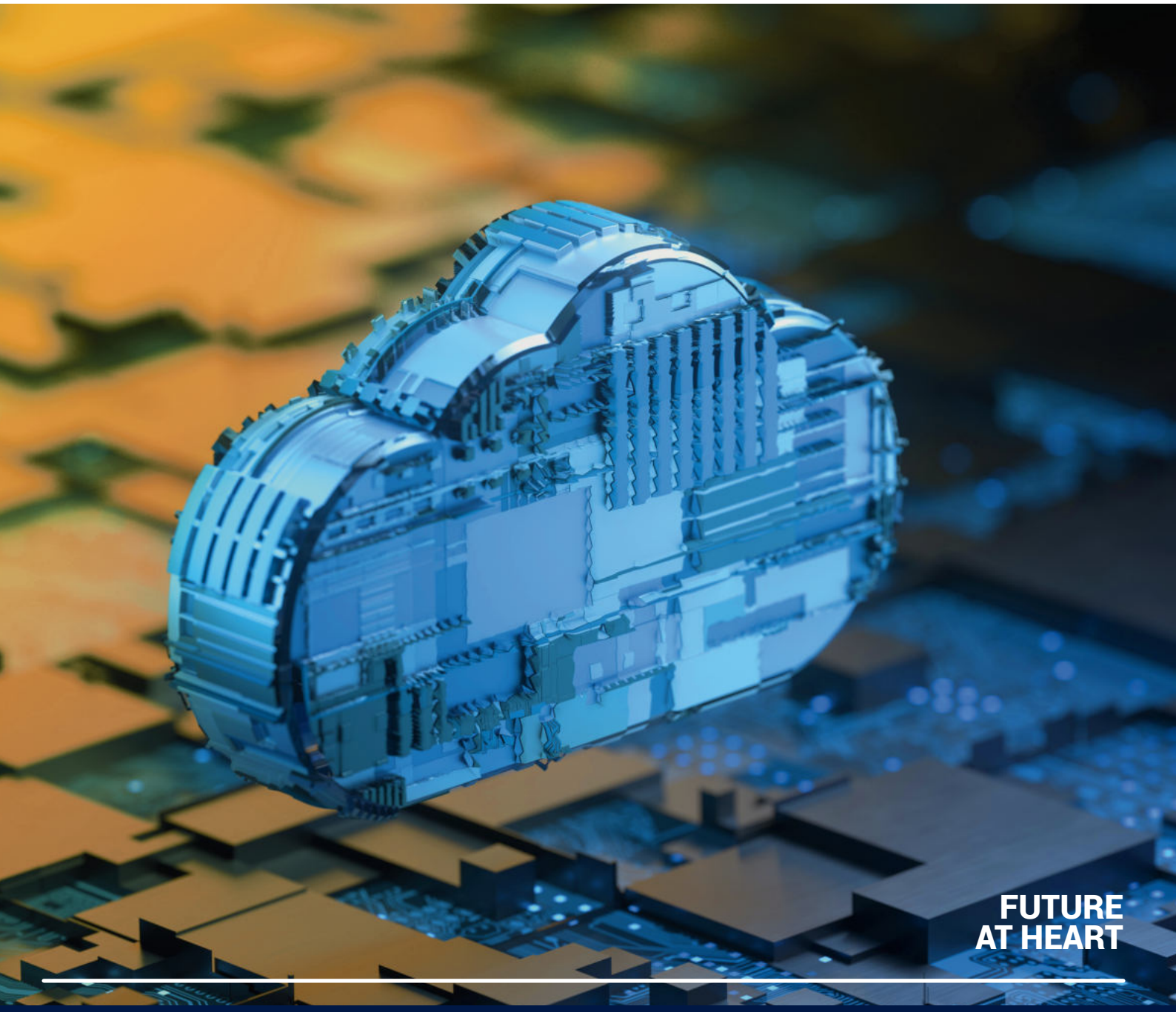
NTT DATA



WHITE PAPER

DYNAMIC CHANGE, UNCOMPROMISING SECURITY

CÓMO HACER DE LA NUBE UN ESPACIO SEGURO PARA LA INNOVACIÓN Y EL CRECIMIENTO

EL RETO NO ES PASARSE A LA NUBE, SINO CÓMO

Las empresas han empezado a darse cuenta de que las operaciones en la nube (cloud, en inglés) no son solo un objetivo deseable, sino esencial para seguir siendo rentables a largo plazo. No obstante, los servicios cloud tienen sus propias exigencias de ciberseguridad, que son nuevas y complejas. Las empresas, en general, tienen bastante trabajo por delante para estar a la altura de este reto. En este documento exploraremos algunas de esas singularidades de la ciberseguridad en la nube.

Es importante dejar claro que los problemas de seguridad no afectan a la lógica básica de la nube. Pero son problemas reales que deben analizarse y solucionarse para poder aprovechar al máximo los beneficios de la nube sin que la actividad empresarial se resienta.

