos recursos se agrupan mediante la abstracción y la orquestación. La abstracción, a menudo a través de la virtualización, libera los recursos de sus limitaciones físicas para permitir la puesta en común. A continuación, un conjunto de herramientas básicas de conectividad y entrega (orquestación) une estos recursos abstraídos, crea los grupos y proporciona la automatización para entregarlos a los clientes.

La plataforma como servicio (PaaS) añade una capa adicional de integración con marcos de desarrollo de aplicaciones, capacidades de middleware y funciones como bases de datos, mensajería y colas. Estos servicios permiten a los desarrolladores desarrollar aplicaciones en la plataforma utilizando los lenguajes y herramientas de programación compatibles con la pila.

Software como Servicio (SaaS) los servicios SaaS son aplicaciones completas para múltiples inquilinos con todas las complejidades arquitectónicas de cualquier gran plataforma de software. Muchos proveedores de SaaS se basan en IaaS y PaaS debido a la mayor agilidad, resistencia y beneficios económicos (potenciales).

La mayoría de las aplicaciones modernas en la nube utilizan una combinación de IaaS y PaaS, a veces en diferentes proveedores de la nube.

La función como servicio es un concepto novedoso, comúnmente descrito como la capa superior de la pila. Las arquitecturas sin servidor (también conocidas como "FaaS" o Function as a Service) permiten a las organizaciones crear y desplegar software y servicios sin mantener ni aprovisionar ningún servidor físico o virtual. Las aplicaciones realizadas con arquitecturas sin servidor son adecuadas para una amplia gama de servicios y pueden escalar elásticamente a medida que crecen las cargas de trabajo en la nube. Desde el punto de vista del desarrollo de software, las organizaciones que adoptan arquitecturas sin servidor pueden centrarse en la funcionalidad principal del producto y prescindir por completo del sistema operativo subyacente, el servidor de aplicaciones o el entorno de ejecución del software. Al desarrollar aplicaciones utilizando arquitecturas sin servidor, los usuarios se liberan de la desalentadora tarea de aplicar continuamente parches de seguridad al sistema operativo subyacente y a los servidores de aplicaciones. En su lugar, estas tareas son ahora responsabilidad del proveedor de la arquitectura sin servidor. La imagen siguiente muestra el modelo de responsabilidades de seguridad compartidas, adaptado a las arquitecturas sin servidor.[4]



4 Cloud Security Alliance, The 12 Most Critical Risks for Serverless Applications

COVID-19 LA CRISIS COMO CATALIZADOR DE LA MIGRACIÓN A LA NUBE

De acuerdo con IDC,[5] 30% de las organizaciones europeas están planeando una migración agresiva a la nube como parte de su estrategia de TI a largo plazo. Esto demuestra por sí solo el papel fundamental de los servicios en la nube, que impulsan el desarrollo de nuevos modelos empresariales en todos los sectores.

Entonces llegó la COVID-19, una pandemia que puso el mundo patas arriba y cambió las prácticas empresariales para siempre, trasladando el lugar de trabajo de las oficinas tradicionalmente centralizadas a sus propias oficinas personales en casa. El estado de cosas provocado por la pandemia ha resultado ser un acelerador de algunas tendencias que ya estaban identificadas, y otras que ya estaban en marcha.

Un estudio realizado por LogicMonitor [6] reveló que el 87% de los responsables de la toma de decisiones de TI citan la COVID-19 como la razón del futuro aumento de la migración a la nube. Casi tres cuartas partes de los encuestados creen que en los próximos cinco años, el 95% de todas las cargas de trabajo se ejecutarán en entornos de nube.

El estudio marca un cambio drástico con respecto a un estudio de 2017 en el que LogicMonitor realizó una encuesta similar en la que solo el 13% de todos los encuestados afirmó que no creía que el cambio a la migración a la nube se produjera nunca; el 62% creía que el 95% de las cargas de trabajo se ejecutaría en entornos de nube en cinco o más años.

5 IDC, COVID-19 Tech Impact in Europe: The Journey to Recovery - Analyzing 3 Waves of Sentiment Survey Data. https://www.idc.com/getdoc.jsp?containerId=EUR146296920

6 Logic Monitor, Cloud 2025: The future of workloads in a cloud-first, post-COVID-19 world. https://www.logicmonitor.com/resource/cloud-2025

EL VALOR Y EL VOLUMEN EXPONENCIAL DE LOS DATOS

En Big Data, la revolución[7], los autores explican por qué el tamaño de los conjuntos de datos es importante y para qué puede utilizarse: "La capacidad de la sociedad de aprovechar la información de formas novedosas para producir conocimientos útiles o bienes y servicios de valor significativo", y "... cosas que se pueden hacer a gran escala que no se pueden hacer a menor escala, para extraer nuevos conocimientos o crear nuevas formas de valor".

La naturaleza de los big data se describe habitualmente con las siguientes características("5 Vs"):

- **Volumen** - el volumen de datos que gestionan las empresas se disparó en torno a 2012, cuando las organizaciones empezaron a recopilar más de tres millones de datos al día. Desde entonces, ¡el volumen se duplica casi cada 40 meses!
- **Velocidad-** Además de la gestión de los datos, las organizaciones se miden a menudo por su capacidad de proporcionar datos rápidamente, lo más cerca posible del tiempo real. La velocidad puede ser más importante que el volumen, ya que puede dar a las organizaciones una mayor ventaja competitiva.
- **Variedad** - Una empresa puede obtener datos de muchas fuentes diferentes: desde los dispositivos internos hasta la tecnología GPS de los smartphones, o utilizando lo que la gente dice en las redes sociales. La importancia de estas fuentes de información varía en función de la naturaleza del negocio, y los puntos de datos suelen aumentar exponencialmente con el tiempo.
- **Veracidad-** La veracidad en este contexto equivale a la calidad. Tenemos todos los datos, pero ¿podríamos estar pasando algo por alto? ¿Son los datos "limpios" y precisos? ¿Son útiles?
- **Valor** - el valor se sitúa en la cúspide de la pirámide de Big Data, refiriéndose a la capacidad de transformar un tsunami de datos en un valioso activo empresarial.

