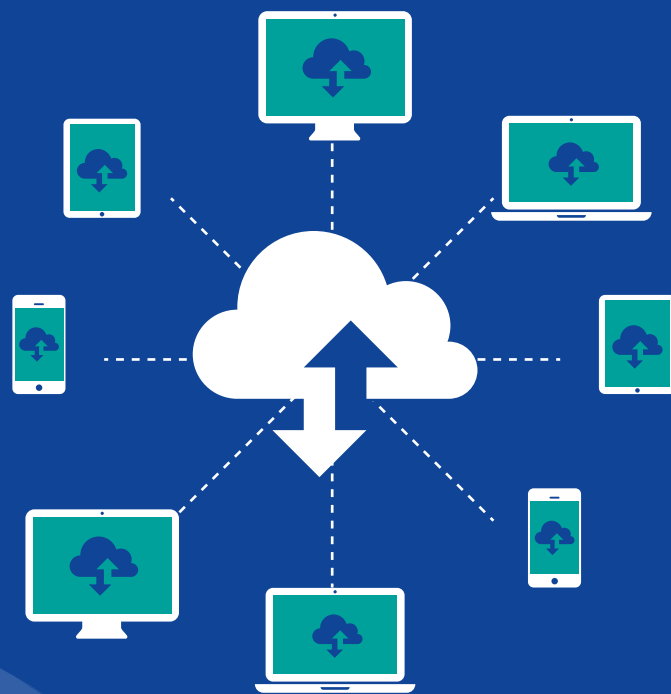


Cloud Computing 1 paso más cerca de ser una Utility digital



Cloud Computing se ha posicionado como una tecnología clave para el uso racional de la infraestructura tecnológica y la reducción de costos de IT. En su evolución hacia los negocios digitales, las Utilities deben conocer por qué es importante esta tecnología y las principales precauciones a tener en cuenta en su proceso de adopción.

Introducción

Hoy en día, los avances tecnológicos incrementan exponencialmente la cantidad de información que las empresas de energía, gas y acueducto reciben y generan, haciendo más costoso el almacenamiento y el procesamiento de los datos al tener que ampliar la infraestructura tecnológica para suplir la demanda de este tipo de recursos.

Por esta razón, estas empresas encuentran en *Cloud Computing* un aliado que les brinda la capacidad de operar en una plataforma tecnológica que satisface sus necesidades de flexibilidad, accesibilidad y disponibilidad. De hecho, en los últimos años, las aplicaciones empresariales basadas en Cloud han sido aceptadas significativamente en la industria de servicios públicos. Por otra parte, el traslado de los datos y los servicios, de los *data centers* propios a la red mundial de servidores, está mejorando el rendimiento y los costos del área de IT.

No obstante, la sensación de falta de control sobre los datos, los servicios y las aplicaciones representa el mayor temor en el proceso de migración a Cloud, no sólo por la seguridad de la información, sino también, por la constante actualización de las aplicaciones en la nube que pueden afectar los procesos críticos de una empresa de energía, gas y acueducto. Para vencer este temor y cambiar el paradigma del *data center* tradicional, las *Utilities* deben conocer en qué consiste Cloud, sus modelos de despliegue y servicio, así como los beneficios que les brinda en la operación del negocio.

"El **58%** de todas las organizaciones encuestadas están adoptando Cloud, utilizando nubes públicas o privadas para más de una o dos pequeñas aplicaciones o cargas de trabajo, con respecto al **24%** de hace **14 meses**."¹



¿Qué es Cloud Computing?

Cloud Computing es un estilo de computación en el que se proveen capacidades relacionadas con las tecnologías de información (IT) de manera escalable y flexible. A través de Internet, facilita el acceso a un amplio conjunto de recursos físicos, aplicaciones y servicios compartidos, que pueden ser utilizados bajo demanda y gestionados con un mínimo esfuerzo.

Apoyándose en el modelo de Cloud Computing, las organizaciones dejan a un lado la preocupación de poseer capacidad suficiente para almacenar y procesar datos en los *data centers* propios. Además, reducen los costos de IT al pagar únicamente por los recursos utilizados, en lugar de mantener una infraestructura costosa y subutilizada durante los periodos de poca actividad.



