PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TRABAJO DE TITULACIÓN DE GRADO

ANÁLISIS DE PROBLEMAS TÉCNICOS Y LEGALES DE CIBERSEGURIDAD Y SUS POSIBLES SOLUCIONES EN EL CONTEXTO DE LA COMPUTACIÓN EN LA NUBE.

ANDREA ULLOA HALLO

Quito, diciembre 2021

Tabla de contenido

Índice de gráficos

Índice de tablas

1. Capítulo 1: Ciberseguridad

1.1. Generalidades

Desde hace varios años se vive en una era de revolución en donde, gracias a la tecnología, se experimenta grandes cambios en la estructura de nuestra sociedad, uno de estos cambios, y el cual generó un gran impacto en la forma de vida de la humanidad es el internet, una herramienta muy poderosa que significó una transformación global y que dio pasó a lo que hoy se conoce como la era digital, en la cual los datos y la información son las herramientas más poderosas.

Tal es así, que en los últimos años el uso de servicios de internet en sus diferentes plataformas ha aumentado considerablemente, y como se evidencia en la actualidad, este entorno dio un giro, incluyendo al crecimiento exponencial de la economía digital, pues los servicios en línea significaron que muchas empresas podían ofrecer servicios sin la necesidad de que los clientes tengan que acudir físicamente, sin embargo, por maravilloso que suene todo esto lo cierto es que también dejó la puerta abierta para un nuevo problema, la seguridad en línea. Una de las medidas de seguridad es el uso de contraseñas, mismas que en varias ocasiones han sido usurpadas y han dado lugar al robo de dinero o suplantación de la identidad de usuarios, entre otras, tanto usuarios como empresas son cada vez más conscientes de esta problemática, en un ambiente donde gran parte de la sociedad considera que la manera tradicional que se tenía para cubrir la seguridad en línea podría ya no ser suficiente.

Si bien los usuarios muestran cierta conciencia y preocupación a los ataques informáticos, pueden tener una idea equivocada de los mismos, por ejemplo, muchos usuarios suelen creer que no poseen ninguna información valiosa y por ende eso los permite de ser blanco de potenciales atacantes informáticos, sin embargo, lo cierto es que, de alguna manera, todos somos vulnerables, pues los atacantes tiene interés en todo tipo de información como listas de contactos, robo de información, pedido de rescates por bloquear un ordenador y solicitar una suma de dinero a cambio de recuperar la información del mismo.

Ante estas amenazas, surge la Ciberseguridad que, dentro del contexto de la tecnología, puede ser definida como un proceso que abarca la prevención, detección, respuesta y que, a su vez debe implicar el aprendizaje como una característica de mejora continua, estos términos se explican mejor de la siguiente manera (Telefónica, 2016):

1. *Prevención*: se recomienda que tanto usuarios como empresas tengan ciertos conocimientos de seguridad a fin de poder darle un uso eficiente y óptimo a los recursos disponibles. Adicionalmente, se deben usar ciertas medidas básicas como son la protección física de instalaciones a fin de evitar en lo posible que alguien sin autorización tenga acceso a esta información. La prevención incluye los siguientes puntos clave (Montoya S. & Restrepo R., 2012):
    a. Control de accesos: va de la mano con la gestión de identidades, puesto que una cierta identidad o rol tiene el acceso a ciertos recursos o datos en una organización. Uno de los principales problemas de este apartado es saber definir bien las acciones que cada usuario puede hacer y bajo qué circunstancias. El control de accesos cuenta con los siguientes componentes principales:
        i. Meta-directorios: servicio que permite la recolección y almacenamiento de información.
        ii. Directorios virtuales: similares a los anteriores con la diferencia de que no trabajan con agentes por lo que son más flexibles.
        iii. Gestión de identidades: permite la creación y manejo de entidades con sus respectivos atributos.
        iv. Gestión de roles: se encargan de tramitar los respectivos roles de los usuarios involucrados en una organización.
        v. Tokens: se refieren a la autenticación de usuarios mediante el uso de contraseñas.
    b. Fugas de datos: es una de las mayores amenazas que tanto usuarios como organizaciones deben afrontar, así como uno de las más complicadas, por lo mismo es abordada desde varios enfoques técnicos (controles de acceso, de contenido, entre otros), de carácter

organizativo (Ej.: políticas de seguridad) y legal (como lo son las políticas de confidencialidad).

c. Seguridad de la red: todas las acciones cuyo objetivo es proteger recursos de acceso en la red y sus respectivos sistemas. Al abarcar un amplio rango de amenazas, es un punto clave dentro de la prevención. En este sentido, es una estructura de capas y bajo esa lógica, lo ideal es contar con varias capas de forma que si una falla, la siguiente sea capaz de actuar. Para ello, se requiere de medidas en los niveles de hardware y software, este último necesita de constantes actualizaciones y debe estar relacionado a una política de seguridad.

2. *Detección*: se puede dar en tiempo real, usualmente debido a la intervención de un algún software, o bien pasado un tiempo desde el ataque, siendo la segunda una problemática mayor puesto les da a los atacantes un intervalo donde pueden actuar libremente. Si bien las herramientas actuales son capaces de detectar ciertas amenazas en base a ciertos patrones conocidos, el problema radica en aquellas que trabajan con patrones desconocidos. Es por ello, que se ha convertido en la base de nuevas estrategias donde varios ataques se produzcan en cualquier momento (Packard , 2015).

   Para abordar este aspecto, ENISA ha determinado que se debe trabajar la gestión de vulnerabilidades siguiendo el siguiente ciclo: el escaneo de estas, seguido de una definición acciones que podrían darles solución y, por último, la implementación de dichas soluciones.

3. *Respuesta*: en caso de que un ataque informático sea efectivo, se debe contar con un plan de respuesta, tanto desde una perspectiva técnica como legal.

   El CREST (Creasey, 2015) considera ciertas medidas desde el punto de vista técnico; desconectar el equipo de internet, puesto que esto podría impedir que el virus infectante se siga propagando por la red, instalar antivirus y, en caso de ya contar con uno, se recomienda descargar y actualizar su base de firmas a fin de conseguir un análisis más eficiente. Adicionalmente, se sugiere una modificación de todas las contraseñas para evitar posibles robos de identidad, y en caso de ser necesario se debe realizar una limpieza manual.

   Con respecto a las medidas legales, se debe comenzar por denunciar el ataque informático, a partir de aquí las acciones pueden variar dependiendo de las

leyes de cada país. El manejo de estas situaciones en el Ecuador se abordará más profundamente en posteriores capítulos.

Finalmente, la fase de respuesta cubre dos puntos importantes: el primero se trata de los sistemas de recuperación (permiten al equipo volver al punto el que se haya encontrado antes de un problema), el segundo son las evidencias digitales (cualquier dato o registro que sirva como prueba en un proceso legal).

4. *Aprendizaje*: esta fase es un poco difícil de analizar pues se trabaja con amenazas dinámicas, lo que requiere de una constante revisión y actualización de software, proceso que necesita de tiempo y dinero, y, por ende, de la participación de usuarios, así como de la intervención de entidades y Estados (Franklin, 2015). A pesar de ello, las nuevas tecnologías hacen lo posible por lograr que se dé este proceso y que sea lo más eficiente posible.

La ciberseguridad se resume en la práctica de defender servidores, sistemas, redes y datos de ataques maliciosos. Se trata de un término demasiado general y que puede aplicarse en diferentes contextos, siendo quizás algunos de los más destacados la seguridad de res, de aplicaciones, de la información entre muchos otros. Es por ello, que su definición se verá limitada únicamente a la temática principal del trabajo.

1.2. La Ciberseguridad en el Cloud Computing

Si bien la Nube es una tecnología atractiva para usuarios independientes, así como empresas u organizaciones debido a sus servicios de almacenamiento, su seguridad representa aún una barrera a vencer y algo que ciertamente esta tecnología aún no ha podido controlar.

Uno de los puntos más críticos es la pérdida de control en infraestructuras, pues el cliente cede cierto control al proveedor de la nube, exponiéndose así a una posible vulnerabilidad, además, los acuerdos de niveles de servicio no garantizan un compromiso del proveedor de la Nube de que vaya a prestar dichos servicios. (Mackay, Baker, & Al-Yasiri, 2012). Actualmente esto es un problema aún mayor gracias a la evolución que ha tenido esta tecnología, es posible que la Nube se encuentre disponible para prácticamente cualquier empresa y que estas busquen sacar

la mayor rentabilidad que estos servicios ofrecen lo que en consecuencia hace que sean objetivo directo de cada vez más ataques cibernéticos.

Partiendo de uno de los puntos más importantes, es decir los datos y su seguridad, las empresas encargadas de almacenar la información de varias organizaciones o usuarios buscan ser tan seguras como sea posible, para ello los proveedores de estos servicios garantizan hacer más supervisiones de las debidas, mismas que se hacen con controles independientes a fin garantizar la protección de la información. (Westmonroe, 2016)

Sin embargo, es imposible afirmar que alguna medida será 100% efectiva, es más acertado decir que la gestión profesional en la gestión de servicios de Cloud Computing, misma que ha sido reforzada a partir de la experiencia, ofrece una considerable seguridad.

Aunque todo suene muy prometedor el problema va más allá de eso, pues los ataques virtuales tienen un abanico de variedades por lo que la ciberseguridad de la Nube es mucho más compleja que solo garantizar la seguridad de los datos, y además la información no siempre es tan privada como uno piensa; es sorprendente la cantidad de información personal que uno voluntariamente publica sin darse cuenta de lo fácil que se expone en Internet (Kosinski, Stillwell, & Graepel, 2013).

Lograr algo realmente efectivo requiere de un conjunto de factores donde destacan las acciones de los usuarios, pues no importa que tan prometedoras sean las medidas de seguridad ofrecidas por estos servicios si los usuarios no hacen un uso apropiado de las mismas no hay garantía de que no sean el blanco para futuros ataques cibernéticos. A partir de este enfoque lo primero es entender que es exactamente el Cloud Computing y el uso que se le dará.

2. Capítulo 2: Computación en la nube

2.1. Definición y características

La computación en la nube es un concepto muy difundido y estudiado en los últimos años, que se define como: “un modelo para permitir el acceso ubicuo, conveniente y bajo demanda a un conjunto compartido de recursos de red configurables, que pueden ser provistos rápidamente y liberados con un mínimo esfuerzo de administración e interacción con el proveedor del servicio” (Mell & Grance, 2011).

Al ser este concepto algo muy general es útil apoyarse en otras organizaciones como la CSA -Cloud Security Alliance-, la cual define al Cloud Computing como: “un modelo a la carta para la asignación y el consumo de computación, a través de la cual se puede utilizar una serie de servicios, aplicaciones, información e infraestructura compuesta por reservas de recursos de computación, redes, información y almacenamiento”, p.13 (Brunette & Mogull, 2009).

A partir de esas definiciones se puede sintetizar que el Cloud Computing, más popularmente conocido como Nube, es el uso de servicios tecnológicos en lugares remotos a los que se acceden mediante una red de telecomunicaciones, es decir un medio para suministrar servicios a través de Internet.

Estos servicios le permiten al cliente (ya sea un individuo o empresa), tener acceso a un conjunto de recursos compartidos y control de estos. Dichos recursos pueden ser: redes, servidores o aplicaciones, y su disponibilidad depende directamente de la demanda existente. En pocas palabras, el atractivo principal de estos servicios su flexibilidad de acceso y dimensionamiento.

Actualmente son muchas las empresas que hacen uso de estos servicios o que han sido pioneras en el uso de estos, tales como Google o Amazon. Todos estos proveedores trabajan con una estrategia común, la cual se resume en presentar todas las ventajas de trabajar con Cloud Computing, en ocasiones llegando al extremo de idealizarlas de esta forma logran atraer a potenciales consumidores y ganar clientes con una campaña publicitaria que no es realmente costosa (Wentao, 2012).

En Cloud Computing, también se debe considerar la red de comunicaciones de usuarios, misma que debe contar con una serie de características esenciales, soportar aplicaciones, contar con un gran ancho de banda, baja latencia, ser segura, poseer simetría, entre otras que le permitan a esta red ser la mejor aliada de servicios en Cloud Computing.

Desde hace algunos años, Cloud Computing se ha convertido en un instrumento de uso diario y a su vez continuará transformando la forma en las que usuarios individuales y empresariales, hacen uso de esta.

Este servicio es el resultado de varios avances tecnológicos como lo son capacidades de almacenamiento, cálculo y procesamiento, velocidad de transferencia, provecho de la extensión y, por ende, el abaratamiento del acceso Internet, siendo así un servicio que no se limita exclusivamente al comercio, sino que cuenta con el acceso a centros de datos y proceso desde cualquier lugar. De forma simple, se dice que el Cloud Computing cuenta con cinco características esenciales (Primorac, 2014):

1. *Autoservicio bajo demanda*: el consumidor puede proveerse de los recursos que necesite (almacenamiento en red o tiempo de servidor, por ejemplo) sin interactuar directamente con su proveedor, esto reduce mucha de las dificultades que usualmente hay al adquirir recursos IT de manera tradicional.
2. *Acceso amplio a la red:* se refiere a la disponibilidad de la red y sus servicios a través del uso de diferentes plataformas, como son las portátiles, dispositivos móviles, PDA (Personal Digital Assistant), entre otros. Es el acceso a recursos de forma a independiente de aspectos externos como la ubicación geográfica.
3. *Agrupamiento de recursos*: actualmente los diferentes recursos disponibles se encuentran agrupados siguiendo un modelo multi-distribuido, donde diferentes consumidores tendrán acceso a esos servicios. Como resultado, los proveedores minimizan costos y maximizan la disponibilidad al compartir recursos con varios consumidores.
4. *Elasticidad rápida*: sus funcionalidades y servicios pueden adquirirse en cualquier momento o cantidad, permitiendo un gran ahorro de costos.
5. *Servicio medido*: el uso de recursos en la nube es contralado, monitorizado y optimizado de forma automática, lo cual representa una ventaja para el consumidor.

