GOBIERNO *de* GUATEMALA
DR. ALEJANDRO GIAMMATTEI

COMISIÓN PRESIDENCIAL
DE GOBIERNO ABIERTO
Y ELECTRÓNICO

MANUAL *de* USO *de la* NUBE *para el* ORGANISMO EJECUTIVO *2023*

MANUAL *de* USO *de la* NUBE *para el* ORGANISMO EJECUTIVO *2023*

ÍNDICE

INTRODUCCIÓN 9

1. OBJETIVO DE LA GUÍA 10

2. COMPUTACIÓN EN LA NUBE 11

3. ALMACENAMIENTO Y TIPOS DE ALMACENAMIENTO EN LA NUBE 12
- 3.1. Almacenamiento en la nube 12
- 3.2. Modelos de implementación 12

4. TIPOS DE SERVICIOS QUE OFRECE LA NUBE 14
- 4.1. Software as a Service (SaaS, por sus siglas en inglés) 14
- 4.2. Platform as a Service (PaaS, por sus siglas en inglés) 14
- 4.3. Infrastructure as a Service (IaaS, por sus siglas en inglés) 15

5. MODELO DE RESPONSABILIDAD COMPARTIDA 17
- 5.1. Tipos de responsabilidad 17

6. ENTIDADES A QUIENES APLICA ESTE MANUAL 19

7. PRINCIPIOS DEL MANUAL 20

8. INTELIGENCIA ARTIFICIAL 23

9. CIBERSEGURIDAD 24

APARTADO I
CONSIDERACIONES LEGALES 25

APARTADO II
DISPOSICIONES GENERALES 26

APARTADO III
ADMINISTRACIÓN DE LA INFORMACIÓN 28

APARTADO IV
SEGURIDAD DE TECNOLOGÍA DE LA INFORMACIÓN 29

APARTADO V
PROCESAMIENTO DE LA INFORMACIÓN 31

APARTADO VI
PROPIEDAD DE LOS DATOS, RECUPERACIÓN Y ACCESOS 33

APARTADO VII
FISCALIZACIÓN DE LOS SERVICIOS EN LA NUBE 34

APARTADO VIII
RECOMENDACIONES DE SEGURIDAD 36

APARTADO IX
DISEÑO DE ARQUITECTURA EN LA NUBE 38

APARTADO X
DISEÑO DE SEGURIDAD DE MIGRACIÓN A LA NUBE 40

Referencias 43

MANUAL *de* USO *de la* NUBE *para el* ORGANISMO EJECUTIVO *2023*

INTRODUCCIÓN

Cuando se habla de nube, debe tenerse en cuenta una serie de elementos que se relacionan entre sí y que permiten de manera simbiótica, el funcionamiento de la misma.

Para que las diferentes instituciones gubernamentales y no gubernamentales puedan funcionar en la nube, es necesaria la contratación de los insumos de hardware (servidores, redes y almacenamiento) de software (sistemas operativos, manejadores de bases de datos, entre otros), herramientas de diagnósticos, por mencionar algunos. El uso o consumo de los mismos, es lo que genera el cobro y por ello, es necesario entender su funcionamiento para contratar dichos servicios de forma provechosa para la institución que realiza el contrato.

Una configuración incorrecta, conlleva a una contratación incorrecta; lo cual, puede hacer más caro el servicio en la nube; es por ello, que es importante determinar los servicios que deben ser puestos a disposición en esta modalidad, así como el nivel de responsabilidad más adecuada tanto para la institución como para el proveedor.

Por otro lado, el tener servicios desde la nube, conlleva otros elementos importantes tales como: el almacenamiento, los modelos de implementación, la inteligencia artificial, la ciberseguridad o la fiscalización de los servicios que se brindan por medio de la computación en la nube. Estos temas, se abordan en este Manual de forma sencilla.

Se invita a todos los investigadores, a hacer sus propias búsquedas y ahondar en los temas abordador en este Manual, para sacar el mayor provecho al momento de una contratación de los servicios en la nube.

1. OBJETIVO DE LA GUÍA

Proporcionar al lector las orientaciones generales para comprender el modelo de computación en la nube, sus características técnicas, ventajas y desventajas, así como las consideraciones legales al momento de optar por alguno de los modelos disponibles.

2. COMPUTACIÓN EN LA NUBE

No existe una definición unificada al respecto, sin embargo, existen algunos organismos como el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology -NIST-), que es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. -A este respecto, el NIST ofrece la siguiente definición:

> "La computación en la nube es un modelo para habilitar el acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración o interacción con el proveedor de servicios. Este modelo de nube se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de implementación." (Mell & Grance, 2011, pág. 2)

Algunas definiciones provistas por los proveedores de servicios de nube más conocidos, son:

> "La computación en la nube es la disponibilidad a pedido de los recursos de procesamiento como los servicios por Internet. Elimina la necesidad de que las empresas obtengan, configuren o administren recursos por su cuenta; de esta forma, solo paguen por lo que usan." (Google)

> "La informática en la nube es la distribución de recursos de TI bajo demanda a través de Internet mediante un esquema de pago por uso. En lugar de comprar, poseer y mantener servidores y centros de datos físicos, puede acceder a servicios tecnológicos, como capacidad informática, almacenamiento y bases de datos, en función de sus necesidades a través de un proveedor de la nube." (AWS)

> "Dicho de manera sencilla, la computación en la nube es el suministro de servicios informáticos (incluidos servidores, almacenamiento, bases de datos, redes, análisis e inteligencia) a través de internet ("la nube"), cuyo objetivo es ofrecer una innovación más rápida, recursos flexibles y economías de escala. Lo habitual es pagar por los servicios en la nube utilizados, a fin de reducir los costos operativos, ejecutar la infraestructura con más eficacia y escalar a medida que cambian las necesidades de tu negocio." (Azure)

Como se puede apreciar, el concepto de nube es la contratación de los insumos necesarios, ya sean estos de hardware (servidores, redes y almacenamiento, entre otros) y software (sistemas operativos, manejadores de bases de datos, herramientas de diagnósticos, por mencionar algunos). Estos insumos, son cobrados o facturados de acuerdo al uso o consumo de los mismos y la facilidad de crecimiento o decrecimiento de acuerdo a las necesidades de las instituciones; sin embargo, esto depende de la configuración y lo contratado. La seguridad, está incluida en todas las etapas cuando se trabaja con nube. El proveedor de servicios, se hace cargo del Hardware, Boot, IPC, seguridad en almacenamiento y encriptado como mínimo.

La computación en la nube, da la posibilidad de aumentar los servicios con base en el internet, mejorando y aumentando el ecosistema digital de gobierno, fortaleciendo la transparencia, el ahorro al pagar por consumo (claro que esto depende de una buena configuración y contratación adecuada), la accesibilidad a los servicios, la sencillez en los trámites, el servicio orientado al ciudadano y el valor público.