Muchas de las grandes empresas internacionales están migrando lo más rápidamente posible al entorno cloud. Las razones para hacerlo son de sobra conocidas. Las exploramos en profundidad en otro white paper de NTT DATA: **The Evolving Enterprise:** ***How new generation Cloud drives change, growth and value.***

En síntesis, el espacio cloud tiene muchas ventajas:

- **Rápida escalabilidad.** La infraestructura pueda satisfacer la demanda en todo momento.
- **Reducción de costes.** En lugar de tener que realizar una inversión de capital, se paga solo por lo que se utiliza.
- **Agilidad.** Los entornos de tecnología de la información permiten adaptarse a los cambios más impredecibles y son mantenidos con las mejores prácticas por los socios externos.
- **Capacidad de innovación.** La nube reduce el nivel de riesgo de los proyectos y crea un ecosistema de trabajo más flexible que da acceso a las innovaciones de los socios externos.

LOS ENTORNOS DE TECNOLOGÍA DE LA INFORMACIÓN PERMITEN ADAPTARSE A LOS CAMBIOS MÁS IMPREDECIBLES.

Solo teniendo en cuenta la reducción de costes fijos que supone la migración -hay quien estima que puede ser de hasta un 31%- resulta evidente que las empresas que operan en un mercado competitivo (es decir, todas) deben dar el paso. Los sistemas de cloud computing son ya una herramienta cotidiana. Por tanto, lo único que hay que explicar es el cómo, es decir, los detalles de la preparación y del proceso de migración, y de qué manera se puede aprovechar al máximo el potencial de la nube.

UN SALTO GRANDE PERO MEJOR POR FASES

Puede parecer que dar el salto al entorno cloud supone un cambio enorme y, a menudo, así es. Implica migrar de un entorno tecnológico heredado a una ubicación virtual, alojada por uno o varios de los principales proveedores de hiperescala del mercado.

En este sentido, el cambio que supone es equiparable al de cualquier gran migración de una plataforma corporativa a otra. Es un proceso caro, disruptivo y que conlleva los riesgos propios de cualquier transformación a gran escala. Además, puede resultar frustrante, ya que las empresas no empiezan a obtener beneficios hasta terminar la migración.

Esto se debe a que la reducción de costes sólo es completamente efectiva cuando se dejan de utilizar los sistemas anteriores, y esto no puede ocurrir hasta que no se completa el cambio. Mientras tanto, los gastos son probablemente más altos de lo habitual, pues la empresa tiene que mantener la plataforma antigua a la vez que invierte en el nuevo modelo operativo, y también permitir la interoperabilidad entre ambos. Además, garantizar la seguridad de este entorno híbrido durante el periodo de transición también conlleva un gasto importante que no debemos subestimar.

LA REDUCCIÓN DE COSTES SÓLO ES COMPLETAMENTE EFECTIVA CUANDO SE DEJAN DE UTILIZAR LOS SISTEMAS ANTERIORES, Y ESTO NO PUEDE OCURRIR HASTA QUE NO SE COMPLETA EL CAMBIO.

Todo ello explica por qué las empresas tratan de migrar paso a paso, en vez de hacerlo de golpe. Así se reduce el riesgo y es más fácil empezar a rentabilizar el cambio, ya que se pueden identificar las ganancias rápidas desde el principio y usar los beneficios obtenidos para financiar el resto de cambios.

En NTT DATA estamos de acuerdo con este enfoque. En nuestro libro electrónico ***Guide to a successful, collaborative journey to Cloud*** analizamos en profundidad qué pueden hacer las empresas para prepararse para esta estrategia por etapas.

Sin embargo, hay una cuestión importante que surge siempre cuando se trata de transformaciones radicales de este tipo. Una cuestión que debemos analizar en profundidad y gestionar con mucho cuidado. Es la ciberseguridad.

GESTIÓN DE LA COMPLEJIDAD PARA FRENAR A LOS CIBERDELINCUENTES

Muchas grandes empresas adoptan distintos métodos para migrar a la nube. Su objetivo es obtener ganancias rápidas identificando acciones prácticas que, aparentemente, conlleven poco riesgo y que permitan recuperar pronto la inversión.

Dada la complejidad de estas acciones (puede que haya muchas en toda la empresa), se suelen incluir en un único programa estratégico. No se trata de una modelo tradicional de migración integral, sino de un programa menos agresivo de supervisión y monitorización.

Estamos convencidos de que la supervisión estratégica funciona, pero la mayoría de los programas de transición al cloud computing que conocemos corren el riesgo de crear inconsistencias entre los distintos elementos del proceso. Ahí es donde se producen fallos de seguridad que pueden ser aprovechados por los ciberdelincuentes o que generan problemas causados por errores humanos.

Tres enfoques, múltiples soluciones.