Además de estas características, también se debe mencionar su infraestructura y funcionamiento, específicamente en sus respectivos niveles de servicios. Como indica el NIST, el Cloud Computing puede funcionar en los siguientes modelos de despliegue:

1. *Nube Pública*: tanto la infraestructura como sus recursos se encuentran disponibles para el público general mediante una red pública, en estos casos se habla de un proveedor que mezcla la infraestructura, es decir, los clientes deberán compartir el espacio disponible con otros usuarios. Un ejemplo de esto es Microsoft Windows Azure.
2. *Nube Privada*: se trata de permitir el acceso a una sola organización donde la administración de servicios es dada por un proveedor o bien por la misma empresa. Este tipo de nubes también se llama In-Situ, y su ventaja principal es ofrecer a las empresas el dominio total de estos servicios garantizando así mayor seguridad de la información, con la desventaja de la ampliación de recursos.
3. *Nube Híbrida*: uno de los modelos más usados y se trata de una fusión de los dos anteriormente mencionados, ofreciendo la ventaja de que las empresas pueden ser dueños de una pare de estos servicios y a su vez comando con los servicios ofrecidos en la Nube pública.
4. *Nube Comunitaria*: se usa dentro de una comunidad exclusiva, un grupo de consumidores con un interés común. Esta comunidad puede ser administrada por totas las organizaciones involucradas en la misma, por un grupo pequeño de estas o bien por un tercero ajeno a la misma.

2.2. Niveles de servicio

El Cloud Computing se caracteriza por sus servicios específicos, mismos que se dividen en tres niveles diferentes (Primorac, 2014):

1. SaaS (Software as a Service): brinda un despliegue de software, específicamente da la capacidad de usar las aplicaciones de software propietarias del proveedor que son ofrecidas como servicios. El cliente no controla la infraestructura subyacente en la nube a excepción de ciertas opciones de configuración particulares del usuario.

En este nivel, todos los recursos son propiedad del proveedor por lo que se evita la implantación de software o hardware, así como la realización de procesos de mantenimiento o actualización por parte del cliente. Toda la seguridad se encuentra controlada por el proveedor de servicios.

Una de las diferencias principales de este tipo de servicios es que su costo se da en base a su demanda y no según su cantidad de usuarios. Estos servicios se caracterizan por ser accesibles a través del Internet, ofreciendo así mayor flexibilidad al librar a los usuarios de una dependencia física. Ejemplos de este nivel son: aplicaciones de almacenamiento, servicios de correo electrónico, aplicaciones para compartir ficheros o como gestores de contenido multimedia, entre otras. Por norma general este tipo de aplicaciones son gratuitas a nivel personal, pero tienen un costo adicional si se las usa de a nivel empresarial.

2. PaaS (Platform as a Service): ofrece un conjunto de herramientas para el desarrollo de software y aplicaciones web de forma que el cliente puede realizar el despliegue de sus aplicaciones. En este modelo, el usuario no gestiona la infraestructura, sin embargo, cuenta con un total dominio de las aplicaciones de esta.

   Este servicio les permite a los desarrolladores de software, fácil accesibilidad a la creación de aplicaciones a través de Internet, independientemente de la ubicación geográfica. Algunos de los ejemplos más sobresalientes incluyen: Azure de Microsoft o Google App Engine, siendo este último el más destacado debido a su extensa infraestructura.

3. IaaS (Infrastructure as a Service): proporciona capacidades de procesamiento, almacenamiento, redes y otros recursos que permiten el ensanchamiento y ejecución de software arbitrario, permitiendo así el control del consumidor sobre aplicaciones instaladas, OSs, almacenamiento y cierto control en algunos componentes de red, más específicamente, los servicios que esta infraestructura soporta incluyen bases de datos, servidores de aplicaciones y ambientes para el desarrollo de las mismas, servicios de streaming entre otros. Su ventaja principal es que el cliente como tal no adquiere estos recursos, sino que accede a los mismos mediante la virtualización. El proveedor ofrece directamente el despliegue de máquinas virtuales, siendo así el responsable total de la infraestructura, y el cliente pasa a estar a cargo de las aplicaciones

que desee adquirir pasando a ser el responsable de sus sistemas y de la seguridad de sus datos.

Amazon Web Services, vendría a ser un ejemplo de proveedor de IaaS, y, por otra parte, al mencionar un ejemplo de clientes que trabajan con este tipo servicios es la Escuela Médica de Harvard.

El uso de estos niveles de servicio ha tenido un crecimiento exponencial en los últimos años, al punto de mostrar una tasa de crecimiento anual compuesto, (CARG por sus siglas en inglés) entre los años 2015 y 2020, tal como se puede ver en la gráfica proporcionada por el Índice Global de Cisco, específicamente el nivel SaaS ha presentado un incremento notablemente superior:

Gráfico 1: Niveles de crecimiento del Mercado Cloud Computing

Fuente: Cisco Global Cloud Index (Cisco, 2016)

A continuación, se presenta una esquematización de ejemplos de plataformas:

Gráfico 2 Esquema de servicios en Cloud Computing

SaaS	PaaS	IaaS
•Correo electrónico •Redes sociales •Recursos humanos •Administración de documentos •Gestión de Relación con el Cliente (CRM) •Finanzas, ventas y cobranzas	•Bases de datos •Implementación de aplicaciones •Fases de integración, desarrollo y pruebas	•Administración de servicios •Almacenamiento •CDN (Content Delivery Network) •Backup y recuperación

Fuente: Autor, en base a las definiciones de Primorac

Los servicios de Cloud Computing se enfocan en un gran abanico de clientes, desde usuarios particulares a clientes corporativos gubernamentales, entre muchos otros. Todos ellos considerarán ciertas preguntas básicas relacionadas con la adquisición de servicios, tales como: ¿Cómo se garantiza la privacidad de datos?, ¿quiénes tienen acceso a la información?, ¿el proveedor cuenta con algún respaldo?, ¿en caso de algún ataque, hay algún tipo de plan de respaldo?, entre muchas otras, y como se evidencia la gran mayoría de ellas estarán relacionadas a la privacidad y confidencialidad de datos, a la integridad de su información.

En este sentido, la seguridad de la Nube debe especificar con que modelo está trabajando para contar con un plan de seguridad acorde a sus necesidades y prioridades.

ENISA elaboró una tabla guía referente a las responsabilidades cliente-proveedor en los diferentes modelos existentes:

Tabla 1 Delegación de responsabilidades cliente-proveedor según ENISA

SaaS	
Cliente	Proveedor
• Cumplir con la legislación de datos recogidos y procesados de los clientes. • Sistema de gestión de identidades. • Gestión de la plataforma de autenticación.	• Soporte de la infraestructura. • Seguridad y disponibilidad de la infraestructura física. • Gestión de parches en sistemas operativos. • Configuración de la plataforma de seguridad. • Sistemas de monitoreo. • Mantenimiento de la seguridad (firewall, antivirus, etc.) • Monitoreo de logs (registros)
PaaS	
Cliente	Proveedor
• Manejo y mantenimiento del sistema de gestión de identidades.	• Soporte de la infraestructura. • Seguridad y disponibilidad de la infraestructura física.

• Administración de la plataforma de autenticación.	• Gestión de parches en sistemas operativos. • Configuración de la plataforma de seguridad. • Sistemas de monitoreo. • Mantenimiento de la seguridad (firewall, antivirus, etc.) • Monitoreo de logs (registros)
IaaS	
Cliente	Proveedor
• Manejo y mantenimiento del sistema de gestión de identidades. • Administración de la plataforma de autenticación. • Gestión de parches en el Sistema Operativo huésped. • Configuración de la plataforma de seguridad huésped. • Monitoreo del sistema huésped • Mantenimiento de la plataforma de seguridad (firewall, antivirus, etc.) • Monitoreo de logs (registros) • Sistemas de monitoreo	• Soporte de la infraestructura. • Seguridad y disponibilidad de la infraestructura física. • Gestión de parches en sistemas operativos.

Fuente: Autor, basado en datos de la ENISA

2.3. Ventajas y desventajas

2.3.1. Ventajas

El trabajar con Cloud Computing les ofrece a sus usuarios varias ventajas de carácter técnico o social.

Se incluyen como ventajas técnicas lo siguiente (Carroll, 2011):

1. Trabajar con virtualización.
2. Alta capacidad de disponibilidad, integridad de datos y garantía de confiabilidad por parte del proveedor al usuario.
3. Soporte disponible en cualquier momento para cualquier problema posible que se presente en los servicios centrados.
4. Capacidad contratada en base a demanda.
5. Cuenta con herramientas y profesionales que se encargan de bridar seguridad a la información y sistemas del cliente.
6. El usuario contará con un respaldo de su información, puesto que su proveedor crea réplicas de datos críticos y a su vez, actualizará los sistemas de respaldo (backup).
7. La infraestructura con la que se maneja el Cloud Computing elimina las limitaciones de provisión, porque la información de los usuarios pasa a almacenarse en plataformas de alta disponibilidad administradas por el proveedor de estos servicios.

Por otro lado, las ventajas sociales y económicas del Cloud Computing se describen de la siguiente manera (Sepúlveda, Salcedo, & Gómez, 2012):

1. Optimización de recursos físicos, humanos y monetarios.
2. Los servidores de estos servicios garantizan la implementación de sistemas de bajo riesgo y mejora continua de los mismos para todos sus clientes.
3. Optimiza el tiempo de implementación de sistemas, siendo esta una de las ventajas más apreciadas.
4. Representa una gran oportunidad económica, puesto que se trata de servicios muy útiles para las empresas sin la necesidad de recurrir a altos capitales de inversión.
5. Se paga únicamente por los servicios y recursos utilizados y a su vez, representa un gran ahorro en gastos adicionales (como licencias y todo lo relacionado a estas).
6. Ofrece gestión y asesoría por parte de profesionales, representando un gran ahorro de datos, ya que las empresas no se ven en la necesidad de contratar especialistas en estos sistemas.

7. Al manejarse en gran parte por la virtualización, también fomenta y refuerza el teletrabajo dándole así a los usuarios facilidades y comodidades.

2.3.2. Desventajas

Estos servicios también cuentan con algunas desventajas que no deberían ser tomadas a la ligera y se resumen en lo siguiente (Clemons & Chen, 2011):

1. El ancho de banda, si bien el internet es la base de los servicios Cloud, también demandan que el usuario o empresa cliente implemente ciertas políticas en este servicio a fin de evitar posibles cuellos de botella.
2. Posible desconfianza por parte de clientes es imposible negar que un grupo de usuarios no son propensos a aceptar la idea de que su información personal esté en manos de un tercero.
3. Posibles falencias en los equipos de almacenamiento, pese a los avances de la tecnología, aun hoy en día no existe equipo que sea 100% seguro e infalible.
4. Falta de control de servidores por parte de los usuarios, estos equipos no están ubicados en un solo lugar, sino que se trabaja con varios intermediarios, por lo que se da la posibilidad de problemas o debilidades en el tiempo de respuesta del servicio.
5. Dependencia del usuario a su proveedor durante la contratación de estos servicios.
6. Al cambiar de proveedor, la migración de datos podría ser crítica por el riesgo que se manejaría.
7. Por último, el riesgo más alto está en los datos que se decida almacenar en estos servicios, pues al editar en manos de un tercero y en un medio relativamente vulnerable como lo es el internet, se corre el riesgo de invasión de la privacidad.

3. Capítulo 3: Seguridad en Cloud Computing

3.1. Descripción general

El Cloud Computing se ha convertido en una herramienta diaria, utilizada por miles de usuarios, incluyendo tanto individuos como empresas, sin embargo, tras todo su crecimiento y potencial, surge una interrogante, ¿Por qué ciertas personas o compañías pueden llegar a mostrar cierta resistencia a este tipo de servicios? En concepto es algo sencillo, la privacidad. No hay bien más valioso que la seguridad de la información, más aún si se trata de una organización, lo que explicaría un riesgo al confiársela a terceros que no garantizan seguridad e integridad total de los mismos.

Los usuarios o potenciales clientes pueden tener ciertas dudas o inseguridades respecto a los servicios de la Nube, mismas que casi siempre se relacionan con asuntos de seguridad y privacidad, por ello es necesario que los proveedores de estos servicios puedan garantizar de alguna forma que se está trabajando con altas medidas de seguridad y con planes de respuesta apropiados a posibles ataques. El Cloud Computing no tiene un tipo de cliente especifico, más bien abarca una variedad de usuarios, empresariales e incluso gubernamentales. Por ende, los proveedores deben ganarse la confianza de todos estos usuarios, una forma de hacerlo consiste en la firma de contratos SLA (Service Level Agreement), los cuales se traducen como Acuerdo de Nivel de Servicio que cubren posibles riesgos, especificando parámetros para garantizar seguridad en todos los niveles de servicios.

Las generalidades en seguridad del Cloud Computing cubren los siguientes puntos clave: seguridad física/lógica, e implicaciones legales técnicas y políticas. Existen múltiples estudios en cada una de estas áreas y a nivel mundial se han formado diferentes organizaciones que trabajan en investigaciones dentro de este campo, a continuación, se presentan ciertas iniciativas más reconocidas:

1. CSA (Cloud Security Alliance): es una organización europea cuyo objetivo es promover las buenas prácticas en el uso de Cloud Computing y su seguridad, sus actividades también incluyen fomentar campañas referentes al tema.