La adquisición y el análisis de esas enormes cantidades de datos y su transformación en conocimientos procesables se extienden mucho más allá del centro de datos tradicional, hasta el borde y la nube como un entorno híbrido sin fisuras. La utilización de dispositivos de borde, almacenamiento y análisis centralizados, junto con las metodologías de aprendizaje profundo que aceleran el procesamiento de datos a escala, requieren un nuevo enfoque tecnológico.

Un estudio realizado por Splunk[8] señala que dos tercios de las organizaciones participantes esperan que la cantidad de datos se quintuplique de aquí a 2025. En la encuesta participaron más de 2.000 directivos de empresas y de TI de todo el mundo, procedentes de Estados Unidos, Europa, China, Australia y Japón.

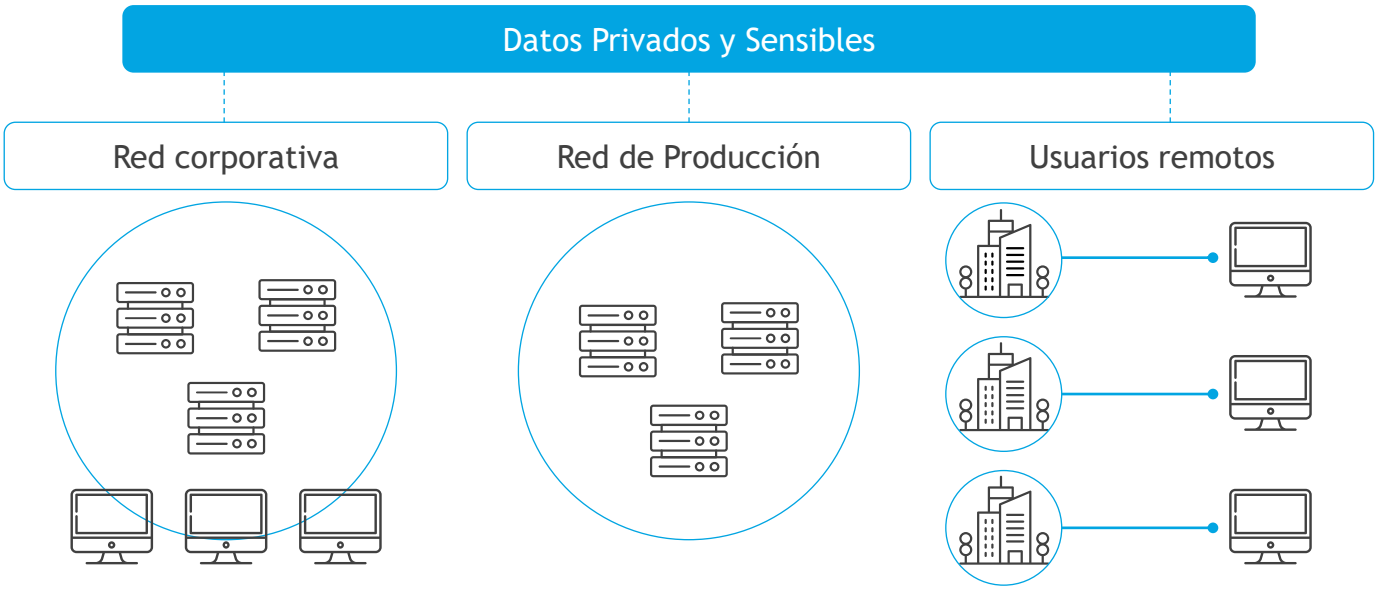
Para prosperar en esta nueva era, todas las organizaciones necesitan una visión completa de sus datos, un panel de información en tiempo real con la capacidad de tomar medidas en tiempo real. El estudio cuantifica la aparición de la Era de los Datos y la constatación de que las organizaciones aún tienen mucho trabajo por hacer para utilizar los datos con eficacia y tener éxito. Entre las principales percepciones expresadas por los participantes en el estudio se encuentran:

- Los datos son extremadamente valiosos para las organizaciones en términos de éxito general (81%), innovación (75%) y ciberseguridad (78%).
- El 66% de los responsables de TI y de las empresas afirman que la mitad o más de los datos de su organización son oscuros (no explotados, desconocidos, no utilizados), lo que supone un aumento del 10% con respecto al año anterior.
- El 57% afirma que el volumen de datos está creciendo más rápido que la capacidad de su organización para acomodarlos.
- El 47% reconoce que sus organizaciones se quedarán atrás ante el rápido crecimiento del volumen de datos.