La mayoría de las empresas siguen uno o varios de estos tres enfoques:

SaaS

Software como servicio (SaaS, por sus siglas en inglés). Las grandes empresas utilizan soluciones comerciales de software estandarizado (COTS) y paquetes de soluciones para acceder cuanto antes a las ventajas de los servicios cloud. Creemos que este puede ser un modo extremadamente racional y eficiente de lograr precios competitivos, de ofrecer servicios intuitivos al usuario final y de emplear la nube como una fuente de ventaja competitiva.

Este enfoque adopta distintas formas:

- Los sistemas ERP, CRM y otras soluciones de gestión a gran escala ofrecen servicios de cloud computing desde hace casi una década. Por tanto, no es necesario invertir en migrar a las últimas versiones de SAP, Oracle, Salesforce u otras soluciones equivalentes. En vez de eso, las empresas tienen acceso a una plataforma en constante evolución que mejora sus funcionalidades continuamente. SAP y otras grandes compañías de software compiten ahora por convertirse en socios estratégicos clave. Esta evolución es significativa y hay que tenerla en cuenta cuando se planifica el cambio.

- Las plataformas de software sectoriales y personalizables son una parte crucial de las estrategias de la nube. En NTT DATA hemos desarrollado nuestra propia oferta de soluciones verticales y horizontales, diseñadas para que empresas de gran tamaño de todos los sectores puedan acelerar el tiempo de comercialización y la obtención de beneficios. Los sistemas nativos (como Platea, nuestra principal plataforma de banca) permiten que las empresas empiecen a conseguir beneficios mucho antes de lo que lo harían con un proceso convencional de migración.

- Algunas compañías están aprovechando ciertos aspectos de los SaaS de consumo para desarrollar portales de servicios para los clientes. Otras utilizan prácticas y modelos que normalmente se aplican a los consumidores para implementar métodos de autoservicio en su entorno corporativo. Estos métodos suelen ser fiables y estables, pero a menudo incumplen las medidas de seguridad más exigentes de las operaciones corporativas.

MIGRACIÓN DE APLICACIONES

Si queremos que la migración sea un éxito y se desarrolle con rapidez, la máxima prioridad es transferir toda la cartera de aplicaciones de la empresa y convertirlas en recursos nativos del espacio cloud.

Para ello, las empresas deben:

- Estudiar su cartera actual y decidir qué aplicaciones se pueden eliminar y cuáles pueden pasar de un modelo con licencia a otro de SaaS.
- Determinar cómo reutilizar y adaptar las existentes, siempre que sea posible, y cuáles se deben reemplazar.
- Optimizar la cartera completa, un ejercicio esencial para lograr una mayor eficiencia operativa.

El objetivo principal en este caso es crear un entorno que optimice las operaciones empresariales y ofrezca una ventaja competitiva a largo plazo. Para lograrlo, es necesario migrar, rediseñar, remplazar y eliminar distintas aplicaciones, lo cual ya supone un cambio enorme de por sí.

Inevitablemente, en el proceso de migración y optimización habrá que mover las aplicaciones a una serie de contenedores (gestionados por tecnologías como Dockers o Kubernetes) diseñados para trabajar de forma simultánea en distintos clústeres. Los problemas que pueden surgir si se abusa de los contenedores son evidentes.

MODELO DEVOPS.

Una de las potenciales ventajas de convertirse en una empresa verdaderamente nativa de la nube es que genera un ecosistema de trabajo más ágil y abierto que permite acceder a las innovaciones rápidamente.
Esto proporciona ventajas clave: una rápida reconfiguración de los equipos de desarrollo, la capacidad de desarrollar en plataformas cercanas a la producción y la agilidad para hacer ensayos y para gestionar opciones de escenarios o gemelos digitales. Todo esto garantiza resultados más estables, avanzados e innovadores.

Una posible desventaja que hay que asumir con este enfoque es una cierta descentralización del control, lo cual es normal en entornos empresariales de este tamaño. Las empresas buscan atajar este problema pasando de un modelo de DevOps (la combinación de operaciones y desarrollo en el mismo proceso) a otro de DevSecOps, donde la seguridad es una responsabilidad fundamental de todos los miembros del equipo.

La seguridad es un componente crucial de este nuevo enfoque. Hay que gestionarla con especial atención y seguir haciendo pruebas para asegurarnos de que la colaboración entre las distintas áreas corporativas no conduce a cierta ambigüedad en las responsabilidades y las competencias de cada miembro del equipo.

» LAS PRINCIPALES AMENAZAS

Algunas de las potenciales amenazas que derivan de la migración son evidentes. Otras, no tanto. A continuación, enumeramos brevemente las áreas donde las grandes empresas tienen que identificar y gestionar problemas durante el proceso.

Resumen

Migrar a un entorno cloud paso a paso tiene mucho sentido. No lo discutimos ni nos oponemos a ello, pero es importante que todo el mundo entienda la complejidad extra que este método añade a la planificación y la ejecución estratégicas. Cada paso que se da afecta a la seguridad, y hay que saber identificar sus consecuencias y ocuparse de ellas de manera tajante y efectiva.