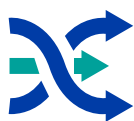
"Para **2020**, una política corporativa "**no-cloud**" será tan extraña como la política de "**no-internet**" hoy en día."²

En efecto, Cloud Computing es un aliado estratégico para la administración de su negocio dado que libera a su personal de tareas repetitivas que no le dejan espacio suficiente para enfocarse en la creación continua de valor para el negocio. También, facilita que las empresas accedan a servicios de aplicaciones empresariales listas para operar, sin requerir de largos proyectos de implantación ni inversiones en servidores de almacenamiento y procesamiento, actualizaciones de software, mantenimiento del hardware e instalaciones, entre otros.

Por medio del uso de aplicaciones en la nube, los funcionarios pueden acceder a la información del negocio desde cualquier computadora o dispositivo con acceso a Internet, garantizando la disponibilidad de la información en todo momento.

1. IDC, IDC's Latest CloudView Multiclient Study Reveals Attitudes and Strategies of the 58% of Organizations Embracing Cloud, Press release, February 2016.

2. Gartner, Gartner Says By 2020, a Corporate "No-Cloud" Policy Will Be as Rare as a "No-Internet" Policy Is Today, Press release, June 2016.



Flexibilidad

Escale rápidamente para satisfacer la demanda de computación.



Reducción de costos

Pague solo por lo que usa y minimice los costos de hardware e IT.



Accesibilidad

Acceda desde cualquier dispositivo y lugar con conexión a internet.



Disponibilidad

Obtenga acceso 24/7 al sistema en la nube desde cualquier lugar y dispositivo.



Simplicidad

Libere al área de IT de la gestión de servidores y la actualización de software.

Figura 1. Beneficios de Cloud Computing



¿Cuáles son los modelos de despliegue en la nube?

Los modelos de despliegue describen la relación entre el proveedor Cloud y los clientes. En cada uno de ellos, se especifica el grado de exclusividad en el acceso al servicio y el responsable de operar la nube contratada. En general, Cloud puede adoptar una de cuatro formas (Nube pública, privada, híbrida o comunitaria) o alguna combinación de ellas, según las necesidades de cada empresa.

Nube pública

Las nubes públicas son propiedad de terceros, quienes se encargan de suministrar servicios a los clientes en una red abierta para el uso público. A menudo, son utilizadas por múltiples usuarios, por lo que el proveedor ejecuta el servicio en un entorno compartido. En este tipo de nube se ofrece escalabilidad casi ilimitadamente dado que el pago se realiza con base en los recursos consumidos y el tiempo de uso.

Las ventajas que ofrece este tipo de nube son principalmente la eficiencia y la disponibilidad. Sin embargo, la principal preocupación de las empresas cliente se centra en la seguridad de sus datos dado que estos son almacenados en servidores que se encuentran fuera (*off-premises*) de sus instalaciones.

Nube privada

Las nubes privadas ofrecen infraestructura para el uso privado de una sola empresa y los servicios se mantienen en una red protegida por un *firewall*³. Se puede construir una nube privada dentro del data center propio de la Utility y acceder a los servicios ofrecidos por un proveedor o una combinación de los anteriores.

Una de las mayores ventajas que ofrece una nube privada es la seguridad y el control de los datos, dado que los recursos físicos no son compartidos.

Nube comunitaria

Las nubes comunitarias son un entorno de servicios dirigido a un conjunto limitado de organizaciones. Se provee exclusivamente para los miembros de una comunidad, quienes comparten requisitos similares de seguridad, rendimiento y cumplimiento.

Este tipo de nube puede ser administrada y operada por una o más de las organizaciones de la comunidad, un tercero o alguna combinación de ellos, y puede existir dentro (*on-premises*) o fuera (*off-premises*) de las instalaciones de la empresa.

Nube híbrida

Las nubes híbridas se componen de dos o más nubes de tipo privada, pública o comunitaria, logrando combinar los beneficios de costos, escalabilidad, control y seguridad. Lo anterior, dado que es posible disponer de servicios de Cloud en diferentes tipos de nube como si se tratase

3. Un firewall es una aplicación o un equipo que controla el acceso a la red y el flujo de tráfico de la misma. Gartner.

de una sola, mediante el uso de tecnología propietaria o estandarizada.

Más del 70% de los usuarios de Cloud están pensando en términos de una estrategia cloud "híbrida".⁴



¿Cuáles son los modelos de servicio del Cloud Computing?

Estos modelos son utilizados por un tercero para proporcionar servicios que normalmente son soportados por las áreas de IT de las empresas y que pueden corresponder a uno o varios modelos:



Infraestructura como servicio (IaaS)

Es un servicio estandarizado por medio del cual las empresas adquieren recursos informáticos a demanda, por ejemplo: servidores, redes y almacenamiento, bajo un modelo de pago por uso con base en la cantidad o duración de los recursos consumidos, el volumen de los datos almacenados, el número de direcciones IP usadas durante un intervalo de tiempo, entre otros.