Algunos de sus artículos más relevantes incluyen las amenazas más importantes en el ámbito de Cloud Computing a fin de ayudar a los usuarios de sus servicios, especialmente a empresas y organizaciones, a identificarlos y a eliminarlos. La CSA también incluye guía de prácticas que cuentan con varias recomendaciones para tener en cuenta en el caso de adquirir servicios de la Nube.

2. ENISA (Agencia Europea de Seguridad de las Redes y de la Información): esta organización surge en el 2004 con el objetivo de mejorar la prevención y gestión de problemas de redes a través del conocimiento de una comunidad selecta y de especialistas.

   ENISA cumple constantemente con la labor de informar a la comunidad general y empresarial acerca del área de redes y todas sus componentes involucradas. Dentro del contexto de Cloud Computing se ha puesto especial atención al ser un área de crecimiento y popularidad exponencial, pero de carácter preocupante debido a sus vulnerabilidades.

   Su artículo más destacado fue publicado en 2009 y se titula “Beneficios, riesgos y recomendaciones para la Seguridad de la Información” y es una recopilación de riesgos técnicos y legales, así como de medidas a tomar contra los mismos.

3. NIST (Instituto Nacional de Normas y Tecnología): es una organización del Departamento de Comercio de los Estados Unidos cuyo objetivo es la innovación de tecnología para el mejoramiento de la vida en diferentes áreas como la nanotecnología o biotecnología.

   NIST incorporó en el 2010 un programa enfocado al Cloud Computing con la finalidad de poder incorporarlo en los sistemas del gobierno, para ello dividió su programa en cinco grupos: (Cloud Computing Target Business Use Cases, Cloud Computing Reference Architecture and Taxonomy, Cloud Computing Standards Roadmap, Cloud Computing SAJACC, Cloud Computing Security) centrados en la guía y estándares del Cloud Computing.

4. DMTF (Distributed Management Task Force): es una asociación que desarrolla estándares de gestión empresarial de IT, y que ha visto necesario la existencia de una administración interoperable entre proveedores, clientes y desarrolladores. Esta iniciativa se compone por

los siguientes grupos de trabajo: Cloud Management Working Group (CMWG), Cloud Auditing Data Federation Working Group (CADF), Software Entitlement Working Group (SEWG) & System Virtualization, Partitioning, and Clustering Working Group (SVPC).

Dentro del contexto del presente estudio, el área más importante es la CADF pues junto a los conceptos de CSA crear una filosofía, que permite satisfacer las obligaciones de nivel del servicio de Cloud Computing y se expresa en un protocolo de auditoría.

5. ITU-T SG17: es un grupo de ITU (Unión Internacional de Telecomunicaciones) dedicado al estudio de la seguridad en la Nube especializado en telecomunicaciones. Su foco central es identificar necesidades y desarrollar recomendaciones de seguridad para luego publicarlas con fines de asesoramiento. Este grupo se encuentra compuesto por cuatro áreas: Guía para Cloud Computing en las Telecomunicaciones; Requisitos de seguridad y estructura de un servicio de telecomunicaciones basado en Cloud; Requisitos funcionales de seguridad para software como servicio (SaaS); Requisitos de la gestión de la identidad en Cloud Computing y OASIS (Identity in the Cloud TC). Este grupo utiliza técnicas de CYBEX (Cybersecurity Information Exchange) para el desarrollo de su investigación y actualmente considera que en la Nube los controles de seguridad que se apliquen deben estar basados en la norma ISO/IEC 27002 y la UIT-T X.1051.
6. OASIS - Identity in the Cloud TC: es un grupo dedicado al desarrollo de estándares abiertos para la administración de la Nube y cuyo objetivo es cubrir los problemas de seguridad en la Nube relacionados a la identidad mediante la búsqueda y análisis de vulnerabilidades de esta. Para ello, busca la interoperabilidad de los estándares actuales, mediante casos de estudios de virtualización seguridad en la Nube, secuestro de identidad, entre muchos otros, que muestren una breve descripción propósito, factores para tener en cuenta y un proceso de aquello que se debe hacer para resolver el respectivo problema.

3.2. Aspectos técnicos

El uso de Cloud Computing acarrea consigo un conjunto de riesgos potenciales, por lo mismo se han realizado varias investigaciones por parte de diferentes organizaciones especializadas en la seguridad informática. De ellas, CSA determinó en 2012 las nueve amenazas más críticas en el contexto de Cloud Computing:

1. Violación de la privacidad: se refiere a la información confidencial que robada, utilizada o copiada por terceros no autorizados.
2. Pérdida de datos: errores dados en los sistemas de almacenamiento o bien en la transmisión de información.
3. Secuestro de cuentas/servicios: proceso en que sistema asociado a un dispositivo, como un correo o un usuario, es robado con propósitos maliciosos.
4. APIs inseguras: interfaces con debilidades que dan la posibilidad de explotar datos o servicios sin autorización.
5. Negación de servicios: intrusión que se da en una red usualmente con malas intenciones.
6. Insider: personas (empleados, socios, proveedores, entre otros) con acceso autorizado a la red o datos del cliente y que usan dicha autorización para afectar la integridad, confidencialidad o disponibilidad de la información.
7. Abuso de servicios: dar un mal uso a los recursos legítimos disponibles.
8. Diligencia dual insuficiente: adoptar servicios en la Nube sin ser consiente de los riesgos de su seguridad o sin hacer una validación de controles de privacidad en la Nube sin el conocimiento del cliente.
9. Hipervisores: vulnerabilidades o debilidades dentro de tecnologías clave que permiten la existencia y uso de la nube.

3.3. Aspectos legales

En el ámbito empresarial, hay ciertos aspectos a tomar en cuenta si se desea implementar servicios en la nube, se tienen (Gómez Treviño, 2010):

1. Procesamiento de datos: la empresa debe determinar qué tipo de datos de esta pueden ser procesados y con qué propósito, así como el porcentaje

de esta información que estará disponible en línea sin que se comprometa la confidencialidad de la empresa.

2. Subcontratantes: tener en cuenta con quien se está negociando, específicamente en qué condiciones el proveedor tiene permito subcontratar partes de servicios en la Nube y por supuesto como se manejará la confidencialidad en estos casos.
3. Transferencia de información: siempre existe la posibilidad de que una empresa decida cambiar de proveedor, en este caso la pregunta es ¿qué ocurre con su información? ¿se tiene alguna garantía de que el proveedor conserve una copia de esta?
4. Ubicación de la información: la flexibilidad de la Nube le da al proveedor la libertad de elegir donde se almacena la información de la empresa, sin embargo, este se ve en la obligación de tener el consentimiento del cliente en el caso de que decidiera almacenarla en otro país puesto que esto podría traer complicaciones legales.
5. Protección de datos personales: si una empresa trabaja con servicios de la Nube, esta debe saber manejar y adoptar las medidas contractuales que sean necesarias a fin de evitar problemas innecesarios.
6. Acuerdo de Niveles de Servicio: también conocido como SLA, se refiere a establecer obligaciones de disponibilidad y recuperación de la información entre el cliente y el proveedor, especialmente si este último tiene intenciones de recurrir a subcontratos.
7. Auditorias: a fin de que un cliente pueda comprobar que su proveedor cumple con aquello que se acordó, es recomendable recurrir a autorías gubernamentales donde ambas partes se comprometan a cooperar.
8. Perdida de información: se debe considerar medidas o planes de emergencia para el peor escenario de pérdida de información por negligencia del proveedor, considerando factores como los recursos legales que pueden aplicarse o algún límite de responsabilidad establecido en el contrato.
9. Medidas de seguridad: la empresa debe saber si su información será encriptada, libre de virus, cuenta con un plan de respaldo, y en resumen debe comprometer al proveedor a informarle de cualquier incidente

relacionado a su información, así como las acciones que se tomarían en dicho escenario.

10. Segregación de la información: se refiere básicamente a saber si los datos de la empresa se encuentran separados de los de otros clientes pues existe la posibilidad de que el proveedor también preste sus servicios a la competencia.

En el derecho a la protección de datos personales, se debe tener en cuenta que este depende de otros derechos que lo consolidan y que hasta la fecha no se ha alcanzado homogeneidad a nivel mundial. Se mencionan tres corrientes que responden a este derecho (Melorose, Perroy, & Careas , 2015):

1. Corriente Europea: es la corriente más completa y desarrollada de las mencionadas. Protege los datos de los usuarios mediante un sistema preventivo, mismo que impone responsabilidades a aquellos encargados del manejo y tratamiento de datos desde el primer momento de su recogida. Este sistema se basa en principios, derechos y hasta la participación del Estado mediante un ente legal, y ha sido ejercido en todo el continente desde su la expedición de la Directiva 25/46/CE en el año de 1995 por parte del Parlamento y Consejo Europeo.
2. Corriente Estadounidense: a pesar de contar con bases similares a las del europeo, carece de mecanismos que garanticen el cumplimiento de las políticas de seguridad establecidas, en su lugar, sus regulaciones se concentran en promover el flujo de información a modo de prevención de los intereses personales, dando como resultado un modelo favorable para la autorregulación y algunas propuestas legislativas que intentan cubrir la falta de mecanismos existentes en este modelo.
3. Corriente Latinoamericana: no es posible definir este nivel con algún nivel de protección específica, puesto que los países alineados a esta corriente, aunque han integrado leyes de protección de datos personales basadas en principios europeos, siguen estando adaptados a la corriente estadounidense, danto como resultado una legislación de criterios diferentes en cada país. No obstante, cuenta con algunos aportes, como el habeas data, que destaca por ser un punto de experiencia común en toda Latinoamérica, incluyendo por supuesto Ecuador. Aunque este modelo

sea ampliamente reconocido a nivel constitucional, solo algunos países cuentan con leyes específicas de protección de datos.

3.3.1. Situación actual en el Ecuador

El Cloud Computing es un tema de alcance global, en Ecuador según los datos del INEC (Instituto Nacional de Estadística y Censos), hasta el 2019 se demostró que aproximadamente el 45.5% de la población cuenta con acceso a internet en sus hogares, mientras que se registra un 59.2% de personas que utilizan el internet.

Herrera explica que se ha demostrado un fuerte uso de la versión gratuita de estos servicios, siendo redes sociales, correos electrónicos, almacenamiento en la Nube (Google, Drive, Dropbox, entre otros), manejo de documentos de forma virtual o control de ordenadores remotos, son algunos de los ejemplos más notables (Herrera, 2014).

En 2019, la revista Datta Business Innovation demostró que, pese al impacto de Cloud, solo el 20% de la información administrada por las industrias con más regulaciones (banca, seguros, salud y sector público) ha sido migrado a la Nube, la misma revista explica que esto se debe a preocupaciones de seguridad y cumplimiento. (Grupo EKOS, 2019).

Al hablar de datos más recientes, Manuel Núñez Murillo, docente de la Universidad Internacional de La Rioja en Ecuador, hablo en una entrevista del 2021 sobre la importancia de trabajar con servicios Cloud en época de pandemia, sus declaraciones se resumen en explicar que aquellas empresas que estaban preparadas para poder trabajar de manera remota con soluciones Cloud fueron más productivas y manejaron mejor el impacto de la pandemia. Núñez también cree que la crisis sanitaria aceleró la digitalización a la par que aumentó los riesgos a ataques de la red, esto ha sido estadísticamente confirmado (aproximadamente entre marzo 2020 hasta abril 2021 el 71% de profesionales de las Tecnologías de la Información y Seguridad aseguran haber detectado ciber amenazas) por varias fuentes como la PwC (PriceWaterhouseCoopers) (UNIR, 2021).

Sin embargo, lo más importante a mencionar quizás no son tanto las estadísticas del Cloud Computing sino su gestión y manejo de la protección de la integridad de datos. En base a esto, se debe tener en que, si bien la protección de datos personales como un derecho es algo que se remonta al 2008, desde 1996 se ha trabajado con un mecanismo de jurisdicción conocido como Habeas Data, mismo que fue pionero en la introducción de normas que ampararían al derecho a la protección de información.

Pese a ello, no existe como tal algún cuerpo legal especifico que ejecute de forma plena este derecho, lo que si existe son leyes relacionadas al mismo, dentro de las cueles, y tal y como J. Collahuazo & J. Alexander (2012) demuestran, algunas de las más destacadas son:

1. Ley de comercio Electrónico del Ecuador: vigente desde el 2005, no hace especificaciones sobre la computación en la Nube, sin embargo, cuenta con ciertas disposiciones relevantes a considerar, en el capítulo sexto indica: "Se reconoce el derecho de las partes para optar libremente por el uso de tecnología y por el sometimiento a la jurisdicción que acuerden mediante convenio o contrato privado, salvo que la prestación de servicios electrónicos o uso de estos servicios se realice de forma directa al consumidor" (Collahuazo & Alexander, 2012).
2. Ley de Propiedad Intelectual en Ecuador: el marco legal de la propiedad intelectual, en el artículo 5 menciona textualmente: "Se protegen todas las obras, interpretaciones, ejecuciones, producciones o emisión radiofónica cualquiera sea el país de origen de la obra, la nacionalidad o el domicilio del autor o titular". En esta protección también se reconoce cualquiera que sea el lugar de publicación o divulgación (Collahuazo & Alexander, 2012).

3.3.2. Constitución de la República del Ecuador

Previamente se hizo una breve introducción de las leyes existentes y relevantes relacionadas a la Computación en la Nube, a continuación, se anexan las leyes citadas (Constitución de la República del Ecuador, 2008):

Tabla 2 Artículos de la constitución con relación a la Computación en la Nube

Sección del Artículo	Contenido
Capítulo tercero: Sección Quinta. Acción de Habeas Data Art. 92	Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.
	Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, esta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.
Capitulo Sexto Sección Segunda. Tipos de Propiedad. Art. 322	Se reconoce la propiedad intelectual de acuerdo con las condiciones que señale la ley. Se prohíbe toda forma de apropiación de conocimientos colectivos, en el ámbito de las ciencias, tecnologías y saberes ancestrales. Se

	Prohíbe también la apropiación sobre los recursos genéticos que contienen la diversidad biológica y la agrobiodiversidad.