Ya con las definiciones anteriores, se puede empezar a tratar los siguientes temas referentes a este Manual.

3. ALMACENAMIENTO Y TIPOS DE ALMACENAMIENTO EN LA NUBE

3.1. ALMACENAMIENTO EN LA NUBE

El almacenamiento en la nube, parece una idea o concepto novedoso; sin embargo, la realidad es que durante muchos años se ha venido haciendo uso de este servicio; ¿Cómo es esto?, el ejemplo más claro es el correo electrónico. Esta herramienta, en muchas ocasiones, está en la nube y lo accedemos por medio del internet, herramienta sin la cual, nada de estos servicios sería posible. Así también, las redes sociales utilizan este tipo de almacenamiento, donde los usuarios suben y guardan fotografías, videos o imágenes; es más, las redes sociales recuerdan lo que se publica en fechas anteriores.

Se infiere entonces, que el almacenamiento en la nube es el hecho de guardar los datos en una computadora o servidor que está remoto o lejano, pero con la facilidad y la posibilidad de acceso por diferentes dispositivos, ya sean móviles o fijos, sin importar el lugar donde la persona se encuentre.

El acceso al almacenamiento en la nube (servicios de almacenamiento en nube), puede realizarse por diferentes medios como: interfaces web, APIs o un web service.

3.2. MODELOS DE IMPLEMENTACIÓN

Se conocen varias descripciones en lo que respecta a este apartado, sin embargo, todos los estándares y descripciones acerca de este tema particular, ostentan sus definiciones en estos 4 tipos:

1. **Público:** Almacenamiento en la nube disponible al público en general de forma abierta e ilimitada. Es un servicio que se aloja de forma externa al usuario, pudiéndose acceder fácilmente a través de Internet.

2. **Privado:** Esta forma de almacenamiento, se encuentra dentro de las instalaciones del usuario regularmente, o en instalaciones de un proveedor de centro de datos externo; es una infraestructura local, operada exclusivamente por un solo cliente que la controla y la pone al funcionamiento de su organización, brindando el servicio a sus usuarios, quienes son parte de sus unidades de trabajo. Este servicio, podría ser proveído también por un tercero a la institución (modelo válido), pero dejando claro que, es para uso Inter operacional.

3. **Híbrido:** Combinación de dos a más nubes, que engloba los modelos anteriores (pública y privada) que siguen siendo únicas, pero interconectadas en los servicios que se necesitan. El cliente es propietario de una parte, sin embargo, comparte otras. Las nubes híbridas permiten a las empresas tener una gran flexibilidad, portabilidad, interoperabilidad, así como no incurrir en tantos gastos como en la nube privada. En forma sencilla, es una combinación de la nube privada y de la nube pública.

4. **Nube Comunitaria:** Este concepto se refiere, a que la nube está provista para uso exclusivo por una comunidad específica a organizaciones que tienen preocupaciones compartidas (por ejemplo, misión, requisitos de seguridad, políticas y consideraciones de cumplimiento). Puede ser propiedad, administrada y operada por una o más de las organizaciones de la comunidad, un tercero o alguna combinación de ellas, y puede existir dentro o fuera de las instalaciones.

4. TIPOS DE SERVICIOS QUE OFRECE LA NUBE

Los servicios en la nube considerados en este Manual, son los establecidos por los 3 modelos de servicios según el modelo de computación en la nube de NIST: SaaS, PaaS e IaaS.

4.1. SOFTWARE AS A SERVICE (SaaS, por sus siglas en inglés)

SaaS es aquella aplicación ofrecida por un fabricante de software o proveedor de servicios informáticos a través de Internet, para la utilización por varios clientes. El fabricante es el que en última instancia se ocupa del mantenimiento de la privacidad de los datos y la personalización de la aplicación, sobre la base de lo requerido por cada cliente. En este modelo de servicio, el usuario paga por el uso y por la infraestructura necesaria (almacenamiento, seguridad, alojamiento, respaldos de datos) limitándose a utilizar la herramienta y sus funcionalidades.

Estos servicios corresponden a la capa, más alta de los servicios en la nube. La mayor responsabilidad está del lado del proveedor de servicios (seguridad, infraestructura, operaciones, identidad, almacenamiento, desarrollo y más) y el cliente de manera privada y aislada, es responsable y dueño de su información, políticas de acceso y el uso.

4.2. PLATFORM AS A SERVICE (PaaS, por sus siglas en inglés)

El portafolio de servicios de nube, amplía las prestaciones del caso anterior; pues se puede desplegar en ella, aplicaciones desarrolladas o adquiridas por el mismo (cliente/entidad), para ampliar las funcionalidades. Todo esto, por supuesto, se deberá desarrollar en aquellos lenguajes de programación que sean soportados por el proveedor de la nube. En este modelo de nube, el usuario no podrá gestionar la infraestructura de la nube (aunque si puede escalar o buscar más recursos), pero tendrá acceso tanto sobre las aplicaciones desplegadas en ella, como en la configuración de las diversas herramientas que utilice.

Estos servicios corresponden a la segunda capa, capa media o del medio. En este caso, la responsabilidad del cliente está en el contenido, políticas de acceso, uso, desarrollo y medidas de seguridad para la aplicación web, así como la personalización para su uso individual

4.3. INFRASTRUCTURE AS A SERVICE (IaaS, por sus siglas en inglés)

Los servicios IaaS, son la externalización de servidores para procesamiento, almacenamiento y redes, lo cual facilita la implantación e implementación de contenedores de servicios a la entidad, el cliente puede tener control sobre los sistemas operativos, el almacenamiento y un control limitado sobre los componentes de red. Se paga por el nivel de consumo de los recursos: espacio en disco utilizado (va variando el precio de almacenamiento de archivo muerto e/o histórico y la cuenta corriente), tiempo de procesamiento -CPU-, espacio en base de datos, transferencia de datos. Este tipo de soluciones, desplaza una serie de problemas al proveedor, relacionados con la gestión de las máquinas y el ahorro de costes. Las infraestructuras como servicio, pueden permitir una escalabilidad automática o semiautomática, de forma que podamos contratar más recursos según se vaya necesitando.

La IaaS, es llamada en algunos casos, hardware as a service (HaaS) y corresponde a la capa inferior en donde se van a encontrar servidores, enrutadores, discos duros o sistemas de almacenamiento, entre otros. En este caso, la responsabilidad aumenta para el cliente usuario de la nube, pues es responsable de las operaciones, acceso, autenticación y seguridad de red. El proveedor de servicios de nube, sigue a cargo del log de auditoría, red en general, almacenamiento, IPC y el hardware.

La responsabilidad compartida, es la que dicta las obligaciones de seguridad en la nube entre el proveedor de servicios de nube y el cliente usuario de la nube. El modelo de responsabilidad compartida, cambia en función del modelo de servicio que se esté implementando.

El proveedor local (partner del proveedor de nube), tiene a su cargo la transferencia de conocimiento, la aplicación de las buenas prácticas y la facturación de (los) servicio(s).