En un servicio IaaS, el cliente no gestiona ni tiene control sobre la infraestructura contratada; por el contrario, los proveedores son los encargados de gestionar el mantenimiento de los recursos y las copias de seguridad. Dado que el cliente no tiene acceso al hardware, los proveedores ofrecen una interfaz gráfica basada en web, a través de la cual los clientes pueden auto-provisionarse.

Algunos ejemplos de proveedores de IaaS son: *Amazon Web Services* y *Microsoft Azure*.



Plataforma como servicio (PaaS)

Se trata de una capa entre Infraestructura como Servicio (IaaS) y Software como Servicio (SaaS) que proporciona una plataforma y un conjunto de herramientas que facilitan a los desarrolladores la construcción y el despliegue de aplicaciones en la nube.

En este modelo, los usuarios pueden acceder desde un navegador a este servicio, sin necesidad de comprar y mantener el hardware y software subyacente. Además, pueden escoger las características que desean con base en una suscripción. Al igual que en el modelo IaaS, el cliente no gestiona ni tiene control sobre la infraestructura contratada, pero en este caso tampoco lo tiene sobre los sistemas en los cuales el desarrollador desplegará su aplicación.

Esta categoría incluye servicios como: Plataforma de aplicaciones, integración, gestión de procesos de negocio y servicios de bases de datos.

Algunos ejemplos de proveedores de PaaS son: *Microsoft Azure* y *Google's App Engine*.



Software como servicio (SaaS)

Hace referencia a aplicaciones disponibles en la web que son gestionadas por uno o más proveedores de forma remota y las cuales se acceden mediante una suscripción. Un servicio SaaS puede ser facturado con base en el número de usuarios, el tiempo de uso, la cantidad de datos almacenados, transacciones procesadas, *logins*, entre otros.

En este modelo, las empresas cliente disponen de la última versión de las aplicaciones, directamente desde un navegador o una interfaz de programa, sin necesidad de instalar o mantener el software. Ésta responsabilidad, así como la gestión de la infraestructura, la seguridad y la disponibilidad de los datos, recae sobre el proveedor del servicio. Normalmente, la empresa cliente tiene el control de la configuración de la aplicación.

4. IDC, IDC's Latest CloudView Multiclient Study Reveals Attitudes and Strategies of the 58% of Organizations Embracing Cloud, Press release, February 2016.

Por otro lado, la adquisición de un SaaS puede darse de dos formas: privada y comunitaria. Mientras que en el primer caso, el servicio es de uso exclusivo de una empresa con múltiples consumidores, como unidades de negocio; en el segundo, es compartido por un exclusivo grupo de organizaciones.

A diferencia del SaaS privado, en el esquema comunitario los datos se almacenan en recursos compartidos por el grupo, aunque ninguno de los miembros tiene acceso a los datos de los demás. A esto último, se le conoce como *multi-tenancy*.

Algunos de los proveedores de SaaS son: Open International y Microsoft Online Services.

Seguridad, ¿el mayor desafío de Cloud?

La mayor preocupación en Cloud es la seguridad de la información, debido a la sensibilidad de los datos que son expuestos al proveedor. Sumado a lo anterior, estos son almacenados en recursos que están fuera del control de la empresa cliente y, en ocasiones, se desconoce la ubicación del *data center* en donde residen. Además, existe la posibilidad que terceros accedan a los datos dado que los modelos de servicio operan a través de internet.