Fuente: Autor, tomado de la Constitución del Ecuador

3.3.3. Leyes existentes en el contexto de ciberseguridad

De forma general, se pueden listar las siguientes reglas y acuerdos que garantizan la ciberseguridad (algunas fueron previamente mencionadas, en especial las que se tratan de protección de la propiedad intelectual):

1. Constitución de la República del Ecuador: el Art. 66. Numeral 19, describe el derecho a la protección de datos de carácter personal, incluyendo el acceso y decisión del titular de tratar estos datos. (Constitución de la República del Ecuador, 2008):
2. Ley de Seguridad Pública y del Estado: el Art. 2 cita que la seguridad del Estado cubre la protección y el control riesgos tecnológicos y científicos, la tecnología, industria militar, entre otros. Por su parte, el Art. 3, menciona ciertas inseguridades críticas de riesgo en la gestión de los sectores estratégicos, el Ministerio de Defensa Nacional tiene permitido disponer de fuerzas armadas la protección de estas y que se garantice un normal funcionamiento ya sea de instalaciones o infraestructuras críticas (Asamblea Nacional, 2009).
3. Ley de Comercio electrónico, firmas electrónicas y mensajes de datos: esta ley regula todo aquello que se relacione con firma electrónica, servicios de certificación, mensajes de datos, prestación de servicios y contratación electrónicos y telemática, con la condición de que la información se maneje en medios tecnológicos. En este caso se asume la protección de la información de los usuarios en las diferentes plataformas utilizadas (Congreso Nacional, 2002).
4. SNAP (Secretaría Nacional de la Administración Pública): el Acuerdo No.166, indica que al interior de cada institución se debe implementar el "Esquema Gubernamental de Seguridad de la Información", cuyo objetivo principal es la protección de los

componentes de la infraestructura gubernamental frente a los ciberataques, y que debe ser aplicado a aquellas entidades de administración pública central que generen, procesen, almacenen, comprendan y compartan información en medios (escritos o electrónicos) que sea de carácter confidencial (Secretaría Nacional de la Administración Pública, 2013).

3.4. Principales enfoques en la seguridad

3.4.1. Servicios de contratación

Existen varios factores de seguridad a considerar al momento de realizar un contrato con servicios de Cloud Computing, por lo que es recomendable que este incluya una cláusula que comprometa al proveedor a revelar cualquier incidente que involucre la información proporcionada por el cliente, sobre todo en casos donde exista la posibilidad de que la información sea alterada o robada sin autorización (Collahuazo & Alexander, 2012).

Se proponen los siguientes principios básicos de seguridad informática (Arminio, Velásquez, Mayor, & Andrés, 2013):

1. Confidencialidad: asegura que no se divulgue publique la información a terceros no autorizados.
2. Integridad: garantiza no permitir cambios en la información proporcionada por personas ajenas.
3. Disponibilidad: le permite al usuario acceder a la información en cualquier momento, independientemente de donde se encuentre.

3.4.2. Protección de datos

El uso de Cloud Computing acarrea varios riesgos relacionados la protección de datos que involucran tanto a clientes como proveedores. Los más importantes son (Camps Sinisterra & Oriol Allende, 2012):

1. Infracciones de seguridad de datos que no sean notificadas al cliente por parte del proveedor.
2. El cliente puede perder el control de los datos procesados por el proveedor, lo que aumenta los problemas de transferencias de datos.
3. El proveedor obtiene datos que no han sido concedidos legalmente por su cliente.
4. Es esencial entender que el cliente es visto como el principal responsable del procesamiento de datos personales y el incumplimiento de la legislación en contexto de la protección legales puede traer consecuencias administrativas, civiles e incluso legales.

3.4.3. Riesgos de Cloud Computing

Pese a todas las ventajas de su uso, el Cloud Computing también abarca una serie de riesgos, para afrontarlos se debe realizar un análisis de aquellos elementos que permitan que los datos sean tratados sin merma de garantías (Tobergte & Curtis, 2013).

En el 2013, la AGPD (Agencia Española de Protección de Datos), determinó que estos riesgos se pueden agrupar en dos grupos (AGPD, 2013):

1. Falta de transparencia: el proveedor es quien conoce los detalles del servicio que ofrece, y si no ofrece información precisa y completa sobre todos los elementos a intervenir (tales como las medidas de seguridad, controles de acceso o subcontrataciones), causa que el usuario no pueda evaluar los riesgos de manera realista y sus decisiones sean incompletas.
2. Falta de protección de uso: la falta de control del responsable se manifiesta como consecuencia de singularidades existentes en el modelo de tratamiento de la nube y de la falta de transparencia. Por ejemplo, el usuario puede tener dificultades en conocer la ubicación de sus datos o en obtenerlos en un formato válido.

4. Capítulo 4: Análisis de riesgos y vulnerabilidades

4.1. Amenazas del Cloud Computing

El Cloud Computing puede aparentar ser un escenario de opciones variadas y favorables para los usuarios, pero debido a todos los problemas de inseguridad descritos en el capítulo anterior, en algunos casos podría darse entornos dañinos. la Nube es considerada como un blanco atractivo para los atacantes, por ser un gran repositorio de información y datos, lo convierte en el lugar perfecto para atacar varias fuentes de datos de forma simultánea (Sabahi, 2011).

Los riesgos y amenazas potenciales de este entorno se han propagado con una preocupante rapidez provocando varias versiones de estas. Debido a esto, varias organizaciones relacionadas con la Seguridad de la Información han realizado investigaciones especializadas a fin de dar a conocer sus resultados y conclusiones a los usuarios.

De todos estos estudios, se consideró como base de análisis a aquellas que más han destacado en la Seguridad de la información:

- Instituto Nacional de Normas y Tecnología
- Agencia Europea de Seguridad de las redes y la información
- Cloud Security Alliance

4.2. Análisis en base al NIST

Los especialistas en Seguridad de Cloud Computing del NIST desarrollaron el reporte “Guías para Seguridad y la Privacidad en Cloud Computing” (Jansen & Grance, 2011), el cual se enfoca principalmente en dos áreas; “Aspectos Claves para la Seguridad” y “Recomendaciones para la seguridad”.

Del primer punto, el NIST ha determinado que son nueve los aspectos más importantes para la Seguridad en Cloud Computing:

1. *Gobernanza*: abarca los aspectos de supervisión y control de políticas, así como el desarrollo de aplicaciones (incluyendo sus procedimientos y estándares), diseño, implementación, pruebas y monitorización de servicios distribuidos.

La gobernanza se considera una prioridad dentro de los servicios que incluye Cloud Computing, pues si no es eficiente, se trabajaría sin regulaciones causando una mezcla de servicios inseguros. Este factor hace énfasis en los roles y responsabilices existentes entre el cliente y proveedor, principalmente en la gestión de riesgos pues es preferible que esta cuente con una revisión y evolución continuas.

Como último punto, se recomienda trabajar como medidas que permitan validar servicios y el cumplimiento de las políticas empresariales, como herramientas de auditoría que determinen como se están almacenando, utilizando y protegiendo los datos.

2. *Cumplimiento normativo*: se refiere a la responsabilidad y capacidad de las organizaciones para operar según las leyes, estándares, regulaciones y especificaciones establecidas. Estas regulaciones dependen de las localidades (países y estados), haciendo que sea complejo para el Cloud Computing establecer su cumplimiento. En este contexto, existen tres áreas principales:
    a. Leyes y regulaciones: quizás el aspecto más preocupante para los proveedores, quienes optan por el almacenamiento y procesamiento de datos en ciertas jurisdicciones junto a garantías se seguridad y privacidad. Por su parte, el cliente pasa a convertirse en la última instancia de un proveedor en términos de responsabilidad de seguridad y privacidad de datos.
    b. Localización de datos: la flexibilidad del Cloud Computing permite a los usuarios acceder a su información desde cualquier localidad, aunque los mismos desconozcan la ubicación real de sus datos, o como están siendo almacenados/protegidos.

       El proveedor debe contar con certificaciones de normas de seguridad a fin generar más confianza a sus clientes.

       En caso de que la información fuese trasladada entre varias ubicaciones, confrontaría diferentes marcos legales, lo que afectaría el tratado de datos. Determinar los límites legales entre los diferentes estados o países involucrados en una traslación, es uno de los puntos más preocupantes de este apartado.

c. Descubrimiento electrónico: es el trato (recolección, procesamiento, análisis, producción e identificación) de la información almacenada de forma electrónica. Específicamente, esta fase analiza correos electrónicos, archivos adjuntos u otros datos que hayan sido almacenados en algún tipo de sistema junto con los metadatos (por ejemplo, las fechas de modificación de archivos). El proveedor debe ser capaz de almacenar la información de sus clientes de la mejor manera posible, esto incluye evitar daños intencionados que podrían afectar potenciales evidencias.

3. *Confianza*: es la clave para que un cliente voluntariamente renuncie al control directo de su información comprometiendo su privacidad y seguridad. Para ello, el proveedor debe considerar los siguientes aspectos:
    a. Acceso interno: es un problema que afecta a todas las organizaciones, refiriéndose a exempleados, empresas asociadas, empleados, y toda persona que tenga o haya tenido acceso a los datos. El daño puede o no ser intencional, pero representa problemas que van desde fraude hasta robo de confidencialidades.
    b. Propiedad de datos: el proveedor, al ser la entidad que tiene acceso a la información de sus clientes, debe asegurar mediante un contrato que los usuarios y organizaciones, siguen siendo los propietarios de esta. El proveedor no tiene permitido utilizar esta información para beneficios personales.
    c. Servicios complejos: el Cloud Computing está conformado por una gran variedad de servicios cuya disponibilidad en general es directamente dependiente de su uso, si alguno de los componentes de servicios sufre problemas en su disponibilidad, el efecto negativo se trasmite a los servicios en general.

       Esto también significa que en caso de que alguno de los servicios sufra de la intervención de una tercera entidad, se deberán dividir las responsabilidades y garantías de cumplimiento entre cada uno, lo que puede provocar un problema en servicios compuestos.

d. Visibilidad: es el monitoreo como herramienta de vigilancia de la seguridad de datos en servicios de la Nube. Esta responsabilidad le corresponde al proveedor pues al ser quien posee el control de la información, está en la obligación de mantener una vigilancia continua de los mismos.

   Dicha responsabilidad demanda que el proveedor sea transparente en la gestión de la información (incluyendo los controles y procesos sados en la administración de seguridad y privacidad). Lógicamente esta información no suele ser de carácter público pues los proveedores piensan que podría volverse una vulnerabilidad, aun así, es menester que el cliente sea consiente de cómo sus datos están siendo manejados.

e. Auxiliares: información complementaria que de una u otra forma involucra al cliente, y que por lo mismo podría ser usada de forma perjudicial, evidentemente, la protección de estos datos también pasa a ser responsabilidad del proveedor.

f. Gestión de riesgo: cubre la identificación y evaluación de potenciales riesgos para la organización, así como de acciones que hagan que estos seas reducidos lo más que sea posible, o en el mejor escenario, mitigarlos. También se involucra la implementación de estrategias y técnicas contra riesgos y una constante de supervisión en la seguridad de todos los sistemas.

4. *Arquitectura*: el Cloud Computing cuenta con dos componentes básicos en su infraestructura: software y hardware. La clave de la seguridad y de potenciales vulnerabilidades en la misma, se encuentra en la comunicación de estos dos componentes. Existen muchas áreas potenciales a ataques que surgen de esto destacando:

   a. Máquinas virtuales: pila o fragmento de software con sus respetivas aplicaciones y configuraciones. Debido a su rapidez de inicio, es bastante común en un entorno de virtualización trabajar mediante la compartición de máquinas virtuales, no obstante, esta práctica puede representar una amenaza a la seguridad de una organización pues corre el riesgo de que sus datos sean replicados en caso de que esta haya creado una imagen con los mismos.

b. Superficie de ataque: se refiere al hipervisor, el cual es una capa de software que permite la conexión entre los elementos de hardware usados en la operación de máquinas virtuales y el sistema operativo. El problema radica en que un fallo en el hipervisor puede comprometer todos los sistemas que lo acogen.
c. La red virtual: abarca numerosas plataformas de virtualización capaces de usar configuraciones de red y software para crear suiches, lo que permite que las máquinas virtuales se comuniquen de forma directa al mismo servidor. Sin embargo, durante esta conexión el tráfico de red no puede ser monitoreado por elementos físicos de red (como los sistemas de detección de intrusos), en el peor escenario esto puede causar ataques internos, así que es necesario tomar las precauciones necesarias para evitar que esto ocurra.
d. Protección del cliente: el uso de conexiones inalámbricas y navegadores, así como la posible existencia de virus o troyanos que realicen robo o espionaje de información, representan algunas de las brechas a la seguridad en el uso de Cloud Computing con las que los clientes se verían comprometidos. Es deber de los proveedores reforzar los sistemas de seguridad de datos existentes o reemplazarlos si fuese necesario.