Ventajas a considerar en la actualidad

- **Economías de escala:** Los proveedores incrementan el portafolio de servicios hacia el mercado tecnológico, quien demanda de cada uno de ellos (los servicios) la especialización en cada área, esto genera un incremento en la demanda y la confianza de la producción de los proveedores, el volumen de clientes que contrata cada especialidad, podría generar la disminución de los costos por servicio y por demanda y/o utilización de cada uno de ellos, lo que genera en cada proveedor altas economías de escala, y que se traduce en reducciones de costo naturales en el mercado de servicios tecnológicos, por lo que debería reflejarse en el mercado de precios y beneficios al contratante. Es de aclarar que, para la institución contratante depende de la configuración del servicio, pues si se mantienen activos, esto aumenta el consumo y por lo tanto el costo. Haciendo una analogía, es como tener un equipo eléctrico encendido todo el tiempo, aunque no sea necesario, y esto aplica en todas las implementaciones que se hagan, por eso se debe siempre consultar a los expertos.

- **Seguridad, privacidad y conformidad:** Al utilizar servicios en la nube, las entidades de gobierno gozarán del servicio de especialistas de

seguridad en los centros de datos del prestador del servicio y de forma conjunta, se implementan políticas de seguridad tecnológica y contra el ciberdelito. Las infraestructuras de la nube están diseñadas y se administran de acuerdo con un gran número de reglamentos, normas y las mejores prácticas recomendadas a nivel internacional; por ejemplo: las Normas ISO 27001, ISO 27017, ISO 27018, entre otros. Estos estándares son algunos a tomar en cuenta en el modelo de negocio a seleccionar, el cual será determinado por el comité de cada entidad, conforme a las necesidades existentes, así como a las consideraciones de ventajas y desventajas que dicho comité haga.

- **Auditoría:** La transparencia y estandarización de los servicios en la nube, permiten que se registre, monitoree y audite uniformemente el uso de dichos servicios: lo cual, favorece una revisión a detalle de los usuarios, grupos, roles, accesos y políticas asociadas para el cabal cumplimiento contractual, el mantener estándares internacionales como CISA, ISO 27001, ISACA/CSA/CCMv4, CSA Star, ISO/IEC 22301, entre otros. Estos estándares, son algunos a tomar en cuenta en el modelo de negocio a seleccionar, el cual será determinado por el comité de cada entidad conforme a las necesidades existentes, así como a las consideraciones de ventajas y desventajas que haga dicho comité.

- **Equipo:** Uno de los grandes beneficios de la nube, es permitir que las instituciones no adquieran equipo físico (Hardware) sujeto a la obsolescencia y los riesgos que esto conlleva; debido a que el proveedor del servicio, es el responsable de mantener la actualización constante de toda la infraestructura en sus centros de datos.

Existen otros beneficios entre los que se pueden mencionar: demanda en auto servicio, amplio acceso a la red, recursos comunes, rápida elasticidad, por mencionar algunos.

Es necesario comprender, que la nube es un derecho de uso de los servicios de tecnologías provisionados bajo demanda, con un sistema de cobro y/o pago por lo que se usa; de esa cuenta, se propone el siguiente Manual como un instrumento base: el cual, debe evolucionar conforme el desarrollo e innovación del mercado tecnológico.

5. MODELO DE RESPONSABILIDAD COMPARTIDA

La responsabilidad compartida, se refiere a la responsabilidad que tiene el cliente que contrata servicios de nube, así como la responsabilidad que tiene el proveedor de servicios de nube.

El blog en donde la autora Sara Harvey escribe sus ideas y opiniones indica:

> "¿Qué es el modelo de responsabilidad compartida?
> El modelo de responsabilidad compartida es un método para determinar cuáles funciones desempeñan los proveedores de servicios en la nube y cuáles los clientes de servicios en la nube en materia de seguridad de la nube. En general, el modelo de responsabilidad compartida establece que los proveedores son responsables de la seguridad "DE" la nube y los clientes son responsables de la seguridad "EN" la nube. Los proveedores de servicios en la nube y los clientes deben trabajar juntos para cumplir los objetivos de seguridad en la nube." (Harvey, 2018)

5.1. TIPOS DE RESPONSABILIDAD

- **Responsabilidad del proveedor de servicios en la nube (CSP) en relación con la "seguridad de la nube":** El CSP es responsable de proteger la infraestructura que ejecuta todos los servicios provistos en la nube. Esta infraestructura está conformada por el hardware, el software, las redes y las instalaciones que ejecutan los servicios de la nube.

- **Responsabilidad del cliente en relación con la "seguridad en la nube":** la responsabilidad del cliente estará determinada por los servicios de la nube que el cliente seleccione. Esto determina el alcance del trabajo de configuración a cargo del cliente como parte de sus responsabilidades de seguridad.

El modelo de responsabilidad compartida cambia en función del modelo de servicio que se esté implementado, ya sea IaaS, PaaS o SaaS.

En el caso de las soluciones de IaaS, el proveedor de servicios en la nube debe gestionar elementos como las instalaciones, los centros de datos, las interfaces de red, el procesamiento y los hipervisores. El cliente del servicio en la nube, es responsable de proteger y administrar la red virtual, las máquinas virtuales, los sistemas operativos, el middleware, las aplicaciones, las interfaces y los datos.

Las soluciones de PaaS cambian las responsabilidades del proveedor de servicios en la nube y añaden algunos elementos a sus funciones. El cliente sigue siendo responsable de proteger y administrar las aplicaciones, las interfaces y los datos.

En el caso de las soluciones SaaS, las responsabilidades vuelven a cambiar. Ahora, el cliente del servicio en la nube es responsable de la seguridad de las interfaces y los datos.

6. ENTIDADES A QUIENES APLICA ESTE MANUAL

Este Manual es de observancia general para todas las entidades del Organismo Ejecutivo, quienes dentro de su planificación estratégica en materia de tecnologías de la información y comunicación, atenderán la instrucción general del gobierno de optimizar y aplicar la inversión en tecnología por medio de enfoque de servicios para optimizar los recursos, respaldar las metas y objetivos relacionados; también podrá ser utilizado de manera supletoria, por todas las demás instituciones que conforman el sector público, que buscan alojar sus datos, aplicaciones o servicios en ese entorno, cuando la Institución no cuente con un Manual propio.

7. PRINCIPIOS DEL MANUAL

Este Manual, se basa en los siguientes principios de conducción:

- Las Tecnologías de la Información y la Comunicación (TIC) a nivel de la entidad, deben enfocarse en la excelencia funcional y en alcanzar un mayor valor hacia el ciudadano.

- La infraestructura de TIC es un habilitador clave para la consolidación y optimización a nivel nacional.

- Estandarizar la gestión de la infraestructura permite:
    - Optimizar el uso de infraestructura.
    - Mejora en la calidad del servicio.
    - Mejora en la calidad en seguridad.
    - Continuidad empresarial eficiente.