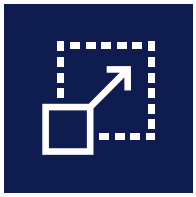
Uso de datos. Este es uno de los riesgos más conocidos de la migración a la nube, ya que los gobiernos y sus órganos reguladores han puesto especial énfasis en él. Los requisitos de soberanía del ciudadano sobre sus datos, combinados con la normativa del Reglamento General de Protección de Datos y otras regulaciones, obligan a las empresas a determinar con exactitud la ubicación de sus datos y a gestionar cuidadosamente su almacenamiento, acceso y utilización.

No obstante, continúa siendo un tema complejo que ha facilitado la aparición de nuevas tecnologías (como el compartimento de los datos) cuyo objetivo es, precisamente, ofrecer una gestión más eficaz. La pérdida de datos debida a errores humanos es un problema que ha afectado y sigue afectando a la mayoría de las empresas.

Gestión de identidades. Las empresas deben ser conscientes de lo importante que es definir claramente el acceso a los datos según el rol, la responsabilidad y los privilegios de sus profesionales. Por ello, se han reforzado los procesos de incorporaciones y bajas, y los niveles de autenticación son también más restrictivos que en el pasado.

Sin embargo, a medida que nos acostumbramos a trabajar en el nuevo entorno cloud, hemos de asumir que también aumenta la complejidad de los sistemas de gestión de identidades y accesos (IAM, por sus siglas en inglés) y que es necesario recurrir a soluciones nativas. La seguridad de las credenciales personales y corporativas es una cuestión que preocupa enormemente a las empresas actuales, ya que los fallos en esta área son la vía de penetración más sencilla para los cibercriminales.

Según nuestra experiencia, muchas empresas no alcanzan a comprender por qué los sistemas IAM en el entorno cloud no pueden ser iguales que los de sus soluciones locales. Queda mucho trabajo por hacer en este campo, tanto a nivel de educación como de ingeniería.



Interfaces. Progresivamente, va quedando atrás la concepción de la nube como centro de datos virtual y se empieza a usar como una red programable e inteligente. La convergencia de tecnologías —como la conectividad de baja latencia que permite el 5G, las plataformas de trabajo colaborativo y las interfaces de última generación, como la realidad extendida— sigue impulsando la revolución de los servicios de cloud computing.

Esto también pone de manifiesto el papel de las API abiertas en el desarrollo de interfaces escalables, multidimensionales y flexibles, que son esenciales para el funcionamiento de plataformas personalizables y entornos corporativos compartidos. Las API ofrecen a los distintos grupos de interés servicios configurables mediante un portal común. Por ello, se han convertido en un área potencialmente vulnerable en este complejo entorno de servicios.

Los ciberdelincuentes son cada vez más sofisticados y, una vez que acceden al código principal de la API de una empresa, pueden encontrar fácilmente los datos de sus servicios y clientes.

Interconexión e intercambio de información. Este apartado aborda dos problemas diferentes, aunque relacionados:

- El uso de tecnología compartida ahorra costes y proporciona mayor estabilidad y velocidad de desarrollo. Sin embargo, un pequeño error que quizás no sea importante para una empresa concreta puede acabar provocando problemas similares en todas las que utilizan el mismo software.

- La colaboración entre empresas es un modelo ágil cada vez más frecuente que ofrece acceso a la innovación, mayor eficiencia operativa y otros beneficios. Pero al mismo tiempo obliga a un mayor control de los sistemas IAM y de las credenciales de los usuarios, así como a una disciplina superior en la gestión de los entornos compartidos, para garantizar que la colaboración, con todas sus ventajas de agilidad y fluidez, no acarree fallos de seguridad.

Ataques maliciosos. Todos tenemos asumido que este tipo de incidentes son una realidad. Aun así, cabe preguntarse por qué empresas de las que todos dependemos, como las compañías eléctricas o las de servicios sanitarios, sufren tantos ataques por parte de bandas criminales y agentes estatales. Lo cierto es que estas amenazas no van a desaparecer por tres razones principales:

- El crimen online, que utiliza criptomonedas procedentes de refugios relativamente seguros, suele ofrecer un retorno rápido de la inversión. A los delincuentes les merece la pena invertir en herramientas sofisticadas, ya que son el mejor recurso que tienen para sacar beneficio.
- Países con intenciones hostiles atacan infraestructuras esenciales de otros estados para poner a prueba sus sistemas de defensa y perjudicarlos sin necesidad de emprender acciones militares.
- Clientes y colaboradores insatisfechos pueden dañar fácilmente a las empresas que les desagradan sin correr demasiados riesgos.

Mientras estos tres factores continúen existiendo, seguirá habiendo ataques que desafíen las infraestructuras de seguridad.