5. *Identidad y acceso de control*: una de las prioridades de los clientes es saber que su información se mantenga segura, para ello se debe tener un control transparente de quienes pueden acceder a dicha información y de la identidad de estos. Ante esto, la Federación de Identidades (SIR, 2021) ofrece una solución que puede ser implementa mediante los estándares SAML (Security Assertion Markup Language) u OpenID. En este aspecto es fundamental tener claro los conceptos de autenticación y control de acceso:
    a. Autenticación: proceso que permite asegurar que un usuario es quien dice ser. Es un factor fundamental y para su garantía los proveedores de estos servicios han optado usar el estándar SAML (mismo que brinda un entorno para el intercambio de información

durante el proceso de autenticación entre dominios) junto al protocolo SOAP (Simple Object Access Protocol) que maneja el envío y recibo de mensajes mediante firmas digitales. Este último debe ser tratado con cuidado pues puede llegar a representar problemas de seguridad (por ejemplo, si se manipulase la información de las cabeceras, este tipo de ataque es conocido como XML Wrapping).

b. Control de acceso: se lo define como un componente encargado del monitoreo, este proceso también suele manejarse con el estándar SAML, pero es recomendable usar complementos que puedan reforzar la seguridad de este.

6. *Aislamiento de software*: mecanismo usado para ejecutar programas de forma segura y separada. En el caso de Cloud Computing, se trabaja con máquinas virtuales a fin de poder lograrlo y garantizar que los servicios demandados sean rápidos y flexibles. Las vulnerabilidades de esta naturaleza son visibles principalmente en servicios IaaS al ser quienes sufren ataques en sus máquinas virtuales, de aquí que surge la importancia del aislamiento en la compartición de plataformas en la Nube. Los factores por considerar en esto último incluyen:
    a. Complejidad del hipervisor: el hipervisor se encuentra diseñado para correr varias máquinas virtuales de forma concurrente, incluyendo su respectivo sistema operativo y aplicaciones, a la vez que brinda aislamiento entre ellas. La complejidad del hipervisor debe ser inferior a la de un sistema operativo a la vez que su inteligencia debe ser superior a la de este, esto último debido a sus características adicionales de seguridad y aislamiento. A fin de comprender los posibles riesgos y soluciones a los mismos que esto acarrea, el proveedor se ve en la obligación de conocer su uso, su funcionamiento y aplicación en el contexto de la virtualización.

    b. Vectores de ataque: el uso de máquinas virtuales está relacionado a vulnerabilidades, cosa que en parte se debe a su uso físico de

recursos compartidos. A continuación, se presentan algunos de los vectores de ataques más utilizados:

- Desbordamiento de buffer en código arbitrario o falencias en denegaciones de servicios.
- MitM (man in the middle) es un ataque usado para alterar el código de autenticación
- Rootkits, se trata de un programa que le da a una computadora accesos para corromper al sistema operativo que a su vez son ocultos del administrador. Se suelen instalar mediante la modificación de memoria de una máquina virtual durante alguna migración.

7. *Protección de datos*: las plataformas usadas por los servicios de Cloud Computing pueden ser desconocidas para los clientes y esto los puede llevar a sentir desconfianza. Ante esta problemática el proveedor debe garantizar y demostrar la confidencialidad y protección de la información. Esto implica proteger tanto la totalidad de sus datos, como aplicaciones y configuraciones. Para garantizar esta protección en todo momento, incluso cuando la información de encuentra en alguna fase de uso, se hace uso de criptografía en la administración de claves y transferencia de a información, aquí se tratan dos factores:
    a. Valor concentrado: la infraestructura de servicios Cloud es un blanco de potenciales ataques pues se maneja de forma concentrada, en el caso de los proveedores esto significa tener en un punto la información de distintos clientes. Esto dio lugar a una de las estrategias más preocupantes y utilizadas es la ingeniería social, la cual se basa en manipulación y engaños psicológicos para conseguir contraseñas y falsificar autenticación.
    b. Saneamiento: en el contexto actual este término no se refiere a su definición literal si no que parte de la siguiente interpretación; cuando un cliente decide dejar de usar algún medio de almacenamiento, este asume que se eliminará de forma infalible y confiable todos sus datos, esto incluye que también se deben eliminar todas las copias de seguridad e información residual.

Aquí surgen dos potenciales brechas de seguridad, la primera es el uso de técnicas para la recuperación, parcial o total, de esta información y que posteriormente sea usada con fines maliciosos; la segunda es que debido a la modalidad compartida de la plataforma se borren accidentalmente datos de otros clientes.

8. *Disponibilidad*: si bien es una de las principales ventajas de los servicios de Cloud Computing, también representa un factor que puede ser afectado temporal o permanentemente (en el caso de fallos por parte de los equipos, brechas en la seguridad, o factores externos como desastres naturales); en un nivel más detallado se tiene:
    a. Fallas temporales: aunque no es algo común, los servicios pueden presentar caídas de desempeño, como falencias en almacenamiento, actualizaciones (o bien ser inoportunas) y dispositivos de red. Estas falencias causan que los clientes sean incapaces de acceder a los servicios durante un intervalo de tiempo, que suele ser entre dos y cuatro horas. Descrito numéricamente los servicios Cloud cuentan con un nivel de aproximadamente 99.95%, lo que representa unas 4.38 horas de falencias en el servidor.

       El proveedor debe dar a conocer a sus usuarios de las fallas temporales y especificar en los contratos de servicios, también debe incluir un plan de continuidad para las ya mencionadas donde se explique lo que se debe hacer durante el intervalo de recuperación.
    b. Fallas permanentes: son de magnitud incluso menos frecuente pero más catastrófica, algunos ejemplos son incautación de equipos, perdida de servicios por parte de los proveedores debido a terceros, bancarrota de un proveedor, entre otros. Como su nombre indica, representan la pérdida total de servicios por un intervalo indeterminado.
    c. Denegación de servicio: saturación de un servicio, se realizan varias peticiones falsas para impedir que las legítimas sean atendidas. Este tipo de ataques suelen hacer uso de una Bonet (una

red de equipos zombis) y no se encuentran limitados a internet, pues también se presentan en la infraestructura. Lo más preocupante es que aun si el ataque carece de éxito, se da un alto consumo de los recursos de defensa debido al elevado porcentaje de peticiones.

9. *Respuestas a incidentes*: el proveedor de servicios Cloud es indispensable en las fases de potenciales incidencias (confirmación, análisis, reunión de evidencias, solución y restablecimiento). Sin embargo, no es una tarea unilateral pues, la naturaleza de las plataformas requiere que el cliente también se mantenga alerta y trabaje en una relación de colaboración a fin de poder detectar brechas de la seguridad. En este sentido, el elemento clave es el contrato entre cliente-proveedor. Este tipo de respuesta se basan en:
    a. Disponibilidad de datos: es un punto básico para la detección de amenazas y se relaciona directamente con el monitoreo.

       Los clientes no cuentan con mucha participación pues por lo general carecen del acceso de una fuente confiable para informarse de eventos, o de una interfaz apropiada para la gestión de incendias, debido a esto, la disponibilidad se encuentra generalmente supervisada y restringida por el proveedor.
    b. Solución de incidentes: antes de ofrecer una solución es necesario realizar un análisis del problema en cuestión y para ello es primero necesario el conocer el grado de afectación, los sistemas y/o aplicaciones que han sido atacados y, por último, ofrecer una reconstrucción del problema. Nuevamente, la limitación del cliente representa un problema, pues el desconocer el funcionamiento de arquitecturas o detección de donde se dio el fallo, le impide tener una participación en la recolección de pruebas y preservación de datos.

En base a las áreas claves mencionas y sus respectivas vulnerabilidades, el NIST ha elaborado una tabla de recomendaciones básicas a realizar en cada una de ellas, misma que se presenta a continuación:

Tabla 3 Resumen de recomendaciones según el NIST

Área	Recomendaciones
Gobernanza	Establecer políticas, estándares y procedimientos en el desarrollo de aplicaciones/servicios de Cloud Computing.
	Implementar mecanismos y herramientas de auditoría y control para garantizar el seguimiento de las políticas establecidas por las organizaciones en el periodo del ciclo de vida.
Cumplimiento	Comprender las leyes y regulaciones que dictan las responsabilidades de seguridad y privacidad en las organizaciones.
	Dar especial atención a las leyes relacionadas con gestión de riesgos y seguridad.
	Usar sus requisitos y necesidades como parámetros para elegir un proveedor de servicios en la Nube y establecer garantías para que se cumplan las condiciones demandadas.
	Obtener garantías por parte del proveedor para saber que este no representará una amenaza a la privacidad de los datos de los clientes.
Confianza	El cliente debe contar con los medios de visibilidad suficientes para garantizar la seguridad y rendimiento de los procesos usados por el proveedor de servicios Cloud.
	Definir derechos de propiedad y exclusividad de datos.
	Asegurar un monitoreo constante del estado de seguridad en los sistemas de información a fin de apoyar las decisiones tomadas en la gestión de riesgos.
Arquitectura	El cliente entender las tecnologías que el proveedor usa en los servicios de suministros, y las repercusiones de estas en la privacidad del sistema y sus componentes.
Identidad y acceso de control	Contar con las garantías necesarias para verificar la autenticación y autorización.
	Garantizar que las funciones utilizadas en este aspecto sean las adecuadas para la organización.

Aislamiento de software	Entender las tecnologías de aislamiento que el proveedor utilice en la arquitectura de software, se recomienda evaluar los riesgos de estas.
Protección de datos	Ser consiente de los riesgos existentes al colocar su información en plataformas virtuales.
	Implementar un proceso de evaluación a las soluciones ofrecidas por el proveedor determinar qué tan adecuadas son en el contexto de control, gestión, acceso, seguridad, transito, uso y desinfección de datos.
	Evaluar los riesgos del manejo y uso de criptografías, para lo cual debe comprender la gestión de estas.
Disponibilidad	Leer las cláusulas y procedimientos que el proveedor ejecutará en la disponibilidad, respaldos y restauración de datos. Garantizar que dichas medidas cuentan con planes de continuidad y contingencia.
	Garantizar la restauración total, oportuna y organizada de las operaciones en el caso de alguna interrupción inesperada.
Respuesta a incidentes	Comprende las cláusulas y procedimientos del proveedor en lo referente a planes de respuesta contra incidentes, asegurando que estos cumplan con los requisitos demandados por la organización.
	El proveedor debe probar que cuenta con procesos y mecanismos transparentes y suficientes de manejo de información tanto antes como después de un incidente.
	El proveedor y organización cuentan con sus respectivos roles y responsabilidades en el entorno informático a fin de poder actuar en respuesta a un incidente, por lo que ambos deben trabajar de forma coordinada.

Fuente: Autor, tomado del NIST

4.3. Análisis en base a la ENISA

ENISA se ha enfocado principalmente en un grupo de consideraciones y buenas prácticas (tanto generales como específicas) a considerar durante la gestión de información de la Nube. Este documento, titulado "Beneficios, riesgos y recomendaciones para la Seguridad de la Información" (ENISA, 2020), tiene el objetivo de aportar sobre las temáticas más importantes para la seguridad informática, como lo son la evaluación de riesgos.

ENISA considera que los aspectos más relevantes del Cloud Computing son:

1. La administración de recursos, se la maneja mediante una gestión física y lógica.
2. La arquitectura de redes actualmente cuenta con una alta demanda donde siempre se espera un servicio de alta calidad, se encuentra directamente ligado con el proveedor de comunicaciones del cliente.
3. La economía, estos servicios representan una economía a escala para las empresas y sus respectivos proveedores, misma que crecerá según la necesidad de recursos existente.

A continuación, se enlistan las ventajas y vulnerabilidades existentes en la Seguridad de la Información referentes al uso de Cloud Computing. Este análisis también especifica el riesgo que las medidas a tomar ante dichas vulnerabilidades. Estas medidas se refieren exclusivamente a los requisitos básicos que un proveedor debe proporcionar si busca garantizar que ofrece un correcto manejo de seguridad.

Las ventajas para la seguridad de la información en Cloud Computing son:

1. *La seguridad como diferenciador*: la mayor demanda existente en este mercado se relaciona a la seguridad, por lo que los usuarios juzgan a los diferentes proveedores en base a parámetros como la popularidad de los ofertantes, el nivel de confidencialidad e integridad, y el grado de protección a fallos junto a un respetivo plan de soluciones a cualquier posible inconveniente.
2. *Interfaces normalizadas*: el proveedor debe facilitar la gestión de los servicios de seguridad. Por ejemplo, si un proceso requiere de la intervención de un tercero se procede mediante la estandarización; se sugiere la aplicación de interfaces abiertas.

3. *Escala de recursos*: los proveedores deben saber manejar aspectos como la administración de recursos, tráfico o autenticación de forma rápida e inteligente. Es obligación del proveedor contar con las herramientas e infraestructura necesaria para solucionar eficiente y eficazmente estos potenciales inconvenientes.
4. *Recogida de pruebas*: se maneja mediante auditorías, y se refiere a dar un análisis detallado a la información sin deshabilitar la infraestructura principal; se hace uso de un clon de la máquina virtual.
5. *Actualizaciones:* se incluyen también todas las opciones por defecto en las máquinas virtuales de los clientes, lo que se traduce a saber reforzar las configuraciones de seguridad de estas. Esto gracias a que, a diferencia de los sistemas tradicionales, los servicios de Cloud se manejan mediante una plataforma homogénea.
6. *Concentración de recursos*: reducción de costos tanto en el control de acceso físico como en los perímetros usados para la protección de centros de datos.

A continuación, se mencionan los problemas de seguridad (riesgos amenazas y vulnerabilidades) derivados del uso de estos servicios. Es importante primero entender las diferencias entre estos términos, para lo cual, se hace uso de las definiciones publicadas en la ISO 27001 (Anónimo, 2007).

1. *Amenaza*: "Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
2. *Riesgo*: "Efecto de la incertidumbre sobre los objetivos" … "El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización."
3. *Vulnerabilidad*: "Debilidad de un activo o control que puede ser explotada por una o más amenazas."