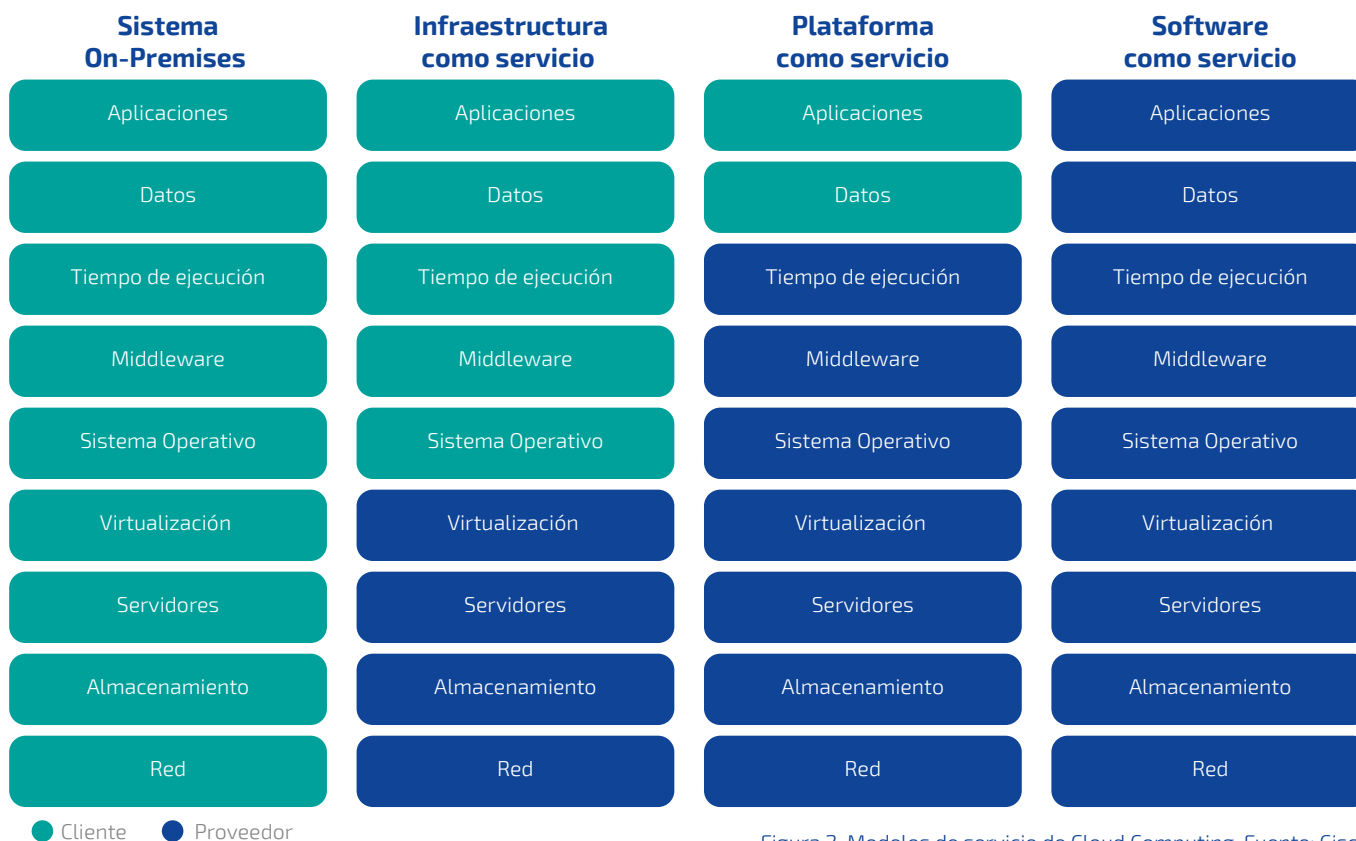


Figura 2. Modelos de servicio de Cloud Computing. Fuente: Cisco

En la Figura 2, se pueden observar los recursos que son manejados por el proveedor y por la empresa cliente en cada modelo de servicio de Cloud. En cada modelo, las responsabilidades del proveedor aumentan, liberando a las áreas de IT de la gestión de la infraestructura, las aplicaciones y los servicios para enfocarse en la búsqueda de otras tecnologías que generen valor para el negocio.

Por esto, la transición de sistemas *on-premises* a *Cloud* causa temor, ya que implica la transferencia a un tercero de gran parte de la responsabilidad en la gestión y el control de este tipo de activos.

Para contrarrestar estas amenazas, los proveedores de estos servicios utilizan diferentes mecanismos de autenticación y autorización, que verifican la identidad del usuario

que intenta acceder a los datos, los servicios y las aplicaciones. Por otro lado, los recursos en *Cloud* son compartidos, lo que obliga a los proveedores a contar con diversas herramientas de seguridad, como los sistemas de detección de intrusos, que les ayuden a evitar el acceso no autorizado.

Asimismo, los contratos con proveedores de servicio en la nube tienen cláusulas que ayudan a garantizar la implementación de controles para la protección de los datos almacenados y procesados, como también, la recuperación de la información en caso de desastres naturales, fallas técnicas u otro tipo de eventos.