7 Mayer-Schönberger, V., & Cukier, K. (2014). Big Data: A Revolution that Will Transform How We Live. Work, and Think, 2.
8 Splunk. The data age is here. Are you ready? https://www.splunk.com/en_us/campaigns/data-age.html

ANTIGUA FRONTERA VS. NUEVA FRONTERA NUEVA FRONTERA

Antiguamente, las organizaciones solían estar compuestas por un perímetro externo con una red interna de confianza y algunos entornos satélite (oficinas laterales y usuarios remotos). La frontera entre las redes internas de confianza y las externas no confiables era muy clara. Todos los datos residían dentro del perímetro organizativo, en centros de datos cerrados y seguros. El siguiente gráfico muestra el aspecto de una arquitectura de red organizativa típica:



Hoy en día, las organizaciones modernas se componen de entornos híbridos con aplicaciones y servicios que a menudo abarcan la nube, los recursos en el lugar, el borde y el punto final. Esto significa que los riesgos para la seguridad de la información pueden originarse igualmente en cada parte de la red de la organización, difuminando las líneas entre los controles de seguridad internos y externos, como se ve en el gráfico:

La Cloud Security Alliance (CSA) trazó un mapa de las principales amenazas a la computación en nube. [9] El último informe destaca las once más importantes, clasificadas por orden de importancia según los resultados de la encuesta:

1. **Violación de datos** - Los ciberatacantes van detrás de sus datos -sobre todo de la información personal- y los datos accesibles a través de Internet son más vulnerables y fáciles de explotar cuando están mal configurados. A medida que más datos se trasladan a la nube, la mitigación eficaz de los riesgos suele comenzar con la pregunta: "¿Quién puede acceder a esto?"
2. **Configuración errónea y control de cambios inadecuado - Configuraciones erróneas** - incluyendo la concesión de permisos excesivos o credenciales por defecto no modificadas - ocurren cuando los activos informáticos y el acceso se configuran incorrectamente. La configuración incorrecta de los recursos en la nube es una de las principales causas de las violaciones de datos y puede dar lugar a la eliminación o modificación de recursos, así como a la interrupción del servicio. La naturaleza dinámica de la nube hace que los enfoques tradicionales de cambio de control para una configuración adecuada sean extremadamente difíciles.
3. **Falta de arquitectura y estrategia de seguridad en la nube** - En todo el mundo, las organizaciones están migrando partes de su infraestructura de TI a nubes públicas. Uno de los mayores retos durante esta migración es la implementación de una arquitectura de seguridad adecuada para resistir los ciberataques. Por desgracia, este proceso sigue siendo un misterio para muchas organizaciones. Conjuntos enteros de datos están expuestos a diversas amenazas cuando las organizaciones asumen que la migración a la nube es un esfuerzo de "levantar y cambiar" simplemente portando su pila de TI y controles de seguridad existentes a un entorno de nube. La falta de comprensión del modelo de responsabilidad de seguridad compartida es otro factor que contribuye.
4. **Insuficiente gestión de identidades, credenciales, accesos y claves** - La nube introduce una serie de cambios y retos relacionados con la gestión de identidades y accesos (IAM) y, en particular, con la gestión de accesos privilegiados (PAM), ya que las credenciales privilegiadas asociadas a los usuarios humanos, así como a las aplicaciones y a las identidades de las máquinas, son excepcionalmente poderosas y muy susceptibles de ser comprometidas en los entornos de la nube.
5. **Secuestro de cuentas** - Utilizando métodos de phishing, explotación de vulnerabilidades o credenciales robadas, los atacantes malintencionados están a la caza de medios eficaces para acceder a cuentas altamente privilegiadas en la nube, por ejemplo, cuentas de servicios en la nube o suscripciones. El secuestro de cuentas y servicios significa un compromiso total: el control de la cuenta, sus servicios y los datos que contiene. Las consecuencias de este tipo de ataques pueden ser graves, desde importantes interrupciones operativas y empresariales hasta la eliminación completa de los activos, los datos y las aptitudes de la organización.
6. **Amenaza interna** - Las personas con información privilegiada maliciosa pueden ser empleados actuales o antiguos, contratistas u otros terceros de confianza que utilizan su acceso para actuar de forma que pueda afectar negativamente a la organización. Dado que los iniciados tienen acceso legítimo, identificar los posibles problemas de seguridad puede ser extremadamente difícil y a menudo implica un costoso proceso de corrección.
7. **Interfaces inseguras y APIs** - Los proveedores de computación en nube exponen un conjunto de interfaces de usuario de software (UI) y API para permitir a los clientes gestionar e interactuar con los servicios en nube. La seguridad y la disponibilidad de los servicios generales en la nube suelen depender del nivel de seguridad y la madurez de dichas API.

9 CSA. Top Threats to Cloud Computing: The egregious 11 https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/

8. **Plano de control débil** - La migración de los centros de datos a la nube plantea algunos retos para crear un programa de almacenamiento y protección de datos suficiente. Los usuarios deben ahora desarrollar nuevos procesos para la duplicación, la migración y el almacenamiento de los datos y -cuando se utiliza la multi-nube- se añade otra capa de complejidad. Una capa de control bien definida debería ser la solución para estos problemas, ya que permite la seguridad e integridad necesarias para complementar la estabilidad y el tiempo de ejecución de la capa de datos.
9. **Fallos en la metaestructura y en la estructura de aplicación** - Los proveedores de servicios en la nube revelan habitualmente las operaciones y las protecciones de seguridad que son necesarias para implementar y proteger sus sistemas con éxito. Normalmente, las llamadas a la API revelan esta información, y las protecciones se incorporan a la capa de metaestructura del CSP. La metaestructura se considera la línea de demarcación entre el CSP y el cliente, también conocida como la línea de flotación.
10. **Visibilidad limitada del uso de la nube** - La visibilidad limitada del uso de la nube se produce cuando una organización no posee la capacidad de visualizar y analizar si el uso de los servicios en la nube dentro de la organización es seguro o malicioso.
11. **Abuso y uso nocivo de los servicios en la nube** - Los actores maliciosos pueden aprovechar los recursos de computación en la nube para atacar a usuarios, organizaciones u otros proveedores de la nube. Los atacantes maliciosos también pueden alojar malware en los servicios en la nube. Los servicios en la nube que alojan malware pueden parecer más legítimos porque el malware utiliza el dominio del CSP. Además, el malware alojado en la nube puede utilizar las herramientas para compartir la nube como vector de ataque para seguir propagándose.