En base a esto, los riesgos de servicios Cloud que ENISA considera son:

1. *Perdida de gobernanza*: los usuarios de la Nube pierden el control de sus datos pues lo ceden a su proveedor.
2. *Vinculación*: procesos de migración entre proveedores, es recomendable que estos sean estandarizados.
3. *Fallo en aislamiento*: posibles fallas en los procesos utilizados para la separación de recursos (almacenamiento, memoria, enrutamiento entre otros).
4. *Riesgos en cumplimiento de normas*: también se relaciona a los procesos de migración, en este caso este proceso puede tener una alteración secundaria a los procesos de una organización, misma que puede complicar los procesos de certificación al alterar alguna normativa.
5. *Interfaz de gestión*: las interfaces, al ser la conexión entre recursos, pueden verse comprometidas en ciertas circunstancias, en la mayoría de los casos esto se debe a factores externos como, por ejemplo, debilidades en el navegador que se esté manejando.
6. *Protección de datos*: factor arduo de garantizar para el proveedor, y que al cliente le resulta difícil saber si está siendo cumplido (si su información está siendo administrada con técnicas correctas y legales). Por esto último, algunos proveedores prefieren usar cierta evidencia con sus clientes a fin de ganar su confianza, estas pueden ser certificaciones de seguridad (SAS 70, ISO 27001 u otras) o informando al cliente de los procesos de control que manejan.
7. *Fallos en suspensión de datos*: los errores de eliminación de información al 100% pueden darse debido a fallas en los sistemas operativos, o bien, contar con una copia hecha por algún tercero sin el consentimiento ni conocimiento del cliente.
8. *Integrante malicioso*: como su nombre indica, se refiere al riesgo de un miembro, ya sea en la organización del cliente o el proveedor, que se aproveche de su posición por beneficios personales.

Finalmente, corresponde listar las vulnerabilidades que pueden presentarse y que dependen principalmente de las tecnologías usadas en la infraestructura, a la vez que tienden a relacionarse con la virtualización, cifrado-manejo de claves, y la administración de autenticación.

ENISA considera como vulnerabilidades generales más importantes

1. Ausencia de conciencia de la Seguridad (tanto proveedores como clientes deben ser conscientes de los riesgos a los que la información puede comprometerse).
2. Carencia de procesos de investigación sobre el perfil de riesgo del personal cuyas funciones incluyen cierto nivel de privilegio.
3. Distribución imprecisa de las funciones y responsabilidades, del proveedor o del cliente.
4. Incorrecta separación de las funciones en el rol del proveedor, es decir que éste y/o sus asociados cuenten con privilegios muy altos.
5. Falta de aplicación del Principio del mínimo conocimiento ("Need to Know"); no ceder accesos innecesarios a las partes.
6. Implementación de débiles procedimientos de seguridad física.
7. Vulnerabilidades generales en el sistema o sistemas operativos.
8. Utilización de software de baja calidad (poco confiable).
9. Deficiencia, o carencia, de un Plan de Continuidad del Negocio y de recuperación de desastres. Estos deben estar puestos a prueba en caso de algún incidente.
10. Activos con un inventario deficiente (incompleto, impropio o ausente).
11. Falta de identificación suficiente en los requisitos de carácter legal y de seguridad.
12. Un análisis inconcluso al momento de elegir un proveedor.
13. Carencia de redundancias
14. Una pobre administración de parches.
15. Vulnerabilidades en el consumo de recursos.
16. Incumplimiento de acuerdos de confidencialidad y no divulgación por parte del proveedor.
17. Procedimientos y/o políticas insuficientes para la compilación y custodia de registros.
18. Recursos de filtrado inapropiados o incorrectamente configurados.

Fuente: Autor, basado en los datos de la ENISA

Por otro lado, ENISA considera que las vulnerabilidades especificas dentro del entorno de Cloud Computing son:

1. Uso de pobres sistemas de Autenticación, Autorización y Auditoría (AAA) pues esto facilitaría un acceso no autorizado a los recursos.
2. Procesos que no se encuentren controlados tanto para el alta como para la baja de usuarios.
3. El comprometer la infraestructura de la Nube debido a un acceso remoto a la interfaz de gestión.
4. Falencias en el hipervisor (todos los equipos virtuales poseen la misma vulnerabilidad).
5. El no aislamiento de los recursos de un cliente de los demás.
6. Autenticación y codificación de la comunicación de baja calidad.
7. Codificación de archivos y datos en el tránsito deficientes.
8. Trabas en el procesamiento de datos codificados.
9. Gestión de claves manejadas con procesos deficientes.
10. Baja entropía para la generación de números aleatorios, en la generación de contraseñas.
11. Carencia de estandarizaciones en soluciones y tecnologías.
12. Proveedores de servicios PaaS o SaaS, sin acuerdos en caso de quiebre.
13. Recursos con un modelado ineficiente. Esto puede darse debido a una falla en los algoritmos de provisión de estos, lo que, en el peor escenario, puede causar su respectivo agotamiento.
14. Posibilidad de que un tercero ejecute un análisis interno de red; ej. un escaneo de puertos, en los clientes que se encuentren en la Nube.
15. Probabilidad de que el proveedor se vea expuesto (dar a conocer a sobre fallas en los procesos de aislamiento y chequeo de los recursos compartidos).
16. Medios sensibles que se vean expuestos a una eliminación fallida o limpieza completa.
17. El cliente siendo total o parcialmente ignorante acerca de sus responsabilidades y/o obligaciones contractuales a las que se ve atado al contratar servicios de Cloud Computing.

18. Organizaciones comprometidas a cláusulas en el contrato que representen, un riesgo para el negocio, es decir, aquellas que le den al proveedor demasiados poder sobre la información almacenada.
19. Clientes sin acceso a auditorías o certificaciones.
20. Sistemas de Certificación que no estén adaptados a las infraestructuras manejadas en la Nube.
21. Recursos e inversiones siendo desperdiciados en infraestructura inapropiadas (deficientes, de baja calidad).
22. Falta o carencia de políticas en la limitación de recursos.
23. La no transparencia; datos siendo almacenados en múltiples jurisdicciones múltiples sin conocimiento de ello.
24. Pobre calidad de información en el contexto de jurisdicciones (probabilidad de que los datos se vean almacenados en sitios de alto riesgo y llegar a ser confiscados).
25. Poca transparencia e integridad en los términos de uso.

Fuente: Autor, basado en los datos de la ENISA

Evidentemente, el uso de servicios Cloud acarrea una considerable lista de riesgos, por lo que, el análisis de ENISA, incluye "la evaluación de riesgos". Se trata de un proceso para determinar la importancia de cada riesgo mediante una comparación en las estimaciones de cada uno de ellos según algún criterio dado.

La Norma ISO 27005:2008 (Anónimo , 2008), presenta los parámetros utilizados para la elaboración de las estimaciones de niveles de riesgo. Los resultados se manejan según la siguiente métrica:

Tabla 4 Clasificación de niveles de riesgo en base a la ISO 27005:2008

Nivel de riesgo	Calificación
Bajo	0-2
Medio	3-5
Alto	6-8

Fuente: Autor, tomado de la ISO 27005:2008

Tabla 5 Estimación de niveles de riesgo en base a la ISO 27005:2008

	Posibilidad de Incidentes

		Muy baja	Baja	Media	Alta	Muy alta
Impacto	**Muy bajo**	0	1	2	3	4
	Bajo	1	2	3	4	5
	Medio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muy alto	4	5	6	7	8

Fuente: Autor, tomado de la ISO 27005:2008

La tabla anterior se maneja de la siguiente forma: para cada riesgo se busca la columna de probabilidad de incidente (muy baja, leve, media, alta, muy alta), y de su nivel de impacto (muy bajo, bajo, medio, alto, muy alto), al tener ambos datos se realiza la intersección de la fila y columna resultante y se ve el numero al que corresponde ese riesgo.

El análisis de ENISA usa los resultados de estas tablas en simulaciones de escenarios PYME (pequeñas y medianas empresas). Cada factor de riego fue analizado en base a: el nivel de riesgo y probabilidad, vulnerabilidades, porcentaje de activos afectados e impacto. Según este análisis PYME, la evaluación de riesgo en la Nube tiene las siguientes clasificaciones:

1. Políticos y organizativos

Tabla 6 Detalles de riesgos políticos y organizativos

	Posibilidad	Impacto	Riesgo
Vinculación	Alta	Medio	Alta
Pérdida de Gobernanza	Muy alta	Muy alto	Alto
Desafíos de Cumplimiento	Muy alta	Alto	Alto
Pérdida del renombre empresarial a raíz de actividades de prestación conjunta.	Baja	Alto	Medio
Error o cancelación del servicio en Nube	-	Muy alto	Medio
Adquisición del proveedor en Nube	-	Medio	Medio
Fallo en la cadena de suministro	Baja	Medio	Bajo

Fuente: Autor, basado en el análisis PYME de ENISA

2. Técnicos

Tabla 7 Detalles de riesgos técnicos

	Posibilidad	Impacto	Riesgo
Agotamiento de recursos	Baja/Media	Medio/Alto	Medio
Fallo de aislamiento	Baja/Media	Muy alto	Alto
Abuso de funciones privilegiadas	Media	Muy alto	Alto
Compromiso de interfaz de gestión	Media	Muy alto	Medio
Interceptación de datos	Media	Alto	Medio
Fuga de datos durante la carga/descarga	Media	Alto	Medio
Supresión de datos ineficaz	Media	Muy alto	Medio
Distribución de denegación de servicio	Baja/Media	Muy alto	Medio
Denegación económica de servicio	Baja	Alto	Medio
Pérdida de claves de codificación	Baja	Alto	Medio
Detecciones maliciosas	Media	Medio	Medio
Motor de servicio de compromiso	Baja	Muy alto	Medio
Conflictos entre procedimientos de refuerzo del cliente y la Nube	Baja	Medio	Bajo

Fuente: Autor, basado en el análisis PYME de ENISA

3. Legales

Tabla 8 Detalles de riesgos legales

	Posibilidad	Impacto	Riesgo
Órdenes judiciales y descubrimiento electrónico	Alta	Medio	Alto
Derivado del cambio de jurisdicción	Muy alta	Alto	Alto
Relativo a protección de datos	Alta	Alto	Alto
Relativos a la licencia	Media	Medio	Medio

Fuente: Autor, basado en el análisis PYME de ENISA

4. No específicos de Cloud

Tabla 9 Detalles de riesgos no específicos de Cloud

	Posibilidad	Impacto	Riesgo
Brechas en la red	Baja	Muy alto	Medio
Gestión de la red	Media	Muy alto	Alto
Modificación del tráfico de la red	Baja	Alto	Medio
Escalada de privilegios	Baja	Alto	Medio
Ingeniería Social	Media	Alto	Medio
Pérdida de los registros operativos	Baja	Medio	Bajo
Pérdida de los registros de seguridad	Baja	Medio	Bajo
Pérdida de copias de seguridad	Baja	Alto	Medio
Acceso no autorizado a los locales	Muy baja	Alto	Bajo
Robo de equipos informáticos	Muy baja	Alto	Bajo
Catástrofes naturales	Muy baja	Alto	Bajo

Fuente: Autor, basado en el análisis PYME de ENISA

ENISA usa como base la Seguridad de la Información del cliente y plantea que todo proveedor debe garantizar como mínimo estos diez aspectos de seguridad:

1. *Personal interno*: las organizaciones de Cloud deben saber qué tipo de personas manejan los datos de sus clientes, por lo que se debe ser muy rigurosos en procesos de contratación, confirmación de identidad, revisión de historial delictivos, capacitación, evaluación al personal, entre otros.
2. *Cadena de suministro*: elementos que hacen funcionar a las empresas de manera organizada. Es analizar y asegurar la confiabilidad del contratista mediante una revisión de identidad, contratos de niveles de servicio

(garantizan que se apliquen estándares, políticas y controles de seguridad internos), entre otros.

3. *Seguridad operativa*: es un aspecto más dirigido al cliente, quien debe incluir en el contrato, sus requisitos y demandas para cumplirlas y así ofrecer un servicio de calidad. El cliente deberá realizar una investigación por cuenta propia a fin de familiarizarse con los procesos que serán utilizados en el tratamiento de su información y así poder consultarle al proveedor de cualquier duda que tenga.
4. *Accesos e identidad*: administración de acceso e identidad, sus procesos (autenticación, autorización gestión de datos, gestión de claves, cifrado, etc.) y los controles de estos.
5. *Administración de activos*: se refiere al inventario que maneja el proveedor, mismo que debe ser actualizado contantemente.
6. *Datos y probabilidad*: al exportar datos desde la Nube, el proveedor debe entregarle al cliente la documentación del proceso que especifique todos los detalles de la exportación. En caso de que se haga lo mismo con las aplicaciones, también se deberá aplicar este proceso.
7. *Continuidad del negocio*: el proveedor debe contar con una administración de manejo de riesgo (procedimientos de recuperación de operaciones, datos, planes de respuestas a incidentes, etc.) que garantice la continuidad del negocio y ofrezca soluciones de calidad.
8. *Seguridad a nivel físico:* el control de personal, acceso físico, uso de equipos externos del personal para acceder a datos, entre otros; deben estar respaldados por el proveedor para probarle al cliente que cuenta con buen nivel de seguridad física. La ISO 21001/2 tiene en su sección 9 un ejemplo más detallado y especifico de control.
9. *Manejo del ambiente:* es el punto sobre el cual menos control tiene el proveedor (factores como interrupción de servicios, problemas de temperatura, humedad, electricidad, castrones naturales, etc.) por lo que debe mostrar las medidas a ejecutar en caso de incidentes.
10. *Legalidad:* se debe llegar a un acuerdo entre el cliente y el proveedor que obedezca a todas las normativas nacionales e internacionales necesarias; dicho acuerdo incluye que el cliente conozca ciertos detalles (ubicación física del proveedor con el que firmará, si se trabajará con terceros, o

especificaciones de carácter juridicial) antes de firmar un contrato con un proveedor de Cloud. También debe consultar que pasará con su información una vez que el contrato expire.