Transformación organizacional. Es un proceso complejo y a gran escala en el que la ciberseguridad juega un papel fundamental. Todas las actividades importantes conllevan riesgos a nivel de seguridad, de modo que es necesario identificar, cuantificar y mitigar dichos riesgos durante el periodo de transformación.

Es cierto que se puede migrar desde una infraestructura tecnológica local a la nube, entendida como centro virtual de datos, sin alterar el funcionamiento de la empresa ni su estructura organizativa. Pero para explotar al máximo el potencial de la última generación de servicios (la nube en red) es necesario rediseñar en profundidad los procesos, la cultura, la mentalidad de los empleados y las operaciones de la organización.

Estos cambios pueden provocar riesgos relacionados con la seguridad. Es necesario por tanto que el proceso de transformación incorpore una evaluación y una actualización rigurosas de los procedimientos y capacidades de seguridad.

» ENTORNOS HÍBRIDOS, RIESGO CRECIENTE

El paso a soluciones que operan exclusivamente en el entorno cloud obliga a las organizaciones a trabajar con tecnología y sistemas operativos híbridos muy complejos.
Eso supone trabajar con múltiples proveedores de servicios cloud, en un ecosistema donde la complejidad aumenta al mismo ritmo que evoluciona la empresa. La entrada en nuevos mercados, por ejemplo, puede exigir la contratación de proveedores digitales de otro país y la conexión con dispositivos de periferia o sensores y tecnología del Internet de las cosas que tengan una ubicación local.

Summary

En resumen, la mayoría de los problemas de seguridad de la transición a la tecnología cloud son bien conocidos (algunos de ellos están en el centro del debate público y sujetos a la acción de los gobiernos), pero muchas de las grandes empresas que están ahora migrando a la nube no disponen todavía de estrategias específicas ni de los recursos que se necesitan para abordar las amenazas de forma integral y eficaz.
Este problema afecta especialmente a las organizaciones que se enfrentan a escenarios de gran complejidad en las distintas etapas del proceso de transición desde un entorno exclusivamente local a otro nativo.

De esta forma, ciertos servicios y procesos han de ser operados por centros de datos, redes y proveedores en la nube con capacidad para adaptarse, escalar y crecer al mismo ritmo que las organizaciones.

Al mismo tiempo, también es necesario contar con nuevas ubicaciones de centros operativos y alojamiento de datos que permitan satisfacer las demandas de los nuevos mercados y cumplir con su normativa legal y la de los organismos reguladores internacionales. La dinámica cloud exige priorizar la agilidad, la rentabilidad y los plazos de comercialización. Por ello, los sistemas de la periferia del entorno corporativo deben ser flexibles y fluidos y ser capaces de a adaptarse a la complejidad y gestionarla.

¿Cómo afectan estas circunstancias a la gestión de la seguridad? El siguiente gráfico da una idea, a un nivel muy general, de las exigencias de seguridad de los sistemas híbridos de nube en red.

La arquitectura que proponemos se apoya en cuatro plataformas operativas interconectadas y especializadas con capacidades y recursos que pueden estar alojados por distintos proveedores de servicios de cloud computing y en muchas ubicaciones diferentes. Lo más importante es conseguir interoperabilidad completa que permita alcanzar la eficiencia y velocidad de los entornos nativos. Los cuatro tipos de plataformas son:

01 Fundamentos. Ofrece recursos para la definición y el funcionamiento del entorno básico operativo y sus servicios, es decir, la topología de red, la arquitectura de almacenamiento y los sistemas básicos de administración.

02 Catálogo. Sirve para localizar, etiquetar, gestionar y ofrecer recursos individuales a los usuarios según reglas creadas por la empresa, y que debe priorizar un sistema de autoservicio seguro.

03 Modelos. Plataforma de recursos de programación que ofrece bloques estándar para acelerar el desarrollo y el lanzamiento de servicios, también de acuerdo con las reglas de negocio establecidas.

04 Capacidades digitales. En la capa superior de la interfaz, da acceso a recursos básicos de desarrollo y acelera el lanzamiento de nuevos servicios. Incluye experiencias unificadas, entornos de trabajo colaborativos, modelos DevOps y otras capacidades clave para los usuarios.

Lo normal es que se trate de plataformas desagregadas que se encuentran en distintas ubicaciones geográficas, pero esta dispersión no resulta un problema, siempre y cuando se hayan establecido capacidades básicas de gestión y seguridad. A partir de aquí, los desafíos crecen. Nuestra arquitectura de referencia está dividida en tres áreas verticales de gestión que se aplican a los cuatro tipos de plataforma.

Observación. Proporciona mecanismos integrales de control de todos los procesos, capacidades y recursos que pertenecen a la arquitectura básica, así como de los que se comunican con la misma. Se establecen sistemas de análisis e informes de todos los parámetros y eventos operativos, así como un sistema de alertas y alarmas.