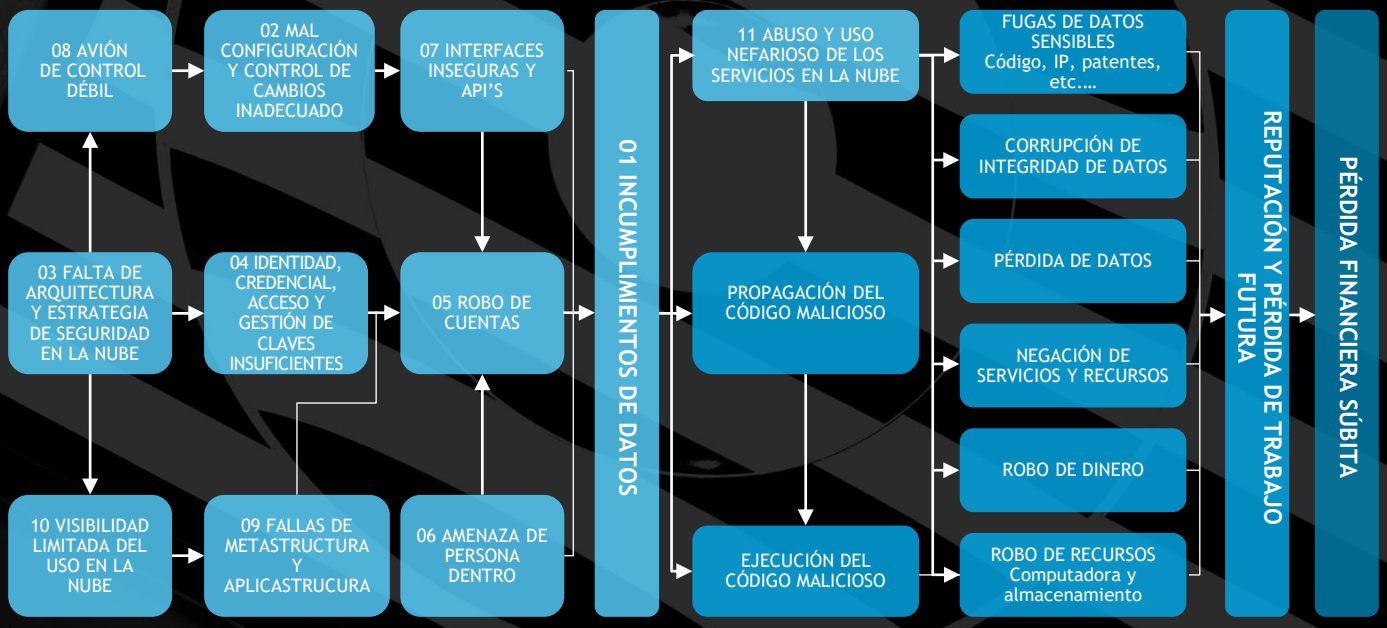
La mayoría de las amenazas "Egregias" presentadas anteriormente pueden dar lugar a los siguientes escenarios de riesgo::

- **Propagación de códigos maliciosos** - Ya sea en una sola máquina virtual o en todo un entorno, la propagación del código malicioso es un multiplicador de potencia en cualquier ciberataque.
- **Ejecución de código malicioso** - La ejecución de un código malicioso por parte de un atacante en un incidente de seguridad del mundo real.

Ambas situaciones de riesgo se pueden concretar en los siguientes incidentes del mundo real:

- Fuga de datos sensibles;
- Corrupción de la integridad de los datos;
- Pérdida de datos;
- Denegación de servicios y recursos;
- Robo de dinero;
- Robo de recursos.

El siguiente gráfico muestra las amenazas "Egregious Eleven" y su implicación en cascada en el estado de la seguridad de la información:



PARTE 2: ESTANDARIZACIÓN IMPULSADA POR LA NUBE

DE LA TRANSFORMACIÓN DIGITAL A LA PERSONALIZACIÓN IMPULSADA POR LA NUBE

Como se ha comentado en los capítulos anteriores, las antiguas fronteras de la informática local, que utiliza una potencia de cálculo y una capacidad de almacenamiento limitadas, han desaparecido. Hoy en día, la mayoría de las organizaciones buscan un almacenamiento y una potencia de cálculo flexibles, que puedan escalar y crecer con la organización, al tiempo que permiten la adquisición y el análisis de enormes cantidades de datos y su transformación en información procesable. El escenario de los "grandes datos" llegó para quedarse, y la computación en nube satisface todas sus necesidades.

Con la migración a la nube, surge un nuevo problema: La organización no controla sus aplicaciones y la forma en que se comunican entre sí. Sorprendentemente, este problema se convierte en una gran oportunidad: Para tener éxito y vender soluciones en la nube, los proveedores de servicios en la nube tuvieron que buscar un lenguaje común, que de otro modo daría lugar a una moderna Torre de Babel.

Por suerte, muchos de esos estándares ya existían cuando los CSP cobraron protagonismo. Esos estándares estuvieron esperando ahí fuera durante años, algunos incluso décadas, hasta que la industria se unió para adoptarlos, haciendo que el cambio de la nube fuera lo correcto en el momento adecuado. Los estándares que tanto tiempo llevaban esperando encontraron el lugar que les correspondía en la historia.

LA ARQUITECTURA HÍBRIDA COMO CATALIZADOR DE LA INVERSIÓN EN CIBERSEGURIDAD

La amplia adopción de plataformas basadas en la nube está generando un cambio significativo en la forma de enfocar las tecnologías de infraestructura y las aplicaciones empresariales.

En la nueva realidad actual, ya no hay grandes integraciones técnicas y la mayoría de los proyectos relacionados con los datos pueden considerarse proyectos de personalización, con la integración realizada en segundo plano por los proveedores de servicios en la nube; para implantar una nueva solución empresarial, la organización sólo tiene que gestionar y aplicar los cambios organizativos.