4.4. Análisis en base a la CSA

La CSA cubre dos reportes referentes al estudio de amenazas y riesgos existentes en la Nube: "Top Threats to Cloud Computing", cuya versión más reciente es de 2019 (CSA, 2019), y la "Guía para la Seguridad en áreas críticas de atención en Cloud Computing", que representan la base del presente análisis.

1. Principales Amenazas en Cloud Computing

Las tecnologías de la información presentan distintos riesgos en las áreas de seguridad, disponibilidad y rendimiento. En Cloud Computing, debido a su característica de concentración de datos en un solo lugar, estos riesgos pueden llegar a maximizarse.

En la seguridad de Cloud Computing, las áreas donde más riesgos pueden presentarse incluyen: uso de arquitecturas orientadas a servicios, virtualización y la infraestructura no externalizada. Es en este último punto, donde entra en juego la seguridad y privacidad de su información.

La CSA considera como áreas de suma importancia la confidencialidad, autenticación, integridad y ubicación de los datos. En base a ello, han elaborado la siguiente tabla de amenazas:

Tabla 10 Amenazas listadas por la CSA

Amenaza	Descripción
1	Abuso y uso inadecuado del Cloud Computing.
2	Interfaces y APIs inseguras.
3	Amenazas internas malintencionadas.
4	Inconvenientes debido a las tecnologías compartidas.
5	Pérdida o fuga de datos.
6	Secuestro de sesión o de servicio.

7	Riesgos por desconocimiento.

Fuente: Autor, tomado de la CSA

1. *Amenaza 1 - Abuso y uso inadecuado del Cloud Computing:* El acceso y uso de plataformas de Cloud Computing cuenta con un estricto proceso de autenticación, para evitar problemas. Ante posibles ataques como son el spam, código malicioso, bloqueos de direcciones Ip, entre otros; se dan algunas de sugerencias:
    a) Aplicar medidas de validación y registro que permitan de forma minuciosa confirmar los datos de cada usuario.
    b) En el caso de tarjetas de crédito, contactar a la entidad que procesa los datos de esta para verificarlos y evitar fraude.
    c) Contactar al proveedor de Cloud Computing para solicitar las listas negras de bloqueo de direcciones Ip y darles monitoreo constante.

2. *Amenaza 2 - Interfaces y APIs inseguras:* Los usuarios de Cloud tienen a su disposición el uso de varias APIs, lo cual, si bien puede representar una ventaja, es a su vez una potencial amenaza a la confidencialidad, integridad y seguridad de la información. Esto se debe a que estas APIs pueden ser un medio para que los atacantes realicen daños al usuario o dar problemas por accidente. Dentro de estos problemas se tiene: autorizaciones indebidas, accesos anónimos o fallos de confidencialidad en la autenticación.
    Ante esto, es recomendable diseñar las interfaces con el objetivo de proteger la información; darles especial atención al cifrado de datos, procesos de autenticación y de verificación. Algunas soluciones sugeridas incluyen:
        - Realizar un análisis en el modelo de seguridad de las interfaces en los servicios contratados.
        - Verificar principalmente la realización del cifrado de datos para así ofrecer un fuerte modelo de control de acceso y autenticación (Chen, Wu, Zhang, Zhang, & Niu, 2012)

3. *Amenaza 3 - Amenazas internas malintencionadas:* Parte del personal de organizaciones deberá interactuar con la información de sus clientes, por lo que inevitablemente se exponen al riesgo de estar trabajando, sin saberlo, con alguien de malas intenciones y que puede hacer uso del acceso a estos datos para beneficio personal. Esto obliga a las organizaciones a contar con estrictos procesos de contratación para asegurarse que no se trate con alguien que busque manipular o robar la información que tiene en su poder.

   Para los proveedores de servicios Cloud el riesgo es doble pues se trata de tanto sus datos como los de múltiples clientes, por lo que deben tener cuidado no solo en la contratación, si no en cualquier proceso donde un empleado interactúe con la data de algún cliente. Existen algunas soluciones a esta problemática, destacando las siguientes:

   - El proveedor de servicios de Cloud Computing debe contar con una estricta área de Recursos Humanos para incluir en los contratos cláusulas confidenciales y legales.
   - Los clientes por su parte deben demandar transparencia total a su proveedor en todos los procedimientos relacionados a la seguridad y manejo de los datos.

4. *Amenaza 4 - Inconvenientes debido a las tecnologías compartidas:* Se refiere a aquellos componentes físicos usados en arquitecturas compartidas sin contar con propiedades de aislamiento. Esto representa mayor peligro para los servicios de tipo IaaS, en estos casos lo más recomendable hacer para evitar inconvenientes es confiar en el hipervisor de virtualización, pues este sirve de intermediario entre los recursos físicos del anfitrión y los del huésped.

   Trabajar con una infraestructura compartida representa un gran beneficio a nivel general, permite superar las dificultades mediante un sistema de defensa sólido, donde se asegure que cada usuario,

no representara ningún impacto negativo en las operaciones de los otros usuarios que trabajen en la misma Nube del proveedor, resumiendo, que ninguno de los clientes activos tengan acceso a ninguna red ajena a la suya.

Históricamente, ha habido casos donde esta amenaza ha representado grandes complicaciones, siendo uno de los ejemplos más sonados los casos de exploits (malware que accedía a los dispositivos del anfitrión). En su momento resonó mucho la Blues Pill de Joanna Rutkowska (al aporte de informática polaca en donde demostró como intestar un malware en el núcleo de Windows Vista mediante el rootkit, un fragmento de software que permite el acceso a privilegios, que ella diseñó denominado Blue Pill). Ante esta amenaza, la CSA propone:

- La instalación y configuración de servicios IaaS debe implementarse con buenas prácticas de seguridad.
- El entorno de los servicios debe ser constantemente monitoreado para que cualquier anomalía sea detectada a tiempo.

5. *Amenaza 5 - Pérdida o fuga de datos:* El entorno manejado por los servicios Cloud hace que tengan un alto número de interacciones, causando que la información almacenada corra el riesgo de ser manipulada de cualquier manera, incluyendo el borrado de datos. Este tipo de pérdidas desencadenaría problemas de carácter económico, legal y operacional. De ahí nace la importancia de los respaldos (backup). Este procedimiento compromete la imagen del proveedor por lo debe garantizar la totalidad de la integridad de los datos. Ante esta problemática, las soluciones sugeridas incluyen:
    - Controlar el acceso implementando de APIs robustas.
    - Protección de los datos en tránsito mediante cifrado
    - Vigilar los datos en sus tiempos de ejecución y realizar un análisis de protección a los mismos.
    - Especificar las políticas de respaldo de información mediante un contrato detallado con el cliente.

- Especificar las políticas de respaldo de información mediante un contrato detallado con el cliente.
- Implementar mecanismos firmes en procesos de generación de claves, almacenamiento y manipulación de información.
- Explicar, mediante el contrato cliente-proveedor, que la destrucción de datos se realizara antes de que algún dispositivo de almacenamiento sea dado de baja.

6. *Amenaza 6 - Secuestro de sesión o de servicio:* se caracteriza por ser una amenaza de nivel superior y se trata de un atacante interviniendo en medio de dos máquinas. De llegarse a dar, el atacante en cuestión puede obtener credenciales, contraseñas, manipular la información, realizar transacciones ilícitas e incluso contactarse directamente con al cliente mediante engañarlo para que se dirija a sitios eliges. Todas estas acciones terminarían afectando al cliente, sino que además dañarían irreparablemente la reputación del proveedor de servicios Cloud.

   Por todo lo mencionado, se recomienda poner especial atención en la Nube, esto incluye aplicar soluciones como:

   - Negar totalmente el compartir credenciales entre servicios y usuarios.
   - Monitorear constante y productivamente de forma que sea posible detectar a tiempo cualquier actividad no autorizada.
   - Asegurar que los procesos de autenticación sean lo más seguros posibles. Para ello se ha trabajado desde 2010 con "Ingeniería de Software y Minería de datos", (SEDM), se trata de la implementación de técnicas de doble factor (adicional al ingreso de una contraseña también se hace uso un código de verificación) (Liou & Bhashyam, 2010).

7. *Amenaza 7 - Riesgos por desconocimiento:* El cliente debe tener ciertos conocimientos de la plataforma, esto incluye ciertos datos básicos de seguridad como: saber que dicha plataforma es

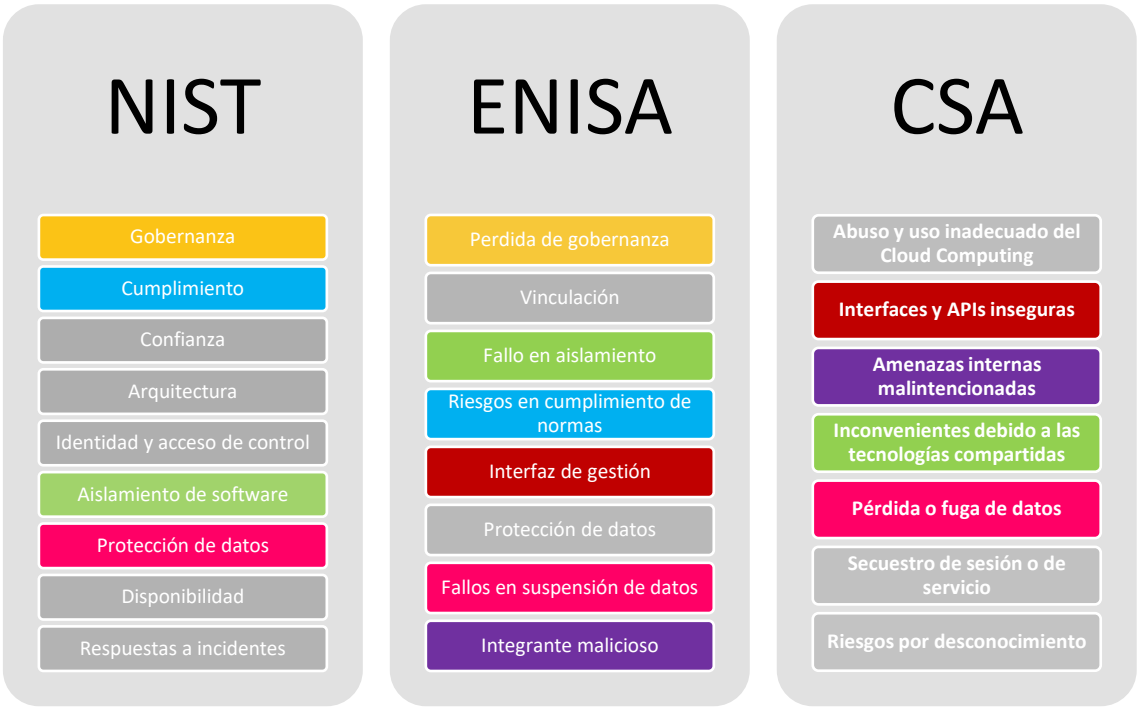
compartida con otros clientes, o el realizar solicitudes directas al proveedor para saber si sus datos están siendo un blanco vulnerable, como lo puede ser el contar con un registro de intentos no autorizados que hayan sido direccionados a la red del cliente.

En este caso algunas de las soluciones sugeridas involucran la participación del cliente siendo estas las siguientes:

- Conocimiento, parcial o total, de los factores técnicos que maneja la infraestructura.
- La implementación de alarmas y monitoreo de las misas al manipular de cualquier forma los datos críticos del cliente.
- Acceder a los logs correspondientes a los sistemas que sean usados por el cliente.

4.5. Comparativa de las tres iniciativas y análisis general

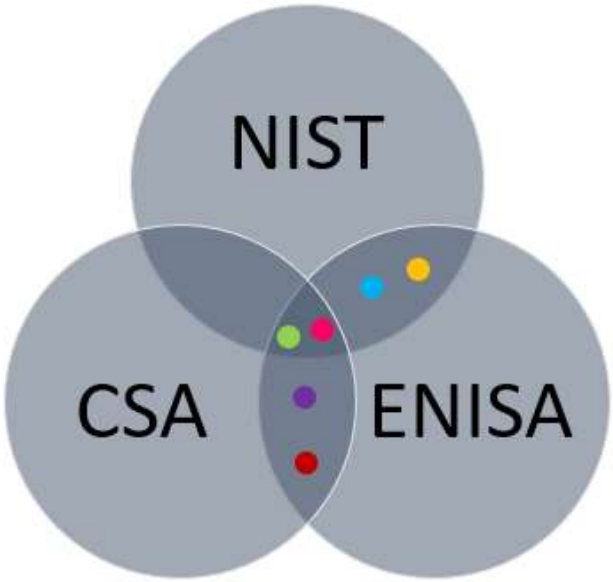
Gráfico 3 Resumen de riegos según las iniciativas NIST, ENISA y CSA



Fuente: Autor, basado en los datos del NIST, ENISA y CSA

La figura anterior cuenta con un código de colores que se usara en el siguiente esquema para representar visualmente la relación entre ellas:

Gráfico 4 Esquema comparativo



Fuente: Autor, basado en los datos del NIST, ENISA y CSA

Gracias a la teoría de conjuntos, es posible ver con facilidad los puntos en común que presentan las iniciativas, como se puede apreciar, las tres iniciativas dan un análisis prioritario a la protección de datos y el aislamiento, a su vez, es interesante observar cómo estos son los únicos puntos en común mientras que ciertos riesgos son aparentemente ignorados en los otros análisis. Por ejemplo, las amenazas internas son un factor que no es considerado en las prioridades del análisis elaborado por el NIST, así como el hecho de que ENISA sea la iniciativa con más puntos en sus intersecciones demostrando ser la alternativa más completa. Este resultado era algo de esperar pues como se especificó en el capítulo 2, la corriente europea es la más completa de todas las mencionadas. En base a los resultados obtenidos, ENISA es el análisis más completo de las tres iniciativas. No obstante, la presente tesis trabaja a la par las recomendaciones técnicas con las legales, estas últimas relacionadas a legislación ecuatoriana. Siendo que ENISA es una institución que rige en Europa, no se tomará como base para la guía de recomendaciones del capítulo 5.