Fiabilidad. Esta área incluye todos los sistemas y procesos relacionados con los planes de continuidad de negocio y de recuperación de desastres (BCDR, por sus siglas en inglés), desde las copias de seguridad y la supervisión en lote hasta la gestión de clústeres. Prevé ubicaciones físicas para los planes de continuidad BCDR, redes y comunicaciones redundantes, protocolos de escalamiento rápido y gestión de incidencias graves.

Seguridad. Las dos áreas anteriores forman parte de una estrategia de seguridad integrada, por lo que esta área está dedicada a la gobernanza y los factores de gestión básicos necesarios para mantener la seguridad de todo el entorno. Incluye la administración de identidades y acceso, las estrategias para gestionar todo el ciclo de vida de la seguridad y los procedimientos clave para la gobernanza integral del ecosistema en toda su complejidad.

Resumen. La transición a la nube está acompañada de un grado de complejidad inevitable y diríamos que hasta necesario. Los sistemas de cloud computing ofrecen libertad para evolucionar, cambiar de rumbo rápidamente y escalar en función del crecimiento de la demanda. Las estructuras no pueden ser rígidas y necesitamos aceptar y trabajar con un cierto nivel de imprevisibilidad.

Por supuesto, todo esto significa que nuestros principios de gestión y seguridad subyacentes deben ser extremadamente firmes, precisamente porque no podemos contar con estructuras, métodos de trabajo y hábitos operativos inamovibles que nos hagan el trabajo. Los procedimientos de seguridad deben tener un funcionamiento dinámico y flexible, pero, al mismo tiempo, ofrecer garantías absolutas de solidez. Esa es la clave para diseñar un sistema efectivo de seguridad.

ADIÓS A LO DE TODA LA VIDA: CÓMO CONSTRUIR UNA ESTRATEGIA DE CIBERSEGURIDAD

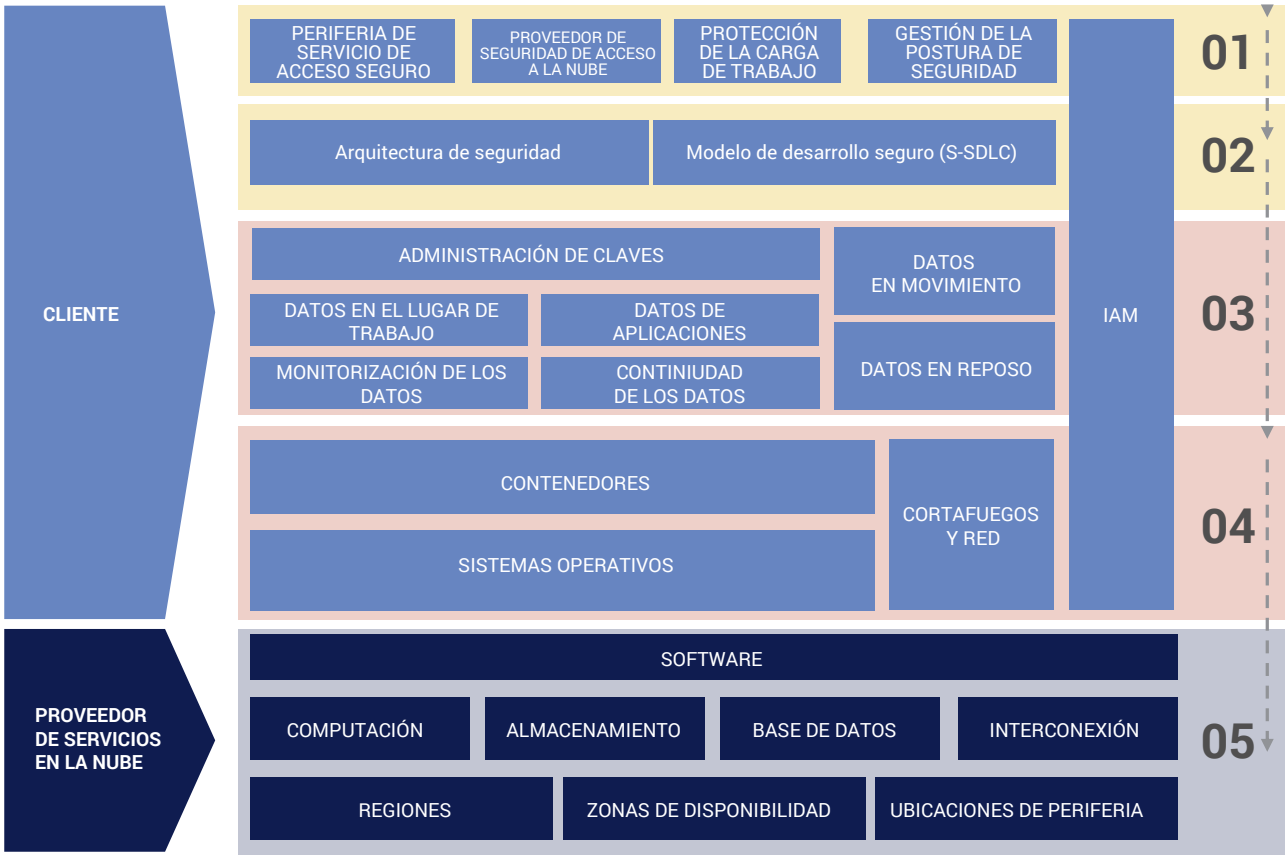
Las ideas y estrategias de seguridad han dejado de ser relevantes y eficaces en la nube, especialmente cuando hablamos de la última generación (nube en la red). En los entornos físicos clásicos tenía sentido buscar formas de seguridad integral y plantearse levantar una fortaleza de murallas gruesas y elevadas para impedir los ataques.