CAMBIOS DE RESPONSABILIDAD

Como se ha descrito anteriormente, existen cuatro modelos de arquitectura en la nube: Infraestructura como Servicio (IaaS), Plataforma como Servicio (PaaS), Software como Servicio (SaaS) y Función como Servicio (FaaS). Cada modelo distribuye la responsabilidad de forma diferente entre el consumidor de servicios en la nube (CSC) y el proveedor de servicios en la nube (CSP).[10]

El modelo de Infraestructura como Servicio (IaaS) ofrece la seguridad física, el hardware y la gestión de la virtualización como un servicio, sin embargo, el cliente sigue teniendo que realizar toda la configuración de seguridad necesaria, las tareas de gestión y los gastos generales de los componentes. Los clientes que despliegan hosts virtuales son responsables de la gestión del sistema operativo invitado, incluidas las actualizaciones del sistema operativo, los parches de terceros, el endurecimiento de la configuración de la seguridad de la red y la configuración segura de cualquier aplicación y utilidad instalada en las instancias. Es importante tener en cuenta que este modelo es muy parecido al antiguo, en el que los clientes debían gestionar la seguridad in situ. No se confunda, una brecha causada por una mala configuración del servidor en este modelo está bajo la total responsabilidad del cliente.

La plataforma como servicio (PaaS) ofrece servicios abstraídos, por ejemplo, base de datos como servicio, mecanismos de cola y cientos de servicios adicionales. Para este tipo de servicios, el CSP opera la capa de infraestructura, el sistema operativo y las plataformas, mientras que los clientes son responsables de la gestión de sus propios datos, la clasificación de los activos, la aplicación de los permisos adecuados y la adhesión a la política de cifrado de la organización.

Los mecanismos de seguridad subyacentes del software como servicio (SaaS) son, en teoría, responsabilidad total del CSP.

El modelo de responsabilidad compartida se extiende también a los controles informáticos. Al igual que la responsabilidad del funcionamiento del entorno informático se comparte entre el CSP y sus clientes, también la gestión, el funcionamiento y la verificación de los controles informáticos compartidos.

Para los entornos IaaS y PaaS, los proveedores ofrecen un amplio conjunto de módulos y herramientas, ya sea como parte integral del servicio o como una integración de terceros disponible en el mercado de CSP. Estos servicios pueden asegurar el entorno basado en la nube y/o otros entornos.

A continuación se muestra una representación del Modelo de Responsabilidad Compartida, inspirado en el CIS :

Responsabilidad	Clasificación de datos y rendición de cuentas	Protección de clientes y puntos finales	Gestión de identidades y Accesos	Controles a nivel de aplicación	Controles de red	Infraestructura del host	Seguridad física
En las instalaciones	●	●	●	●	●	●	●
IaaS	●	●	●	●	◒	◒	◎
PaaS	●	●	◒	●	◎	◎	◎
SaaS	●	◒	◒	●	◎	◎	◎
FaaS	●	◒	◒	●	◎	◎	◎

● Cliente en la nube ◎ Proveedor de nube

10 As a reference, see AWS' explanation of their shared responsibility mode here https://aws.amazon.com/compliance/shared-responsibility-model/