- Promover el enfoque de nube pública primero respetando todos los roles, legislación y mandatos de los Ministerios de Estado, Secretarías y demás entidades del Organismo Ejecutivo. El siguiente razonamiento de este principio se aplica para:

    - Evitar las múltiples ocurrencias innecesarias de la información de las personas en las entidades del sector público, y simplificar la complejidad asociada en cada una de ellas (entidades).
    - Diseñar la infraestructura de TIC de las entidades de la función pública con un enfoque de interoperabilidad fácil y rápido.
    - Permitir la optimización con arquitecturas modernas que basadas en servicios en la nube puedan facilitar la prestación de servicios intergubernamentales.

Derivado de lo anterior, todas las entidades estatales deberán evaluar el uso preferencial de los servicios basados en la nube al realizar las adquisiciones por concepto de TIC.

A las instituciones gubernamentales, se les exhorta a adoptar y usar servicios en nube en todos los casos, excepto:

- Cuando se pueda demostrar que una estrategia alternativa en la innovación tecnológica de implementación, implantación y/o complemento a las TIC no cumple con requisitos especiales que una entidad gubernamental a corto, mediano y/o largo plazo necesite.

- Cuando se pueda demostrar que una estrategia alternativa de implementación de las TIC es rentable desde una perspectiva de Costo Total de Propiedad (TCO), y demuestre por lo menos el mismo nivel de aseguramiento que ofrece un despliegue de computación en la nube.

Establecer que todos los servicios en nube sean aplicables a las normativas que regulan la función pública es fundamental, por lo que cada caso debe tener un análisis que sustente su apartado y la justificación adecuada para contratar cada servicio; sin embargo, la tendencia de beneficio en cuanto a lo financiero, y a diluir las especialidades del recurso humano en las diferentes áreas de las TIC, la facilidad de incrementar la capacidad instalada en hardware y software son tangibles, y contratar las mismas por el tiempo que sea necesario en su incremento o disminución es de forma ágil.

La versatilidad de su contratación puede hacerse bajo distintos modelos, entre ellos:

- **Demanda:** este modelo es pagar según el uso, es un pago por suscripción como se practica en las entidades de la energía eléctrica. Se debe considerar las características de flexibilidad de este modelo que incluye los servicios que puedo activar/desactivar (los cuales generan un costo al estar activos), crecer o disminuir que serían por ejemplo un procesador, un contenedor a diferencia de los servicios que son pre reservados; con los cuales, aunque la infraestructura esté inactiva (apagada) igual se consume, como en el caso de almacenamiento; pero también, puede aumentar o disminuir su capacidad.

- **Créditos:** este modelo es solicitar un "bolsón" de créditos (cada uno equivalente a US$1 de uso en la nube, y su equivalente a la moneda de curso legal). El valor del crédito lo da el proveedor, quien debe incluir los servicios de implementación, soporte, capacitación, así como los impuestos regulados en Guatemala. Para definir la cantidad de créditos, la institución debe asesorarse para hacer un estimado de lo que necesita de acuerdo a sus requerimientos. El estimado se obtiene al definir los recursos que se necesitan. A pesar de que se estime, puede ocurrir que, durante el uso de recursos, se encuentre una ventaja en un recurso no seleccionado anteriormente o el Proveedor de Servicios de Nube, sume a su oferta un recurso nuevo. Al usar este modelo de contratación, la institución podrá utilizar los nuevos recursos y la flexibilidad de la nube siempre y cuando se mantenga el estimado total de créditos.

- **Compromiso a un año o más (basado en contrato):** se compromete un valor contractual con pago fijo mensual/anual, donde se debe respetar el valor contratado. Hay opciones para Gobierno de Acuerdo de Suscripción, donde se garantiza el monto anual, y los casos que regula la Ley de Contrataciones del Estado. Generalmente, un compromiso implica que no se podrá reducir el valor mensual (lo cual no implica que no pueda cambiar los servicios) pero si puede expandir.

Cabe resaltar, la importancia de definir un modelo; para lo cual, la institución debe asesorarse para la estimación de acuerdo con el requerimiento adecuado a sus necesidades de los servicios a contratar, tanto para IaaS, PaaS y SaaS. Cada una requiere un análisis separado, pues un SaaS es diferente

a un IaaS, el cual se puede combinar con un PaaS. Adicionalmente, los diferentes proveedores de servicios de nube ofrecen los servicios con algunas variables y los servicios se pueden mezclar. La institución puede solicitar una evaluación de su infraestructura actual antes de definir los requerimientos con la asesoría respectiva.

Este Manual orienta a las entidades gubernamentales de la República de Guatemala, a implementar un entorno operativo común con el objetivo de alcanzar mayor dinamismo y agilidad. La computación en nube agiliza el desarrollo, el soporte y el alojamiento de soluciones TIC, lo cual resulta en un mejor rendimiento del servicio y una implementación más rápida de los mismos.

- Soportar los servicios gubernamentales con computación en la nube, da como resultado la reducción inmediata de tiempo para implantar e implementar infraestructura y mantenimiento.

- Incrementar la capacidad de gestión y la productividad de las soluciones de TIC, por medio de las actualizaciones del hardware y el software que gestiona el proveedor del servicio.

- Mejorar la integración entre servicios. Se habilitará una colaboración más efectiva a medida que las entidades tengan más facilidad para verificar y compartir información entre instituciones, mejorar la eficiencia y habilitar la creatividad en la prestación de servicios públicos.

- Lograr la continuidad operacional y recuperación de los servicios gubernamentales esenciales. Esto con el uso de copias de seguridad y almacenamiento de datos centralizados y redundantes, recuperación de datos en tiempos de crisis más rápidos y rentables.

- Optimizar el gasto público. La interconectividad de entidades y personas en las áreas urbanas y rurales, brindando servicios sin discriminación en las regiones sin cobertura física en el espacio geográfico nacional por las entidades, promoviendo un modelo virtual donde se atienda la demanda en la misma proporción a nivel general.

- Aumentar la seguridad contra ataques cibernéticos que atiende intereses económicos y políticos de organizaciones criminales en el mundo. De esta manera, los servicios en nube ofrecen a los usuarios la protección para que utilicen el potencial total de las TIC con tranquilidad; donde a los administradores, se les ofrece los recursos requeridos para lograr esta protección. Esto se logra siguiendo lineamientos de mejores prácticas que el proveedor debe ofrecer. No se puede comparar la extensión, costo y flexibilidad que se puede ofrecer en la nube vs equipo local.

8. INTELIGENCIA ARTIFICIAL

En palabras sencillas, la Inteligencia Artificial -IA- es un recurso computacional que aprende, adapta e interactúa con los usuarios de manera más natural.

Los servicios en la nube, abren la puerta para obtener productos, soluciones y servicios innovadores de Inteligencia Artificial (IA) y aprendizaje automático con la tecnología y las investigaciones de la nube seleccionada.