Ahora ese enfoque ya no funciona. Por definición, todos estamos dentro de la fortaleza (el entorno cloud), y eso incluye a nuestros enemigos potenciales, a los que no podemos impedir la entrada. Ya no basta con proteger la ubicación donde están alojados los activos. Es necesario proteger todos los activos individuales, estén donde estén, así como las conexiones circunstanciales entre ellos, los puntos de entrada de los colaboradores en el ecosistema, que son cada vez más numerosos, y los componentes estándar que se adaptan para construir soluciones personalizadas, sin importar ni el quién ni el dónde ni el cuándo.

Se trata de un concepto mucho más flexible, que refleja los cambios continuos de alcance y escala que se producen de forma rutinaria en todo momento. El espacio de nuestras operaciones empresariales cambia constantemente en función de los clientes, los niveles de interacción en nuestros ecosistemas y el equilibrio entre las acciones que se gestionan a nivel local y las que exigen conectividad entre distintas ubicaciones y departamentos operativos.

El siguiente gráfico muestra el diseño y la estructura de este nuevo enfoque.

MAPA DE SEGURIDAD EN LA NUBE



01 **Protección de acceso a la nube y administración de identidades**

02 **Protección de software**

03 **Protección de datos**

04 **Software IaaS y PaaS**

05 **Infraestructura global**

CLOUD SECURITY MAP

Reference Model

En esta estructura operativa, nos basamos en las cuatro plataformas de nuestra arquitectura digital e implementamos medidas de seguridad en todas sus secciones.

- **Fundamentos.** Empleamos la infraestructura como servicio (en inglés, IaaS) y la plataforma como servicio (en inglés, PaaS), e implementamos soluciones específicas de políticas, integridad de redes y cortafuegos, sistemas operativos y contenedores.
- **Catálogo y modelos.** Nos centramos en todo lo relacionado con los datos. Es decir, datos en movimiento y en reposo, monitorización, continuidad e intercambio de información en el lugar de trabajo. Todo ello protegido mediante un riguroso sistema de gestión de claves.
- **Capacidades digitales.** Protegemos el software en la fase de desarrollo mediante un proceso eficaz de SecDevOps, con una sólida arquitectura de seguridad para la identificación y gestión de amenazas, respaldada por medidas continuas de revisión y protección de los componentes.

Estas políticas, soluciones, procesos y metodologías se aplican en todas las partes del entorno corporativo y en el ecosistema nativo de la nube, y su ubicación y su tecnología son totalmente agnósticas, es decir, que son compatibles con cualquier sistema. Las prioridades operativas y generadas por la demanda obligan a que las fronteras del espacio cloud se adapten y evolucionen, y el modelo de seguridad debe poder ampliarse o reducirse en función de las necesidades de la empresa.

Los tres componentes clave de la gestión de la seguridad, que permiten operar eficiente y continuamente en el entorno virtual, son los siguientes:

- Un sistema de **gobernanza** eficaz y uniforme. Se aplica a todos los recursos, puntos de datos, procesos y ubicaciones que tienen cualquier tipo de conexión con la nube corporativa.
- Una administración rigurosa de **identidades y accesos**. Se usa en todos los puntos de contacto, locales, remotos y en la periferia del espacio cloud, mediante túneles seguros y otras conexiones, y con los estándares de acceso más exigentes.
- Metodologías y prácticas de **todo el ciclo de vida de la seguridad**. Se actualizan continuamente para adoptar las mejores prácticas de prevención, detección, respuesta y capacidades de continuidad.

Se trata de un enfoque mucho más complejo que el tradicional, lo que obliga a plantearse seriamente la seguridad en la nube antes de empezar a ejecutar estrategias.

AUTOMATIZACIÓN PARA ANTICIPARSE A LOS ATAQUES

Las empresas que operan en el entorno cloud, sea cual sea su tamaño, se ven obligadas a desarrollar, implementar y gestionar entornos híbridos donde hay elementos que pueden controlar directamente y otros que no. Las empresas de menor tamaño y las organizaciones nativas son las que lo tienen más fácil para operar en un entorno exclusivamente virtual. En cambio, las de mayor tamaño siguen manteniendo ciertos sistemas en ubicaciones físicas y dependen de un número creciente de dispositivos de periferia y de Internet de las cosas repartidos en distintas localizaciones.