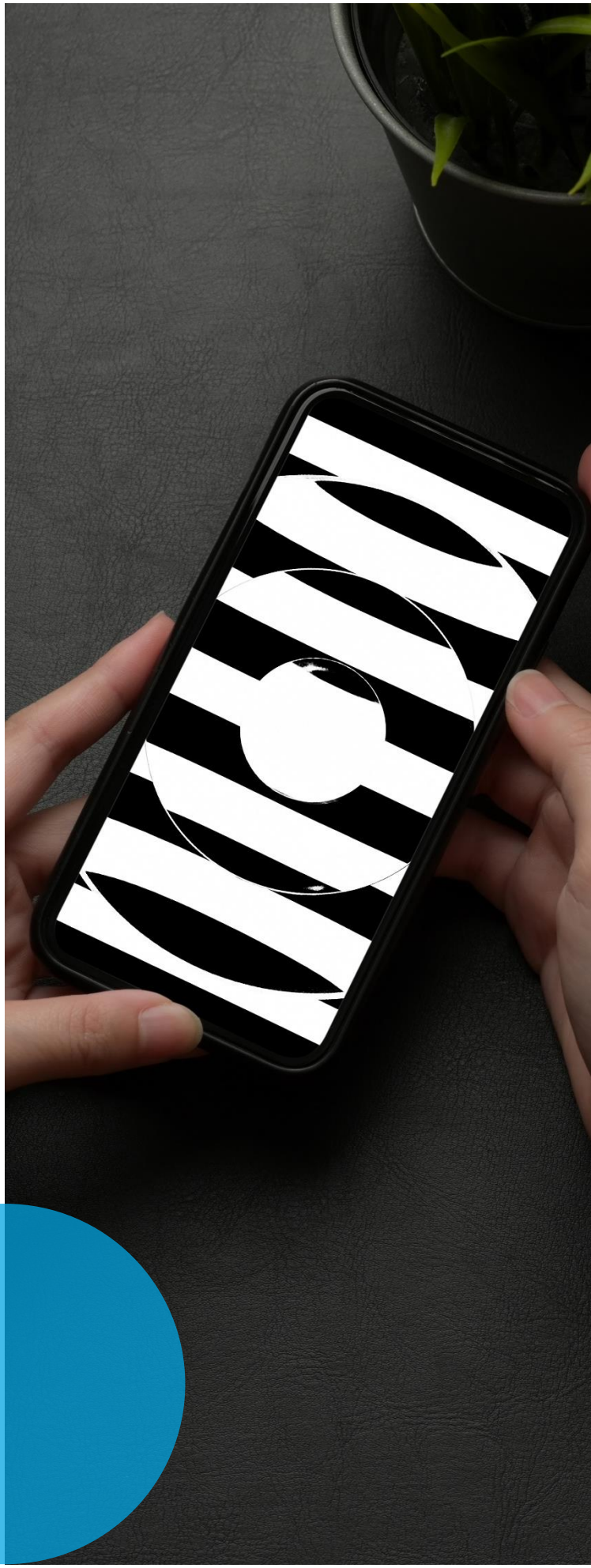
INTEGRACIÓN DE SERVICIOS EN LA NUBE: EL NUEVO ESTÁNDAR DE TI

Hace unos años, cada vez se adquiría más software y hardware y se utilizaba para el funcionamiento autónomo. Los clientes se esforzaban y se implicaban a fondo en el desarrollo de aplicaciones internas y en la integración de varias plataformas que se negaban a "hablar" entre sí.

Reconociendo el potencial de este nuevo cambio de paradigma, los consumidores de tecnologías y servicios de TI empezaron a exigir normas que les ayudaran en su transición a la computación en nube. Entre ellas se encuentran los conceptos y tecnologías fundamentales, la resolución de problemas operativos y las interacciones entre los entornos de computación en nube y otros sistemas distribuidos.

En el lado de los CSP, los proveedores se dieron cuenta de que la apertura es el nombre del juego. Los CSP empezaron a promover la estandarización de la gestión de identidades, CRM, SIEM y otros servicios importantes. El impacto de esta estandarización es innegable y ha hecho que las inversiones en ciberseguridad sean mucho más seguras.

En la era on-prem, la integración de aplicaciones internas y externas requería un enorme esfuerzo. Es especialmente complejo cuando se trata de integrar dos o más componentes diferentes en la misma arquitectura de seguridad, con cada uno de ellos utilizando protocolos diferentes, muchos de los cuales no estaban documentados y se mantenían como un secreto dentro de la cabeza del desarrollador, lo que convertía la tarea en algo casi imposible. La computación en nube está cambiando todo eso.



INTEGRACIÓN DE SERVICIOS EN LA NUBE: UN CAMBIO DE PARADIGMA PARA LA SEGURIDAD DE LA INFORMACIÓN

La seguridad en la nube protege la información almacenada, accedida y compartida en la nube. Es diferente de la seguridad de la red, principalmente por el hecho de que la nube se sitúa fuera de la red organizativa tradicional.

El uso de entornos en la nube permite a los equipos de TI externalizar la seguridad y el mantenimiento de la infraestructura. La computación en la nube está construida sobre un nuevo modelo, que permite las aplicaciones tanto en la nube como on-prem. Con las soluciones de seguridad basadas en la nube, ahora es posible separar la funcionalidad de seguridad de la lógica de la aplicación utilizando componentes comunes, probados y gestionados de forma centralizada. Estos componentes se denominan Seguridad como Servicio (SecaaS)[11]. Algunos ejemplos de servicios de seguridad comunes ofrecidos por varios CSP son :

- **Gestión de identidades y accesos (IAM)** permiten a los departamentos de TI garantizar que los entornos en la nube, on-prem e híbridos proporcionen el nivel correcto de acceso a las funciones y personas adecuadas en el momento adecuado. Las soluciones IAM se utilizan para gestionar el acceso a los recursos de la empresa asegurando que la identidad de una entidad se verifique y se conceda el nivel correcto de acceso basado en dicha identidad asegurada. La gestión de identidades y accesos puede gestionarse de forma centralizada mediante una solución basada en la nube (IDaaS). Este enfoque evita muchas de las complejidades y posibles lagunas de seguridad al crear conexiones con proveedores de SaaS para la autenticación y la gestión de cuentas. Algunos de estos servicios también pueden actuar como puente con la gestión de identidades o las herramientas de gestión de accesos en las instalaciones. Como resultado, muchos de los que adoptan IDaaS lo utilizarán para sustituir la IAM on-prem. El inicio de sesión único (SSO) suele combinarse con las soluciones IDaaS. Estos servicios ofrecen a los usuarios la posibilidad de acceder a todas sus aplicaciones empresariales en la nube, así como a algunas de sus aplicaciones locales, utilizando un único conjunto de credenciales de acceso. El SSO también ofrece a los administradores de TI y de la red mejores capacidades para supervisar el acceso y las cuentas.

  Con el auge de los protocolos de autenticación estándar, como SAML, OATH 2, Radius y Kerberos, la integración de varias aplicaciones se ha convertido en un proceso fácil y sin complicaciones. Hay que tener en cuenta que estos protocolos existían mucho antes de que se concibiera la noción de nube. Sin embargo, ahora están ampliamente adoptados.

  Gracias a estos protocolos abiertos, las soluciones de distintos proveedores pueden integrarse sin problemas. Por ejemplo: Oracle Cloud Infrastructure puede federarse con Azure Active Directory (AD) configurando Oracle Cloud Infrastructure como una aplicación básica de inicio de sesión único SAML en Azure AD. [12]

- **Prevención de la pérdida de datos (DLP)** son soluciones que supervisan, protegen y verifican la seguridad de los datos en reposo, en movimiento y en uso, tanto en la nube como en las instalaciones. Las soluciones de protección de datos on-prem no tienen visibilidad de los datos en los servicios en la nube como Office 365 y no pueden controlar la colaboración o el uso compartido dentro de la nube. Muchas organizaciones se plantean añadir una solución de protección de datos independiente para su entorno en la nube, pero al hacerlo, fragmentan sus políticas, mecanismos de información y respuesta a incidentes. Esto da lugar a una mayor sobrecarga operativa y a una protección de datos incoherente entre dispositivos, redes y servicios en la nube. Las soluciones de DLP basadas en la nube proporcionan una protección de datos unificada en los puntos finales, las redes y la nube, ofreciendo una experiencia de protección de datos unificada y minimizando el riesgo de pérdida de datos al tiempo que se maximiza la eficiencia operativa. Este tipo de soluciones son ofrecidas por numerosos proveedores, por ejemplo, Checkpoint, Code42, Digital Guardian, Fidelis, Forcepoint, McAfee, Proofpoint y Trend Micro.[13]