Los proveedores de nube, aplican IA en todos sus recursos computacionales para hacer productos más utilizables. Existen distintos usos y soluciones para ellos:

- **Ciencia de Datos:** para hacer modelos de IA más eficaces, teniendo flujos de trabajo de la ciencia de datos.
- **Desarrollo:** para entrenar modelos de aprendizaje de acuerdo con requerimientos personalizados, para obtener información a partir de texto no estructurado, para crear experiencias de conversación, convertir voz a texto y viceversa, para traducciones y más.
- **Infraestructura:** máquinas y recursos preconfigurados para el aprendizaje.
- **Seguridad:** aprovechar las analíticas con IA y aprendizaje automático para eliminar categorías completas de amenazas.

9. CIBERSEGURIDAD

La ciberseguridad, es la práctica de garantizar la confidencialidad, integridad y disponibilidad de la información mediante la protección de redes, dispositivos, personas y datos contra el acceso no autorizado o la explotación criminal.

Los adversarios de hoy, son unidades patrocinadas por algunos estados y grupos organizados de ciberdelincuencia. Estos actores de amenazas, operan a nivel mundial como un trabajo de tiempo completo y se dirigen a las organizaciones, con amenazas y malware para robo de información y chantajes.

A pesar de esto, las instituciones tratan de luchar contra estas amenazas con solo una pieza del rompecabezas: la telemetría de la red.

En esta época, en la que el perímetro se ha extendido fuera de las instituciones, se hace necesario contar con herramientas de Ciberseguridad que permitan correlacionar los eventos a nivel de los end points y también de los servicios de nube. Así mismo, es importante contar con herramientas que reflejen el contexto de las amenazas para poder enfrentarlas de la mejor manera posible.

Cualquier solución de ciberseguridad que las organizaciones adquieran, deberá cubrir alguno de los dominios definidos de Ciberseguridad:

1. Seguridad y Gestión de Riesgos.
2. Seguridad de activos.
3. Arquitectura e Ingeniería de Seguridad.
4. Comunicaciones y Seguridad de Redes.
5. Gestión de identificación y acceso.
6. Evaluación y pruebas de seguridad.
7. Operaciones de seguridad.
8. Seguridad de desarrollo de software.
9. Inventario de infraestructura crítica.

APARTADO I
CONSIDERACIONES LEGALES

1.1. Sustento legal del Manual. La sustentación legal del presente Manual, está contenida en lo establecido en la normativa legal vigente, tanto en los artículos de los Decretos del Congreso de la República de Guatemala y, los Acuerdos Gubernativos siguientes:

a) Constitución Política de la República de Guatemala, Artículo 30.- Publicidad de los actos administrativos.

b) Decreto 31-2002 del Congreso de la República de Guatemala, Ley Orgánica de la Contraloría General de Cuentas, Artículos 3 literal d) y 4 literales u) e y).

c) Decreto 47-2008 del Congreso de la República de Guatemala, Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Artículos 13 y 14.

d) Decreto 57-2008 del Congreso de la República de Guatemala, Ley de Acceso a la Información Pública, Artículos 3, 9, 30, 36, 37, y 39.

e) Acuerdo Gubernativo número 9-2017, Reglamento de la Ley Orgánica de la Contraloría General de Cuentas, artículo 28 literal h).

f) Acuerdo Gubernativo número 135-2009, Reglamento para Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, Artículos 5, 6, 8 y 9.

g) Acuerdo Gubernativo número 360-2012 y sus reformas, que crea la Comisión Presidencial de Gobierno Abierto y Electrónico, Artículos 2 y 6.

h) Acuerdo número A-039-2023 Normas Generales y Técnicas de Control Interno Gubernamental; Norma no. 3, Normas Aplicables a las Actividades de Control.

APARTADO II
DISPOSICIONES GENERALES

2.1. Definiciones. Para los efectos de este Manual se establecen las definiciones siguientes:

- **TI (Tecnologías de la Información):** Se refiere al uso de equipos de telecomunicaciones y computadoras para la trasmisión, procesamiento y almacenamiento de datos. La noción abarca cuestiones propias de la informática, la electrónica y las telecomunicaciones.

- **TIC (Tecnologías de la Información y la Comunicación):** Comprende el equipo de cómputo, software y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información (datos, voz, imágenes, video y objetos informáticos en general).

- **Computación en la Nube:** La computación en la nube es un modelo que permite acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden aprovisionarse e implementarse rápidamente con un mínimo esfuerzo o servicio administrativo con interacción del proveedor.

- **Infraestructura TIC:** Consiste en el hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar la demanda de los servicios de TIC.

- **Seguridad de la información:** Capacidad de preservar la confidencialidad, integridad, autenticidad y disponibilidad de la información, así como la prevención, detección y la resolución de amenazas de una manera más ágil.

- **Servicios en la nube:** Son todos aquellos programas, herramientas, equipos de soluciones o servicios que se acceden a través de redes públicas (internet) o privadas (VPN, enlaces dedicados) los cuales incluyen, pero no se limitan a: Cómputo, Redes, Seguridad,

Almacenamiento de la información, Bases de Datos, Plataformas de aplicaciones WEB y APP´s, así como soluciones para la configuración, monitoreo y auditoría de cada uno de sus componentes.

- **Proveedor de Servicios en la Nube:** Se refiere al integrador de la plataforma de servicios de nube a través de centros de datos geográficamente separados uno de otro, siendo los propietarios y responsables del mantenimiento de los equipos conectados en red que son necesarios para dichos servicios, mediante un esquema de auto servicio a pequeñas, medianas y grandes empresas, con la característica de adaptabilidad para sumar valor a los inventarios y/o necesidades manifiestas entre el cliente y uno o más proveedores de solución.

- **Sistemas de Información:** Es un conjunto de elementos que interactúan entre sí con el propósito de lograr un fin.

- **Datos sensibles o datos personales sensibles:** Conforme lo indicado en el artículo 9 numeral 2 del Decreto 57-2008 del Congreso de la República de Guatemala, Ley de Acceso a la Información Pública: "Son aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, el origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencia o vida sexual, situación moral y familiar u otras cuestiones íntimas de similar naturaleza."

- **Información confidencial:** Conforme lo indicado en el artículo 9 numeral 5 del Decreto 57-2008 del Congreso de la República de Guatemala, Ley de Acceso a la Información Pública, "Es toda información en poder de los sujetos obligados que, por mandato constitucional, o disposición expresa de una ley tenga acceso restringido, o haya sido entregada por personas individuales o jurídicas bajo garantía de confidencialidad."

- **Información reservada:** Conforme lo indicado en el artículo 9 numeral 7 del Decreto 57-2008 del Congreso de la República de Guatemala, Ley de Acceso a la Información Pública, "Es la información pública cuyo acceso se encuentra temporalmente restringido por disposición expresa de una ley o haya sido clasificada como tal, siguiendo el procedimiento establecido en la presente ley"

- **Servicios pre reservados:** Se refiere a servicios que se definen de forma anticipada, se compromete con la reserva. Ejemplo de un servicio pre reservado es el almacenamiento.