En ambos casos, es necesario un cierto nivel de automatización de la seguridad para conseguir el grado de uniformidad deseado en todo el entorno operativo, independientemente de su complejidad. Ya existen soluciones eficaces que permiten automatizar la gestión y la vigilancia de la seguridad en entornos de gran complejidad. No obstante, como todo lo que tiene que ver con la ciberseguridad, cualquier solución está inmersa en una batalla continua para anticiparse a las amenazas y adaptarse a la creciente complejidad.

LAS SOLUCIONES CLAVE SON:

Infraestructura como código (en inglés, IAC). Permite programar y adoptar automáticamente las políticas de seguridad en todas las actividades y obligan a su cumplimiento. Es decir, no es posible llevar a cabo las tareas sin aplicar las políticas de seguridad definidas para las mismas.

Este es el enfoque perfecto para las empresas con una estrategia nativa y que alojan todos sus activos en la nube. Ofrece visibilidad, control centralizado y aplicación automática, incluso para las empresas que solo tienen un mínimo de funciones de tecnología de la información.

Gestión de la posición de seguridad en la nube (en inglés, CSPM). Este enfoque es especialmente adecuado para las empresas que ofrecen servicios en múltiples países y cuyas entradas y colaboradores cambian regularmente (por ejemplo, en el caso del sector de los bienes de consumo).

La gestión de la posición de seguridad requiere un conjunto de políticas y procedimientos que es idéntico para todas las actividades y conexiones, y que automatiza la identificación y corrección de riesgos en cualquier parte del sistema cloud que esté en contacto con la organización. Esta solución ofrece un único punto de visibilidad para múltiples entornos y proveedores de la nube, unifica las alertas y optimiza la eficiencia de los centros de operaciones de seguridad.

Plataformas de protección del trabajo. Este tipo de herramientas protege la seguridad de tareas específicas que se desarrollan en múltiples entornos cloud. Se trata de un concepto que ha sido desarrollado para adaptarse a las nuevas circunstancias de trabajo, en las que las tareas quedan divididas en contenedores o kubernetes en muchas plataformas distintas.

Esta distribución hace que con los sistemas de gestión tradicionales sea muy difícil tener una idea clara de dónde se encuentran los distintos recursos y activos de contenido o desarrollo de software en cada momento. También complica la identificación de amenazas y problemas que pueden poner a la empresa en peligro a consecuencia de errores en cualquiera de los múltiples puntos donde está presente.

Resumen. Se están desarrollando herramientas que permiten automatizar, integrar y mejorar los procesos de seguridad en los entornos que ofrecen los distintos proveedores de la nube y que están conectados entre distintas ubicaciones y organizaciones. Puesto que las oportunidades y las amenazas no hacen más que aumentar, esperamos que el desarrollo de estas soluciones se acelere próximamente.

LA VISIÓN DE NTT DATA: COMPROMETIDOS CON UNA MENTALIDAD DISTINTA

La seguridad de los servicios cloud de última generación plantea problemas muy diferentes a la de los ámbitos físicos (aunque ésta no está exenta de complicaciones). Es urgente por ello tomar medidas para desarrollar una mentalidad distinta que vaya acompañada de nuevos procedimientos, métodos, sistemas y áreas organizativas que permitan a las empresas aprovechar al máximo las ventajas de los sistemas de cloud computing, sin dejar de gestionar y minimizar los riesgos.

En NTT DATA estamos alineados y comprometidos con el desarrollo de la nube en red de última generación. Contamos con una larga experiencia en telecomunicaciones y somos líderes en conectividad de baja latencia de 5G, lo que nos permite entender el concepto cloud como algo que va mucho más allá de la idea de centro virtual de datos que se le atribuyó en su origen.

Muy pronto, las fronteras entre la nube y la red desaparecerán y la división entre ambos conceptos dejará de tener sentido. La nube se convertirá en un conjunto de redes programables inteligentes con activos enteramente desagregados y ubicaciones completamente repartidas. Se pasará a un entorno altamente dinámico, con conexiones que se negocian, crean y destruyen a cada instante entre millones de activos de forma impredecible.

En este entorno de geometría variable y adaptable, es imprescindible garantizar en todo momento la seguridad de los datos, los protocolos de Internet, los procesos y los demás activos. Los sistemas de seguridad tradicionales que resultan eficaces en las infraestructuras físicas pierden su utilidad en este nuevo entorno. Es imposible aprovechar al máximo el potencial ilimitado de la nube sin contar con soluciones eficaces de gestión de la seguridad.

En NTT DATA somos líderes en arquitectura de la nube en red y tenemos un conocimiento profundo de este entorno. Aplicamos las mejores prácticas de pensamiento y gestión para hacer de la transición un proceso seguro y rentable para todas las empresas.