**EL CAMINO A LA NUBE**

La adopción de las nubes es un camino, no una única implementación. La consolidación y la Vitalización de la tecnología, y la re automatización de su administración se producirán pronto en el camino, y darán beneficios financieros inmediatos

Pasos para comenzar el camino a una nube confiable:

•Entender los requisitos de confianza de un ambiente computacional y los perfiles de confianza de las opciones de nube potenciales.

•Identificar las cargas de trabajo candidatas para implementar en nube, con especial atención a la naturaleza y el flujo de la información.

•Evaluar los beneficios económicos de transferir cada carga de trabajo a la nube y qué opción de nube se prefiere.

•Evaluar la factibilidad funcional y los beneficios de transferir cada carga de trabajo a la nube y qué opción de nube se prefiere.

•Evaluar la factibilidad relacionada con la confianza y los beneficios de transferir cada carga de trabajo a la nube y qué opción de nube se prefiere.

•Asignar las cargas de trabajo candidatas a las opciones de nube, desarrollar una imagen Compuesta, y evaluar las implicancias y los beneficios generales.

•Evaluar la preparación de la organización y desarrollar un plan de trabajo para colocar las piezas nuevas en su lugar, desde la tecnología y la automatización, hasta los cambios de procesos y capacitación del personal, la migración de cargas de trabajo específicas a sus nubes de destino, todo bajo la guía de una estructura clara de buen manejo y control.

•Estar preparado para evaluar continuamente la combinación de implementaciones y destinos de nube a medida que los servicios de nube y las tecnologías detrás de ellas continúan avanzando.

**SOLUCIONES PARA UNA NUBE CONFIABLE**

Las organizaciones que pasan a la nube pueden realizar acciones específicas para encarar cada uno de los seis requisitos de confianza que se trataron anteriormente. En cada caso, las acciones recomendadas son tanto tecnológicas como organizacionales. En conjunto, forman una solución completa para una implementación de nube confiable. Cumplimiento de normas se deben evaluar y documentar minuciosamente los requisitos de los tipos de datos, cargas de trabajo y jurisdicciones. Luego, deben implementarse estos requisitos, ya sean legales, de la industria o contractuales, en los procesos de administración y en código, para garantizar tanto su cumplimiento como la prueba del cumplimiento. Debe monitorearse cómo cambian los requisitos, especialmente, a medida que se hacen más específicos de la nube.

**BUEN MANEJO Y CONTROL**

Deben monitorearse las operaciones de nube, incluidas las reglas y políticas relacionadas con la confianza, y su implementación. Se deben establecer explícitamente las responsabilidades y educar al personal sobre el autoservicio y el uso eficaz de los servicios de nube. Debe crearse una cultura de compartir información en forma responsable.

**ADMINISTRACION DE RIESGOS**

Deben evaluarse la viabilidad a largo plazo de los proveedores de servicios de nube, así como su capacidad inmediata de cumplir con los estándares legales e industriales. Deben evaluarse los procedimientos de monitoreo y gestión de riesgos, y asegurarse de que la organización del cliente pueda mantener visibilidad suficiente mediante herramientas y registros de auditoría. La adopción de estándares asegura una mayor portabilidad y ayuda a evitar la obligación de trabajar con un proveedor determinado.

**DISPONIBILIDAD**

Es necesario asegurarse de que la implementación de nube incluya métodos sólidos de resiliencia y recuperación, que pueden incluir cambios de productos transparentes y “sistemas activos” listos para entrar en marcha en caso de una falla integral del sistema. También es necesario asegurarse de que la solución proporcione la escalabilidad y el rendimiento adecuados.

**INTEGRIDAD**

Deben emplearse encriptación de datos, controles de acceso y métodos para garantizar que las transacciones se completen y no se rechacen. Cada vez que sea posible, deben incorporarse reglas para el acceso y uso de conjuntos de datos confidenciales. Se debe prestar especial atención a la seguridad y la transparencia en un ambiente con múltiples arrendatarios.

**CONFIDENCIALIDAD/PRIVACIDAD**

Limitar el acceso a información de partes no autorizadas requiere una sólida administración de identidades, controles de claves y contraseñas, autenticación física y lógica, y controles sólidos de la transferencia de datos entre sistemas. Debe garantizarse la segregación física de los datos donde sea necesario. También se debe tener un enfoque de ciclo de vida hacia la administración de datos, incluida la destrucción oportuna de datos.

**OPCIONES E IMPLEMENTACION DE LAS NUBES**

Cloud computing abarca varias opciones de implementación, cada una de las cuales tiene un perfil de confianza diferente. Por eso, la pregunta no es si se debe confiar en “la nube”, sino qué opción de nube (si la hubiera) (pública, privada o híbrida) es confiable y adecuada para cualquier aplicación dada y sus datos. Las variables clave a considerar desde la perspectiva de la administración y la confianza son:

•Ubicación física y propiedad. ¿El cliente o el proveedor son propietarios y administradores de las instalaciones, la infraestructura de hardware y otros recursos tecnológicos

•Segregación física de activos. ¿Los servidores y otros recursos se mantienen separados o se comparten entre clientes? Incluso cuando la ubicación física y el control pertenezcan al proveedor, se pueden reservar recursos para un solo cliente, o se pueden agrupar físicamente y provisionarse como recursos virtuales.

•Control operacional. ¿Quién administra la operación diaria de los servicios de nube? Incluso cuando el control es compartido o principalmente del proveedor, ¿el cliente de la empresa tiene visibilidad y control suficientes para administrar el consumo de los servicios?

**NUBE PÚBLICA**

La nube pública todavía enfrenta inquietudes válidas de confianza. Algunas de ellas se relacionan con la capacidad tecnológica del proveedor. Por ejemplo, la personalización es un desafío para cualquier proveedor “principiante” de servicios de nube. Algunas inquietudes se relacionan con la organización del cliente, por ejemplo, quién tiene autoridad para contratar servicios de nube pública y quién es responsable de proteger los datos que puedan pasar al proveedor.

**NUBE PRIVADA**

La nube privada enfrenta un conjunto más pequeño de desafíos de cumplimiento con normas en comparación con la nube pública porque la ubicación geográfica de los datos es clara y el control de los activos es directo. Las organizaciones pueden adaptar los procesos y procedimientos existentes a un ambiente más virtualizado y de autoservicio al mismo tiempo que mejora la transparencia y la capacidad de administración del ambiente computacional. Se debe tener presente que la implementación de nubes privadas puede realizarse fuera de las instalaciones con una nube privada externa.

**Una nube privada puede fortalecer la confiabilidad en tres formas profundas:**

•Visibilidad. En un ambiente de TI tradicional, el monitoreo del rendimiento y la seguridad en una infraestructura diversa y heterogénea es un desafío constante. La tecnología, comenzando con el hipervisor “que ve todo”, que automatiza la operación de una nube privada bien implementada, también brinda una visibilidad sin precedentes de esas operaciones.

•Confiabilidad. La virtualización de los activos, al separarlos lógicamente de físicamente, aumenta la tolerancia a las fallas y la resiliencia. En el caso de una falla local, las aplicaciones pueden migrar automáticamente a recursos disponibles cercanos.

•Protección de activos. El fabric de administración de seguridad actual de la empresa, incluidos firewalls, encriptación y contraseñas, se puede extender al ambiente virtualizado. En el proceso de