- **SLA:** Es un contrato entre un proveedor de servicios y sus clientes que documenta qué servicios proporcionará el proveedor y define los estándares de servicio que el proveedor está obligado a cumplir.

- **NIST:** Instituto Nacional de Estándares y Tecnología (EEUU), fundado en 1901.

APARTADO III
ADMINISTRACIÓN DE LA INFORMACIÓN

3.1. Tipificación de la Información. Los organismos del Estado, entidades Autónomas y Descentralizadas, las Municipalidades y sus empresas y demás Instituciones que conforman el sector público, son los obligados a clasificar la información en datos Públicos, Confidenciales o Reservados que se van a transmitir y almacenar en la nube tomando los criterios de riesgo y seguridad de la información contenidos en las, ISO/IEC 27001, ISO/IEC27017 y ISO/IEC 27018, ISO/IEC 27701 así como los criterios de Habeas Data y de Confidencialidad que enmarca la Ley de Acceso a la Información Pública (LAIP). Estos estándares son por mencionar las referencias a considerar en el modelo de negocio que sea determinado por el comité de cada entidad.

3.2. Protección de la Información. La información deberá ser catalogada para indicar la necesidad, prioridad y grado de protección esperada para su manejo. En los casos en que la información se clasifique ya sea como Confidencial o Reservada, los organismos serán responsables de que dichos datos sean encriptados usando estándares y algoritmos aprobados por la industria.

3.3. Información Pública, Información Confidencial e Información Reservada. Todas las instituciones que utilicen el servicio de nube deben garantizar el estricto cumplimiento de lo indicado en el Decreto 57-2008 del Congreso de la República de Guatemala, Ley de Acceso a la Información Pública, Artículos 9, 22, 23, 30, 31, 32, 33, 34 y 35.

Para la información clasificada como Información Reservada, los organismos serán responsables de que dichos datos sean encriptados usando estándares y algoritmos aprobados y reconocidos como las mejores prácticas en seguridad tecnológica, vigentes en el momento de contratación.

APARTADO IV
SEGURIDAD DE TECNOLOGÍA DE LA INFORMACIÓN

4.1. Gestión de la seguridad de la información. Las instituciones de gobierno deben gestionar la seguridad de su información, con el objeto de garantizar la confidencialidad, integridad y disponibilidad de los datos; así también, deben administrar y gestionar los medios y canales adecuados que permitan transmitir y acceder de forma segura a los datos e información. De forma proactiva, realizar las acciones pertinentes para mitigar los riesgos de pérdida, extracción indebida y corrupción de la información debiendo considerar como mínimo los aspectos siguientes:

- Identificación, clasificación y protección de la información de acuerdo con criterios de sensibilidad y criticidad;
- Roles y responsabilidades para la gestión de la seguridad de la información;
- Monitoreo de la seguridad de la información y la actividad de acceso a datos en búsqueda de desviaciones;
- Seguridad lógica que incluya controles y medidas de prevención para resguardar la integridad y seguridad de los sistemas de información y de los datos, considerando:

    - Administración de los permisos de acceso de usuarios y sistemas con condiciones específicas sobre las operaciones que pueden realizar, para garantizar el acceso a los recursos. Incluyendo el registro, monitoreo continuo y retención de la actividad relacionada con estos permisos.
    - Administración de los permisos de acceso a los sistemas de información, datos y elementos de la infraestructura de TI. Incluyendo el registro, monitoreo continuo y retención de la actividad relacionada con estos permisos.
    - Monitoreo del uso de permisos para detectar actividades no autorizadas, detección de riesgos de acceso o filtraciones de datos involuntarias;
    - Bitácoras de las transacciones realizadas en los sistemas de información críticos;
    - Pruebas periódicas para detectar vulnerabilidades en la infraestructura de TI, los sistemas de Información y las bases de datos.

4.2. Continuidad operativa y recuperación del servicio. Las instituciones públicas deberán tomar siempre en cuenta las medidas previsoras para mantener de manera continua y sin interrupciones su operación y/o sus servicios, para lo cual deberán contemplar las siguientes medidas:

- Asegurar contractualmente la transición de servicios entre un proveedor y otro en los procesos de renovación de contratos y/o servicios que pueden ser: mismo proveedor otra nube; diferente proveedor misma nube; diferente proveedor diferente nube. Dicha transición debe de tomar en cuenta:

    - Transferir todas las cuentas relacionadas al servicio a la Institución o a quien la Institución designe al finalizar el contrato del servicio. En ese momento, ya sea la Institución o quien ésta designe, pasará a ser responsable por cualquier elemento técnico relacionado al servicio de nube.
    - Entiéndase como transferencia de la propiedad de la cuenta, al proceso de mover de manera administrativa su posesión, y todos los recursos asociados a ella, sin tener que incurrir en procesos de migración que pudieran impactar a la operación de las Instituciones. Es por esta razón que todos los recursos asociados deben ser creados bajo una o múltiples cuentas con recursos únicamente de la Institución para que, en caso de que requieran ser movidos en el futuro, esto pueda realizarse sin tener impacto.

APARTADO V
PROCESAMIENTO DE LA INFORMACIÓN

5.1. Procesamiento de la información. Las instituciones públicas, podrán alojar y procesar su información dentro o fuera del territorio nacional, el proveedor deberá indicar en el contrato si aplican: los gastos derivados de repatriación de datos, servicios con costos extra o violación de datos que por conservadoras no pueda estar almacenado fuera del territorio nacional, debiendo contar para el efecto con la infraestructura de TI, sistemas de información, bases de datos y personal técnico capacitado con el propósito de asegurar la disponibilidad, integridad, confidencialidad y accesibilidad de la información.

En el caso de tener todos los servicios institucionales con servicios en la nube, las entidades se deben resguardar que los mismos estén garantizados en su adecuada portabilidad, accesibilidad, y seguridad hacia los mismos, desde adecuados niveles de servicio o los que se pueden aplicar de la Norma de ISO 20000, o los estándares reconocidos con el modelo de ITIL, más algunas sugerencias como:

- Confirmar que se cuenta con un plan de continuidad, o en su caso, hay que confirmar que la información alojada en el(los) Servicio(s) de Nube está debidamente replicada (los que correspondan a esa necesidad), priorizada, y catalogada para garantizar su acceso según determine por medio de un comité de seguridad de la información de cada entidad.
- Que, por el acceso a datos en sitios alternos replicados por servicios de nube en diferentes áreas geográficas del proveedor, no incremente el costo de servicios en Guatemala. Esto dependerá de la estrategia de continuidad que se vaya a implementar en la nube y sus costos.
- Disponer de personal técnico, que conlleve una transferencia de conocimientos del proveedor hacia las entidades en territorio nacional para tener un soporte inicial apropiado al momento del registro de incidentes.
- Confirmar una arquitectura redundante con protección de datos adecuada conforme el sistema lo requiera.