Al tratarse de servicios que operan sobre internet, se vuelve vital contar con mecanismos de seguridad como cifrado de datos, desde el dispositivo del usuario final hasta el proveedor *Cloud*, reduciendo la posibilidad de ataques cibernéticos durante la transmisión de los mismos. Otra estrategia que pueden adoptar las empresas clientes para afrontar los retos de seguridad es la inversión en nubes híbridas, especialmente para los procesos de misión crítica.

Sin embargo, es importante que, durante el proceso de contratación, las empresas cliente tengan especial cuidado con aquellos aspectos de seguridad que recaen sobre ambas partes. Para esto, es necesario contar con una excelente estrategia de gobernanza, la cual consiste en definir los límites de las responsabilidades entre el proveedor y el cliente, y la aplicación de políticas en el uso de los servicios, en otras palabras, establecer las reglas y los principios organizativos desde el inicio de la relación comercial, para obtener mayores beneficios del servicio.

Por otra parte, es muy común que las personas reutilicen sus contraseñas de correo electrónico y de redes sociales para acceder a las aplicaciones empresariales, implicando una potencial falla de seguridad y una mayor responsabilidad de la empresa cliente en la implementación de políticas que mejoren la gestión de las credenciales. Además, es importante que las empresas cliente cuenten con planes de contingencia para que sus procesos críticos continúen operando incluso durante una falla eventual del SaaS. Por estas razones, garantizar la seguridad de los datos no radica únicamente en el proveedor.

Finalmente, existe un conjunto de estándares en el mercado que buscan unificar los criterios para evaluar la seguri-

dad y continuidad de los proveedores Cloud, como la ISO/IEC 27001 y SOC 3, que son las dos evaluaciones formales más reconocidas y utilizadas. Además, se espera que en los próximos años se verifiquen los controles de seguridad y privacidad establecidos en los estándares ISO 27017 y 27018, respectivamente, durante este tipo de evaluaciones.



¿Qué precauciones debe tener en cuenta si piensa migrarse a la nube?

Como parte de su migración hacia los servicios Cloud, las empresas deben evaluar las diferencias del costo total de propiedad entre mantener un *data center* tradicional y la contratación de un proveedor Cloud en cuanto a: recursos de almacenamiento y procesamiento, generación de copias de seguridad, recuperación de desastres, mantenimiento de software, licenciamientos, seguros y contratación de personal.

A través de este ejercicio, se podrá determinar cuáles servicios de IT son susceptibles de migrarse a Cloud y cuáles se mantienen en el modelo tradicional, con la finalidad de suplir las necesidades del negocio, empleando un menor presupuesto.

Antes de realizar una inversión en Cloud, las empresas deben asegurarse de contar con un proveedor que demuestre la capacidad de mantener segura su información y garantice el borrado de los datos cuando el cliente lo solicite.

Otra consideración que deben tener en cuenta es la negociación de acuerdos de niveles de servicio (SLAs), que ayudan a determinar los tiempos de respuesta que manejará el proveedor ante cualquier eventualidad en la operación, así como los tiempos de disponibilidad. Adicionalmente, considere el nivel de portabilidad ofrecido dado que la transición de cargas entre nubes es todavía un factor que puede causar retrasos en la operación del negocio.

Por otro lado, las personalizaciones de una aplicación empresarial en la nube (SaaS) son limitadas e incluso

inexistentes. Para ayudar a disminuir la preocupación de las *Utilities* en este aspecto, el proceso de selección del proveedor SaaS debe tener como criterio que la aplicación evaluada cumpla con las necesidades actuales de su negocio y esté desarrollada bajo las prácticas de la industria, de modo que se reduzca la necesidad de realizar modificaciones al software.

Por último, Cloud no es un diferenciador clave de su negocio, por tanto, para las empresas de servicios públicos, éste no representa una ventaja frente a su competencia, sino un conjunto de beneficios significativos en su operación.



El gasto de capital de las empresas de servicios públicos disminuye, mientras que el operacional aumenta.



Hasta el **2019**, las soluciones basadas en SaaS serán usadas como nuevas soluciones para reemplazar y complementar a los sistemas existentes⁵.

¿Por qué las empresas de servicios públicos están moviéndose hacia Cloud?



Los clientes acceden una aplicación sin los costos iniciales de la adquisición de equipos y software, el cual es reemplazado por un valor de alquiler.



Los tiempos de instalación y configuración disminuyen, dado que los sistemas se encuentran listos para operar.



Las actualizaciones del software son más frecuentes y menos disruptivas.