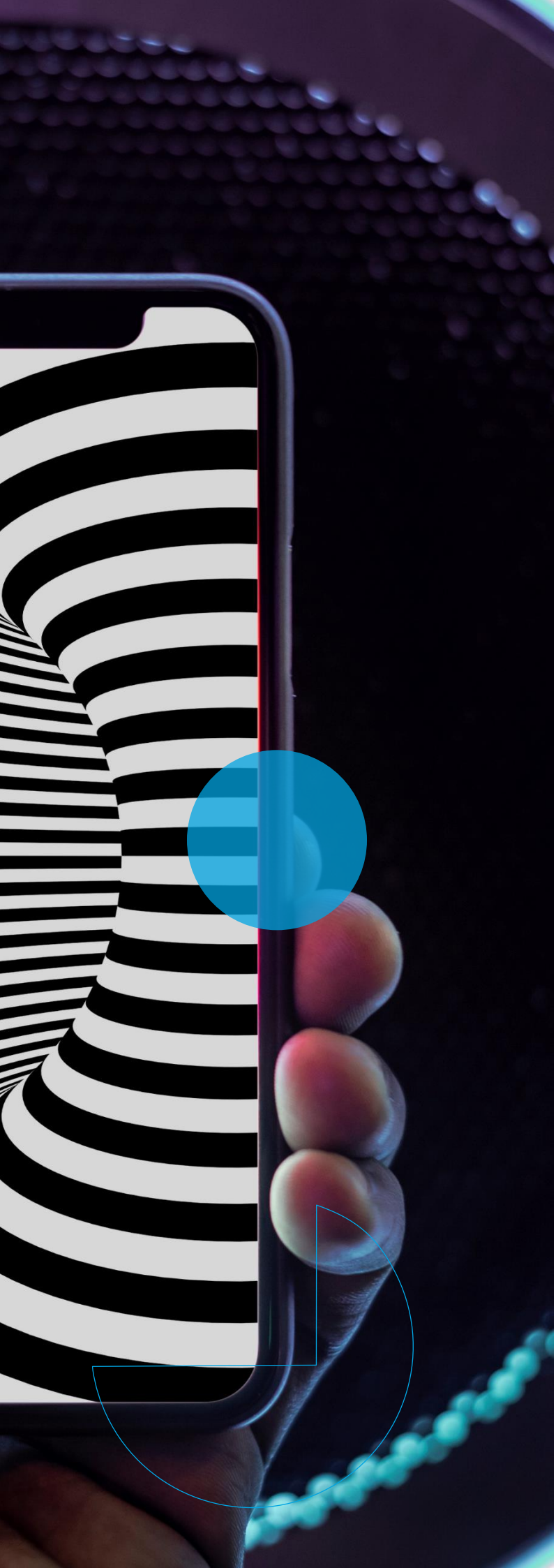
11 Cloud Security Alliance, Defined Categories of Service, https://s3.amazonaws.com/content-production.cloudsecurityalliance/dKyC3pQhxEsiXZjhVMcGWffg?response-content-disposition=inline%3B%20filename%3D%22SecaaS_V1_0.pdf%22%3B%20filename%2A%3DUTF-8%27%27SecaaS_V1_0.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAJ7D6HHC2YHBAPZ2Q%2F20201101%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20201101T171650Z&X-Amz-Expires=300&X-Amz-SignedHeaders=host&X-Amz-Signature=eedabcd1087cc9e54977a0892410d96d0072a5095fc1505462717b49e09ff75f

12 https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/federatingADFSazure.htm