5.2. Subcontratación. Cuando se contraten servicios en la nube, las instituciones serán las responsables de efectuar lo instruido como mínimo en este Manual. En los contratos que se suscriban deberán incluir, entre otros componentes lo siguiente:

- Que el proveedor resguardará la confidencialidad de las operaciones y servicios que realizare y demás información a que tenga acceso con motivo de su relación de servicios con la institución contratante;

5.3. Certificaciones de Servicios en la Nube. Las entidades de gobierno, para seleccionar a los Proveedores de Servicios en la Nube, deberán considerar a aquellos que cuenten, como mínimo, con las certificaciones siguientes: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701, Informe de controles de organización de servicios (SOC) 1, 2 y 3, y PCI DSS, o los estándares vigentes en el momento de contratación. Se deben considerar también los siguientes estándares: NIST SP 800-88: Media Sanitization, NIST 800-171 NIST 800-53, NIST CSF cuando aplique.

APARTADO VI
PROPIEDAD DE LOS DATOS, RECUPERACIÓN Y ACCESOS

6.1. Propiedad de los datos. Las instituciones públicas mantendrán el control y la propiedad total sobre sus datos, haciendo obligatorio el uso de los servicios de Identificación y Acceso que brindan los proveedores de servicios en la nube, así como los controles de acceso disponibles para restringir el acceso a la infraestructura y los datos. Los Proveedores de Servicios en la Nube deben ofrecer a las entidades públicas la opción de almacenar, administrar y proteger sus datos.

6.2. Propiedad de la información. Los contratos de servicios y otros acuerdos de nivel de servicio (SLA) relacionados con la provisión de Servicios en la Nube para agencias gubernamentales deberán estipular claramente que cualquier información migrada a la nube sigue siendo propiedad de la entidad gubernamental contratante. La institución contratante retendrá los derechos de acceso, recuperación, modificación y eliminación de datos, independientemente de la ubicación física de los servicios en la nube, incluido el derecho a aprobar, denegar y revocar el acceso de terceros, sin que esto contradiga lo establecido el ítem 7.1 del presente Manual.

6.3. Acceso a la información. El acceso, recuperación, modificación y eliminación de datos sigue siendo un derecho del organismo gubernamental contratante y se reflejará en los contratos de servicios pertinentes. Las políticas y procesos relacionados con el acceso a los datos se definirán de acuerdo con las necesidades de la entidad contratante y se especificarán en el acuerdo entre la entidad gubernamental y el proveedor de la nube o la empresa que lo represente en la República de Guatemala.

APARTADO VII
FISCALIZACIÓN DE LOS SERVICIOS EN LA NUBE

La auditoría de los servicios de nube, se debe realizar conforme al modelo de responsabilidad compartida explicada anteriormente y de acuerdo a la normativa aplicable.

Sugerencias para efectuar una fiscalización fortalecida de los servicios prestados por terceros en la nube:

7.1. Accesos para la realización de Auditorías en nube. Todas las instituciones públicas, al momento de contratar los servicios en nube, deben asegurarse de proporcionar al ente fiscalizador un usuario de sólo lectura a los auditores gubernamentales nombrados por La Contraloría General de Cuentas y las Unidades de Auditorías Internas de las entidades a los recursos relacionados con el servicio contratado por la institución; además, de proporcionar acceso a sus recursos de nube, sus sistemas de información y sus bases de datos con la única finalidad de realizar la auditoría correspondiente.

7.2. Auditoría sobre las Certificaciones. El Auditor Gubernamental debe verificar las certificaciones del proveedor de servicios en la nube, identificando que se cumple lo requerido en el numeral 5.3 y que las acreditaciones son vigentes al momento de la revisión.

7.3. Auditoría sobre Confidencialidad de la Información. El Auditor Gubernamental interno y externo de las entidades, deberá considerar como mínimo en los estándares dictados a la época los riesgos a los que está expuesta la información en los servicios contratados, para lo cual es necesario identificar lo siguiente:

- Verificar que el servicio contratado cumple con los requerimientos antes mencionados para garantizar la confidencialidad, integridad y disponibilidad de la información de acuerdo con su grado de criticidad, así como el cumplimiento de los contratos establecidos en las SLA.

- Efectuar una revisión de los dominios siguientes:
    - La arquitectura de la nube y los servicios contratados, así como, en caso de existir, que el proveedor local elegido esté certificado por el proveedor de Nube para proveer el servicio.
    - Acceso a servicios desde diferentes equipos móviles.
    - El cumplimiento de los SLA provistos y la respuesta de soporte contratado.
    - Operación de la nube, cifrado y manejo de llaves de cifrado.
    - Manejo de Identidad y acceso a los servicios contratados.

APARTADO VIII
RECOMENDACIONES DE SEGURIDAD

Las siguientes son las recomendaciones mínimas de seguridad que las instituciones deberán de llevar a cabo al momento de usar servicios de nube pública:

- Habilitar el uso de múltiples factores de autenticación para todas las cuentas, ya que esto añade una capa adicional de seguridad a las cuentas. En lugar de simplemente introducir una contraseña, la autenticación de dos factores requiere un segundo factor de autenticación, como un código enviado al teléfono móvil;

- Usar cuentas de usuario separadas con acceso restringido para las tareas del día a día, reservando el acceso raíz (usuarios administradores) para tareas administrativas específicas que lo requieran. Además, es importante limitar la cantidad de usuarios que tienen acceso a la cuenta raíz e implementar otras medidas de seguridad, como contraseñas seguras y autenticación de dos factores, ya que cualquier acceso no autorizado a la cuenta raíz puede resultar en un control total del sistema;

- Utilizar los registros de auditoría que ofrecen los proveedores de nube para poder investigar incidentes, configurándolos para retener los registros por el tiempo que establezca el ente fiscalizador en su normativa;

- Mantener actualizados los datos de contacto de seguridad para que las diferentes áreas de la institución sepan a quién contactar;

- Configurar alarmas de facturación o consumo de los servicios de nube (“billing”) para identificar actividad inusual en su cuenta, como potenciales ataques relacionados a minería de bitcoins o despliegue de instancias para formar parte de redes de robots, entre otros.

- Revisar continuamente todos los roles para asegurarse que solo se otorguen los privilegios mínimos necesarios, para limitar el campo de acción en caso de compromiso;

- Automatizar controles de buenas prácticas y centralizar hallazgos de seguridad;
- Contratar servicios de Web Application Firewall para proteger los servicios y aplicaciones contra los ataques más críticos y frecuentes (OWASP Top 10), así como bloquear IPs de mala reputación (como las IPs de las Botnets e IPs de atacantes);
- Otorgar siempre los permisos mínimos necesarios en los Security Groups (principio de mínimo privilegio); y
- Definir activamente dónde almacenar sus datos sensibles y verifique que no se encuentren datos sensibles expuestos públicamente o compartidos con cuentas desconocidas.