Los costos de mantenimiento se reducen, los proveedores SaaS dividen este valor entre todos los suscriptores del servicio.



El proveedor del SaaS se encarga de realizar las actualizaciones del software y solucionar las eventualidades del día a día, así como de la gestión y el control de la infraestructura.



Las empresas cliente pueden utilizar sus propias licencias, dependiendo de los términos establecidos.

Escale sin límites con...

Open Smartflex, una suite de soluciones basadas en las mejores prácticas y estándares de la industria de *Utilities*, que puede ser implementada en la nube pública (en Amazon AWS y Microsoft Windows Azure), en la [nube](#) privada o en sus propias instalaciones contando con Open para la administración de la infraestructura como servicio. Además, funciona en 2 modelos: Software como un servicio (SaaS) o con un plan de licencias tradicionales (on-premises).

A través de las herramientas de control de acceso que ofrecen los proveedores de servicios en la nube y los mecanismos de [autenticación](#) de Open Smartflex, las empresas evitan accesos no autorizados y ataques informáticos, impidiendo la fuga de información.

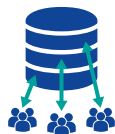


Open Smartflex ha sido desplegado en la nube para **3.6 millones** de usuarios.

5. Gartner, Adapting Your IT Strategy for a Cloud-Dominated Business Application Environment, webinar, Michael Maoz, 2016

Utilizando la solución CIS de Open Smartflex, las empresas de [energía](#), [acueducto](#) y [gas](#) administran los procesos de servicio al cliente, medición del consumo, facturación y recaudo de forma ágil, logrando mejorar sus procesos, asegurar sus ingresos e implementar rápidamente cambios normativos, al mismo tiempo que aumentan el retorno de inversión (ROI) en tecnología.

Adicionalmente, Open Smartflex integra estos procesos comerciales con los operativos, a través de su solución [Field Service](#) que ayuda a las empresas a planear, ejecutar y mejorar sistemáticamente su operación en campo, con los más altos estándares de calidad.



Uno de los mayores beneficios que brinda Open Smartflex es la consolidación de la base de datos a través del modelo *multitenant*, que consiste en un servicio compartido que aísla de forma segura los datos propios de cada empresa cliente.

Ahora, con *Open Smartflex como servicio*, las empresas pueden enfocarse en la administración de los procesos de su negocio y el desarrollo de estrategias innovadoras que fortalezcan su posición en el mercado, acompañadas de un grupo de expertos encargados de la administración de la [infraestructura](#), la [capacitación](#) de usuarios finales y el [soporte](#) 24/7 a la operación, garantizando alta disponibilidad y continuidad en su negocio.

Beneficios con Open Smartflex

- Gestione su empresa en cualquier momento y lugar
- Reduzca costos en su infraestructura tecnológica
- Asegure la continuidad de su negocio
- Opere con confianza y seguridad
- Evite el acceso no autorizado a la información

Conclusión

Cloud Computing es una tecnología clave que ofrece flexibilidad y disponibilidad en el acceso a servicios y aplicaciones a empresas de energía, acueducto y gas. Además de satisfacer la demanda elástica de recursos informáticos, a través de diferentes modelos de despliegue y servicio, también ofrece la reducción significativa de costos y un mejor aprovechamiento del área de IT de las compañías.

Con el fin de obtener estos beneficios del Cloud, las empresas de servicios públicos están adoptando aplicaciones empresariales en la nube, como Open Smartflex, que además de apoyarlas en la gestión de sus procesos de misión crítica, garanticen la seguridad de su información para una migración ágil y confiable hacia Cloud.

Conozca cómo su empresa puede generar mayores beneficios con Open Smartflex en la nube

Solicite un Demo

USA:

600 California St, Suite 14-032
San Francisco, CA 94108
Teléfono: +1 305 265 0310

6190 SW 116th St.
Miami, FL. 33156
Teléfono: +1 305 265 0310

COLOMBIA:

Carrera 103 No. 16-20, Cali, CLO
Teléfono: +572 - 331 9999
Fax: +572 - 331 9911



Visita www.openintl.com

Copyright © 2016, Open International. Todos los derechos reservados. El contenido de este documento es de carácter informativo y puede ser modificado sin previo aviso. No está permitida su reproducción total ni parcial. Este documento y su contenido no representan una obligación contractual con respecto a las soluciones que provee Open International.

White paper "Cloud Computing: 1 paso más cerca de ser una Utility digital".
Autor Dirección de Producto