13 https://www.esecurityplanet.com/products/top-dlp-solutions.html

- **Seguridad en la web** ¡Es una protección en tiempo real que se ofrece tanto en la empresa mediante la instalación de software/aparatos como en la nube mediante el proxy o la redirección del tráfico web al proveedor de la nube. Esto proporciona una capa adicional de protección sobre soluciones como la AV para evitar que el malware entre en la empresa a través de actividades como la navegación web. Las reglas de política en torno a los tipos de acceso a la web y los momentos en que son aceptables también pueden aplicarse a través de estas tecnologías. Los Cloud Web Gateways se gestionan de forma centralizada a través de la nube redirigiendo la web a través del proveedor de la solución. Protegen a las empresas bloqueando los virus en línea y filtrando los sitios web peligrosos. También proporcionan informes sobre el comportamiento de los usuarios en línea. Hay una gran variedad de plataformas de filtrado web que se adaptan a una gran variedad de casos de uso. Algunos ejemplos de proveedores que ofrecen Cloud Web Gateway son Zscaler, Symantec, Forcepoint y MacAfee.[14]
- **Seguridad del correo electrónico** proporciona control sobre el correo electrónico entrante y saliente, protegiendo así a la organización contra la suplantación de identidad y los archivos adjuntos malintencionados, aplicando políticas corporativas como el uso aceptable y el spam, y proporcionando opciones de continuidad del negocio. Además, la solución permite el cifrado del correo electrónico basado en políticas y la integración con varias soluciones de servidores de correo electrónico. Las firmas digitales que permiten la identificación y el no repudio son también características de numerosas soluciones de seguridad del correo electrónico. Algunos de los proveedores de pasarelas web mencionados a continuación también ofrecen Cloud Based Email Security como parte de su paquete de pasarelas.
- **Gestión de eventos e información de seguridad (SIEM)** Los sistemas aceptan (a través de mecanismos push o pull) información de registros y eventos. Esta información se correlaciona y analiza para proporcionar informes y alertas en tiempo real sobre incidentes/eventos que puedan requerir una intervención. Es probable que los registros se conserven de forma que se evite su manipulación, para permitir su uso como prueba en cualquier investigación. El SIEM basado en la nube (también conocido como servicio SIEM) está proporcionando a los equipos de TI una mayor comodidad, flexibilidad y potencia a la hora de gestionar las amenazas en múltiples entornos, tanto en la nube como en la propia empresa. El SIEM basado en la nube ofrece una forma eficaz y eficiente de supervisar constantemente todos los dispositivos, servidores, aplicaciones, usuarios y componentes de la infraestructura tanto en la red como en la nube, todo ello desde un panel central basado en la nube. Con una plataforma SIEM basada en la nube, se puede :
  - Supervise los sistemas, las aplicaciones y las cargas de trabajo, ya sean físicas o virtuales, en cualquier lugar de su red, ya sea en su centro de datos, en una nube privada o en una o varias nubes públicas;
  - Reciba alertas en tiempo real sobre incidentes de seguridad;
  - Servir de base para el análisis de riesgos y las auditorías;
  - Consolide y gestione los datos de los registros de seguridad y eventos
  - Automatizar los informes de cumplimiento.
- **Corredores de seguridad de acceso a la nube (CASBs)** son un conjunto integrado que ofrece una serie de servicios diseñados para ayudar a proteger la infraestructura de la nube. Los CASB se sitúan entre los consumidores de servicios en la nube y los proveedores de servicios en la nube para aplicar las políticas de seguridad, cumplimiento y gobernanza de las aplicaciones en la nube. Estas herramientas supervisan y actúan como seguridad para todas las aplicaciones en la nube de una empresa. Los CASB tienen cuatro ventajas clave, que Gartner denomina los "Cuatro Pilares de Funcionalidad":
  - **Visibilidad** : Los CASB centralizan el control de la seguridad en la nube y permiten al personal de seguridad supervisar toda la actividad en la nube, dentro y fuera de la red de la organización, incluidas las aplicaciones informáticas en la sombra y el acceso de los trabajadores remotos.
  - **Cumplimiento** : Los CASB pueden controlar la actividad de los usuarios para garantizar el cumplimiento de los requisitos normativos del sector, por ejemplo, HIPAA y PCI, y detectar si el uso de la nube supone una amenaza para el cumplimiento.
  - **Seguridad de los datos** : Los CASB aplican políticas de seguridad internas en relación con el cifrado, la tokenización y el acceso a los datos sensibles sin interferir con las funciones de la aplicación, como las capacidades de búsqueda. La mayoría de las soluciones CASB también pueden evitar la fuga de datos etiquetando determinados datos como sensibles, impidiendo su descarga o redactándolos. También pueden proporcionar plantillas a las organizaciones que actualmente no tienen políticas de DLP para identificar los datos sensibles.
  - **Protección contra amenazas** : Los CASB impiden que los usuarios y dispositivos no autorizados accedan a los servicios corporativos en la nube y protegen contra el malware, proporcionan información sobre amenazas y detectan anomalías.

14 https://www.expertinsights.com/insights/the-top-5-cloud-web-gateways-for-businesses/



RESUMEN Y CONCLUSIONES

En este capítulo, hemos revisado el impacto de la transformación digital en la proliferación de la computación en nube y en el establecimiento de interfaces y servicios estándar, permitiendo así una rápida integración entre los servicios manteniendo un alto nivel de seguridad.

La computación en nube permite recopilar y procesar enormes datos para luego procesarlos utilizando recursos prácticamente ilimitados. Aunque esto revela un sinfín de nuevas posibilidades, también plantea problemas de seguridad de la información. Estos incluyen, entre otros, las violaciones de datos debido a la exposición a Internet, la falta de una arquitectura segura y los insuficientes controles de identidad y acceso que, a su vez, pueden conducir a fugas de información sensible, corrupción de la integridad de los datos, pérdida de datos y robo de fondos y/o recursos. Todo lo anterior puede dar lugar, además, a una pérdida de reputación, que puede causar importantes pérdidas financieras.

Sin embargo, con una adecuada concienciación sobre la seguridad, las mejores prácticas de seguridad y las nuevas tecnologías, la computación en la nube puede ser tan segura como los servicios locales y, en muchos casos, incluso más.

Los estándares de los protocolos de seguridad han evolucionado durante la última década. Un ejemplo es SAML - Security Assertion Markup Language, desarrollado por OASIS en 2002. Con el aumento de la adopción de servicios basados en la nube, estos protocolos se están "soltando" ampliamente para abordar su intención original: construir un lenguaje común para los servicios de seguridad.

Estos estándares permiten un método rápido, fácil y seguro para que los servicios se comuniquen entre sí. Además, permiten separar completamente los componentes de seguridad de la aplicación, y ofrecen servicios externos de autenticación segura, por ejemplo, Single Sign On, seguridad web y auditoría de seguridad.

Creemos que una combinación de normas bien definidas, junto con servicios novedosos, modernos e innovadores, puede facilitar la rápida introducción de estos servicios sin necesidad de reinventar los componentes de seguridad, manteniendo un alto nivel de seguridad.

OPHIR ZILBIGER

Líder Global de Cibernética
Socio, Director del Centro de Ciberseguridad
BDO Israel
OphirZ@bdo.co.il

GILAD YARON

Director
Director de Privacidad & GRC
Centro de Ciberseguridad de BDO, Israel
GiladY@bdo.co.il

www.bdo.global