APARTADO IX
DISEÑO DE ARQUITECTURA EN LA NUBE

En esta sección, se describe un modelo de diseño de la arquitectura de implementación de la nube y usar las capacidades de este servicio para mejorar la solidez del servicio y usar mejor la nube. Además, esta sección ayuda a los usuarios a desarrollar la capacidad de migrar servicios tradicionales a la nube. La arquitectura del sistema de servicio no se considera en el ámbito de la cloudificación.[1] La arquitectura debe ser diseñada por el proveedor del sistema de servicio.

9.1. Método de diseño jerárquico. Basándose en las características funcionales de cada componente, el sistema de servicio se puede dividir en tres capas: capa de acceso, capa de aplicación y capa de datos.

Cuadro 1. Estándar de capas de servicio

CAPA LÓGICA	DESCRIPCIÓN DE LA FUNCIÓN
Capa de acceso	Acepta la entrada de datos de los usuarios y presenta datos a los usuarios, recibe solicitudes de invocación externas y devuelve los resultados de invocación, e interactúa con la capa de aplicación.
Capa de aplicación	Controla los flujos de trabajo e implementa la lógica de servicio. La capa superior procesa la solicitud desde la capa de acceso y devuelve el resultado de la solicitud. Se conecta a la capa de datos para agregar, eliminar, modificar y consultar datos.
Capa de datos	Datos de servicio del sistema persistentes, como bases de datos, sistemas de archivos y caché distribuida, y proporciona soporte de datos para la implementación de lógica de servicio de capa superior.

Elaboración propia.

1 "Ámbito de Cloudificación" se puede definir como: El proceso de migrar servicios, aplicaciones y datos de sistemas locales e infraestructuras tradicionales hacia entornos basados en la nube.

9.2 Diseño de arquitectura de implementación: Se describe la idea del diseño de arquitectura de la aplicación en capas y proporciona la arquitectura recomendada para cada capa que se va a migrar a la nube. La combinación de varias capas forma una arquitectura de implementación de servicio completa. En el despliegue real del servicio, varias capas pueden desplegarse juntas debido a factores tales como la escala del servicio y el volumen de acceso. Por lo tanto, se introducen tres arquitecturas de implementación.

Cuadro 2. Arquitecturas de implementación comunes

ARQUITECTURA DE IMPLEMENTACIÓN	CARACTERÍSTICAS DE LA ARQUITECTURA	ESCENARIO DE LA APLICACIÓN
Arquitectura de implementación de capa 1	1. Despliegue convergente de la capa de acceso, la capa de aplicación y la capa de datos	1. Volumen de servicio en pequeña escala (usuarios diseñados < 500)
Arquitectura general de dos capas	1. La capa de acceso y la capa de aplicación se despliegan juntas, y la capa de datos se despliega de forma independiente.	1. Volumen de servicio de escala media (500 < Usuarios diseñados < 3000)
Arquitectura compleja de tres capas	1. Despliegue separado en la capa de acceso y la capa de aplicación 2. La capa de acceso admite múltiples modos de acceso. 3. Equilibrio de carga de dos niveles: El equilibrio de carga se implementa en la capa de acceso y la capa de aplicación. 4. Los componentes de seguridad se despliegan en la capa de acceso.	1. Generalmente dirigido a los consumidores finales. 2. El número de usuarios diseñados es más de 3000. 3. Arquitectura de abastecimiento general para los sistemas de servicios básicos.

Elaboración propia.

APARTADO X
DISEÑO DE SEGURIDAD DE MIGRACIÓN A LA NUBE

10.1. Cumplimiento de seguridad

El diseño de seguridad, se basa en los estándares de seguridad de la industria. Por un lado, se puede aprender de la mejor experiencia de pensamiento en la industria en la construcción de sistemas de seguridad, con el fin de evitar el riesgo de falta de integridad y falta de integridad en el diseño general de la solución. Por otro lado, se puede cumplir con los requisitos impulsores del cumplimiento de la seguridad, especialmente el cumplimiento de la protección gradual, para el diseño y la planificación de proyectos de seguridad en escenarios gubernamentales.

10.2. Riesgos de seguridad controlables

La mejor práctica para la construcción de sistemas de seguridad, es identificar amenazas de seguridad específicas, analizar los riesgos potenciales y tomar las medidas adecuadas para reducir los riesgos generales a un nivel aceptable.

En términos de seguridad en la nube, es necesario equilibrar la relación entre seguridad, eficiencia y costos. Se deben utilizar las mejores medidas de seguridad, para garantizar que la red en producción pueda responder a las amenazas de seguridad, maximizar la eficiencia de la seguridad y racionalizar los costos de seguridad.

10.3. Responsabilidades de seguridad claras

La nube debe seguir estrictamente los principios de “quién está a cargo, quién es responsable de la construcción y quién es responsable de usar” y “las responsabilidades de gestión de la seguridad, la propiedad de los datos. La nube implementa un sistema jerárquico de gestión de seguridad y cumple con las responsabilidades de gestión de seguridad de todas las partes. La unidad de usuario de recursos en la nube, es responsable de la seguridad del sistema en la nube y de los datos de servicio.

10.4. Planificación general y construcción paso a paso

Integre el sistema de garantía de seguridad en el proceso de planificación, construcción, operación y mantenimiento de la nube. El objetivo de la construcción, es garantizar que la construcción de seguridad de la plataforma en la nube cumpla con los requisitos básicos de protección y proporcionar orientación de seguridad y normas para la cloudificación de los servicios de comisiones, departamentos y oficinas. En el período posterior, con la migración gradual y la integración de más sistemas de aplicación, el sistema de garantía de la seguridad se mejorará gradualmente de acuerdo con el marco de seguridad y el plan general.

REFERENCIAS

AWS. (n.d.). Amazon Web Services (AWS). Retrieved from https://aws.amazon.com/es/what-is-cloud-computing/

Azure. (n.d.). Microsoft. Retrieved from https://azure.microsoft.com/es-mx/resources/cloud-computing-dictionary/what-is-cloud-computing

Google. (n.d.). cloud.google.com. Retrieved from https://cloud.google.com/learn/what-is-cloud-computing?hl=es-419

Harvey, S. (2018, abril 17). KirkpatrickPrice. Retrieved from https://kirkpatrickprice.com/blog/whos-responsible-cloud-security/

Mell, P., & Grance, T. (2011, 9). National Institute of Standars and Tecnology. Retrieved from NIST: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

GOBIERNO *de* GUATEMALA
DR. ALEJANDRO GIAMMATTEI

COMISIÓN PRESIDENCIAL
DE GOBIERNO ABIERTO
Y ELECTRÓNICO

4ta. Calle 6-17 zona 1
Guatemala, Guatemala

(502) 2220-5383

www.transparencia.gob.gt