5. Guía para la seguridad en áreas críticas

En el capítulo anterior se observó un análisis de riegos y vulnerabilidades de donde se eligió a CSA como base de la elaboración de la guía de seguridad. Esta decisión se tomó en base a considerar: es la que cuenta con mayor rango de soluciones a amenazas y por la participación de Ecuador en la organización, como se muestra en su capítulo "Cloud Security Alliance Ecuador" (CSA EC, s.f.).

En 2017 Jim Reavis, cofundador y CEO de la CSA, expresó su gratitud al reporte "Security Guidance For Critical Areas of Focus In Cloud Computing V4.0", el cual representó una gran contribución a área de seguridad del Cloud Computing (Mogull, y otros, 2017). Este reporte de asesoramiento se compone de catorce dominios descritos en la siguiente tabla y que comprenderán la base de las recomendaciones en el área técnica:

Tabla 11 Dominios de seguridad en Cloud Computing

Dominio	Definición
1. Arquitectura del Cloud Computing	Marco conceptual general relacionado al Cloud Computing.
2. Gobierno y gestión de riesgos	Gestión enfocada en la Seguridad de la Información dentro de la Nube
3. Legalidades y e-Discovery	Aspectos legales y de descubrimiento electrónico más importantes en la Nube
4. Auditorias y cumplimiento	Revisión de la normativa existe y como se ha adaptado a la Nube
5. Gobernanza de la información	Conceptualización y gestión del ciclo de vida de la información.
6. Plan de gestión y continuidad del negocio	Recomendaciones enfocadas en gestión manejada y del negocio y su respectiva continuidad del negocio y recuperación de catástrofes.
7. Seguridad de infraestructura	Enfoque en redes y equipos que constituyen la base de servicios Cloud.

8. Virtualización y contenedores	Características de máquinas virtuales, contendedores y recomendaciones para evitar problemas de virtualización
9. Notificación, respuesta y subsanación a incidentes	Gestión de incidencias entre el cliente y el proveedor
10. Seguridad de aplicaciones	Revisión en cada capa de una aplicación
11. Seguridad de data y la información	Cifrado de datos y todo lo relacionado a la gestión de claves.
12. Accesibilidad	Funciones relacionadas a la gestión de acceso e identidades.
13. Seguridad como un servicio	Tecnologías enfocadas en la seguridad de la Nube.
14. Tecnologías relacionadas	Tecnologías adicionales que ayudan al desarrollo y operabilidad en la Nube

Fuente: Autor, tomado de la guía de seguridad de la CSA

1. ***Arquitectura del Cloud Computing***

   Se refiere al Cloud Computing de forma general; definiciones, características y modelos de servicios, conceptos ya explicados en los primeros capítulos. Las recomendaciones que surgen en este dominio mecen del modelo de trabajo de Cristopher Hoff (Mogull, y otros, 2017):

   1. Entender las diferencias entre infraestructura tradicional y Cloud Computing y como sus conceptos de abstracción y autonomía afectan a la seguridad.
   2. Familiarizarse con conceptos del NIST y la CSA para referencia de modelo de Cloud Computing y de arquitectura respectivamente.
   3. Evaluar y comparar a los proveedores de servicios Cloud mediante herramientas como la CAIQ (Consensus Assessments Initiative Questionnaire).
   4. Trabajar con herramientas como CSA Cloud Controls Matrix para acceder a la documentación y proyectos de seguridad y requerimientos/controles publicados, y sus responsables.

5. Usar procesos de seguridad para la elección de proveedores, diseño de arquitecturas, detección de brechas e implementación de controles de seguridad y cumplimiento.
6. A nivel de proveedor, publicar la documentación necesaria de sus controles y características de seguridad mediante herramientas como CSA CAIQ.

2. Gobierno y gestión de riesgos

Los involucrados en los servicios Cloud deben manejar un marco de gestión de seguridad que a su vez cubra una gestión de riesgo. Su objetivo de be ser la identificación e implementación de procesos, estructuras y controles que permitan tomar acciones referentes al gobierno y gestión de seguridad informática en la organización.

La gobernanza cuenta con herramientas usadas tanto por los proveedores externos como por desarrolladores internos:

- Contratos: son la clave para extender la gobernanza a asociados del negocio y proveedores.
- Evaluaciones al proveedor: se dan en base a factores como visibilidad financiera, herramientas ofrecidas, entre otros.
- Reporte de cumplimiento: se basa en la documentación ofrecida por el proveedor.

Este dominio contempla algunas recomendaciones tales como:

1. Identificar las responsabilidades compartidas de seguridad y gestión de riesgos según el proveedor y modelo de servicio. Se sugiere implementar prácticas, estándares y regulaciones como IDO/IEC 27017, COBIT 5, CSA, NIST, entre otras.
2. Entender el contrato que se está firmando y como afecta a la gobernanza de la organización.
3. Examinar exhaustivamente las capacidades y parámetros de seguridad dispuestos por el proveedor.
4. Realizar un seguimiento en la organización mediante auditorias para verificar el cumplimiento de requisitos.

5. Trabajar de forma colaborativa entre cliente-proveedor para cumplir los objetivos de la organización de forma paralela a la seguridad de la información.
6. Evaluar los procesos del cliente y proveedor para determinar si son eficientes y óptimos según los parámetros de seguridad de la información.
7. Garantizar el cumplimiento de requisitos de seguridad mediante la participación del personal especializado de la organización en la elaboración del contrato SLA, que como mínimo debe incluir:
    - Planes de manejo de riesgo (con resultados)
    - Estándares y métricas en gestión de seguridad
    - Evaluación de riesgo del proveedor de servicios Cloud
8. Definir parámetros para elegir un proveedor, por ejemplo: el nivel de colaboración con el cliente, disposición de satisfacción de requerimientos de seguridad, entre otros.
9. Realizar un análisis general a la cadena de suministro, especialmente si se pieza deba involucrar a un tercero.
10. Cubrir la seguridad del cliente mediante el desarrollo de los siguientes procedimientos:
    - Administración y análisis de riesgos dirigidos al servicio contratado.
    - Aceptar riesgos residuales que se deriven de la utilización de servicios Cloud.
    - Diseño de planes de respuesta enfocados en la continuidad del negocio y recuperación en caso de catástrofes.

3. Legalidades y e-Discovery

Al hablar de datos, el proveedor no es responsable de todo lo relacionado a estos, especialmente al considerar el apartado legal. Esto último se refiere a que el cliente haga un análisis completo y minucioso de todos los aspectos legales relacionados con los servicios Cloud, se incluyen tres dimensiones principales:

- Funcional: identifica los servicios que directamente se implican legalmente.

- Jurisdiccionales: relacionadas al gobierno y la administración de leyes y normas en Cloud Computing.
- Contractuales: cubren la estructura legal y de seguridad entre cliente-proveedor.

Dentro del área legal, países y continentes han desarrollado regímenes de protección de datos que suelen estar en conflicto entre sí. Como resultado, los proveedores de servicios Cloud que operan en varias regiones tienen problemas para cumplir con las leyes existentes: la ubicación del proveedor, del usuario de la Nube, de la data, los servidores, herramientas/frameworks usados en varias localidades, jurisdicciones legales del contrato entre las partes involucradas, entre otras.

A su vez, los requerimientos demandados a los proveedores incluyen:

- Leyes absolutas adoptadas por varios países cuyo objetivo es proteger la privacidad de los individuos.
- Medidas que garanticen la seguridad en la privacidad de datos.
- Restricciones de la transferencia de datos entre fronteras (se suelen permitir solo si ambas regiones cuentan con un buen nivel de protección a la información personal y al derecho a la privacidad).
- Leyes de seguridad y privacidad regional: se manejan dependiendo de la región, siendo que es un área demasiado extensa, únicamente se describen a nivel general las regiones globales existentes:
    - Asia del Pacifico: destacan por las leyes de Australia, China, Japón y Rusia enfocadas en la protección de información personal definidas en actas como: “The Privacy Act of?” de 1988, la ACL, (Australian Consumer Law), la APPI (Act on the Protection of Personal Information); o entidades como la Cyber Security Law del 2017 o el Roskomnadzor (Regulador Ruso de Protección de Datos).
    - EU (Unión Europea) y el Área económica de Europa: cubren la protección de personas físicas y a la legislación de ciberseguridad mediante reglamentos como la GDPR

(General Data Protection Regulation) (Intersoft Consulting, 2016) y la directiva NIS Directive (Network Information Security Directive) (European Commission, 2020).

- Las Américas: sus leyes se dividen en
  - Estados Unidos se América: sus entidades regulatorias principales son la Federación de Leyes de U.S., Leyes de Divulgación de Infracciones de Seguridad.
  - La región de América Central y del Sur: adoptan leyes de protección de datos, cada una con sus respectivos requerimientos de seguridad colocando en la data la carga de garantizar la protección de datos personales en cualquier lugar especialmente si se transfieren a un tercero.

Por su parte, el e-Discovery se define como el proceso donde una parte contraria obtiene documentos privados. Este proceso se aplica a todo documento que dé lugar a pruebas admisibles, tal cual lo define la regla 26 de la FRCP (Federal Rules of Civil Procedure) (Michigan Legal Publishing Ltd. , 2020).

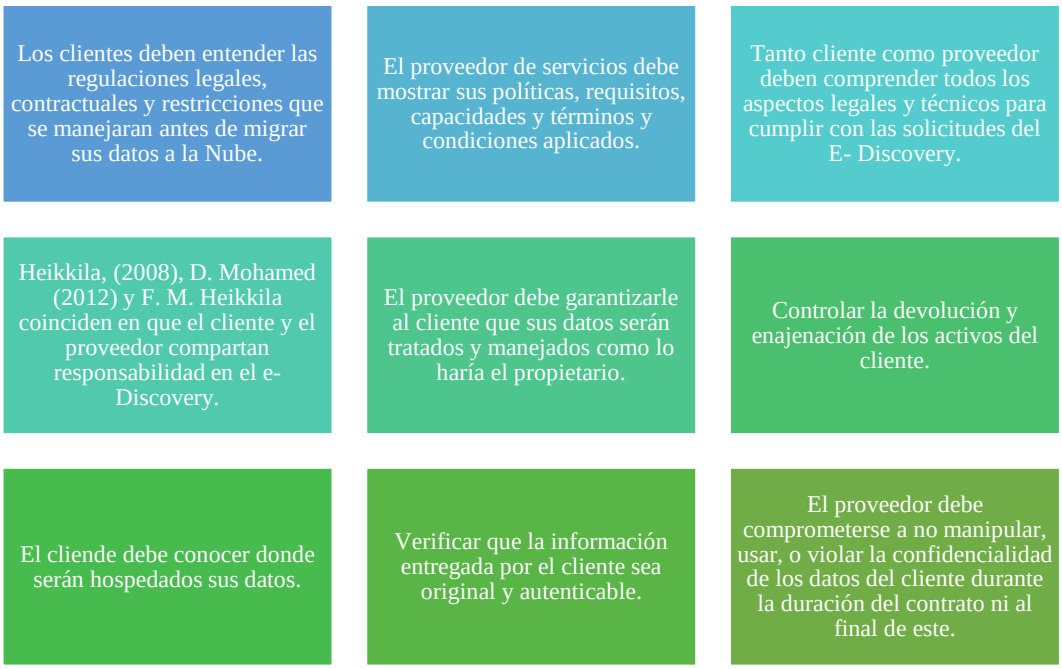
Según la ESI (Electronically Stored Information), los servicios Cloud representan el repositorio más necesitado en procesos de investigación. Esto hace que tanto proveedores como clientes deban planear como identificar todos los documentos que pertenezcan a un caso a fin de cumplir los requisitos impuestos por FRCP 26 con respecto a ESI. En esta área se deben considerar los siguientes factores:

- Posesión, custodia y control
- Entorno y aplicaciones de nube relevantes
- Capacidad de búsqueda y Herramientas de E- Discovery
- Preservación
- Leyes de retención de datos y de mantenimiento de registros
- Colección de data
- Acceso directo

- Producción Nativa
- Autenticación
- Cooperación entre proveedor y cliente en E- Discovery
- Respuesta a una citación u orden de registro
- Entre otros; otras especificaciones y detalles se encuentran en las guías de uso de la ESI (Seeborg, Judge, Soong, & Of Court, 2015)

En términos generales, este dominio se maneja bajo las siguientes recomendaciones:

Gráfico 5 Recomendaciones de Legalidades y e-Discovery



Fuente: Autor, tomado de la guía de seguridad de la CSA

4. Auditorias y cumplimiento

El cumplimiento se encarga de validar el conocimiento y acatamiento de las obligaciones de la organización. Este proceso evalúa el estado de la empresa enfocándose principalmente en los riesgos y potenciales riesgos en caso de incumplimiento normativo. Por su parte las auditorías representan una herramienta para probar o refutar el cumplimiento normativo y como una forma de respaldar las decisiones de riesgos de incumplimiento.

En la Nube el cumplimiento es un modelo de responsabilidad compartida, la división de etas responsabilidades se define mediante contratos, asesorías y especificaciones de los requerimientos de cumplimiento.

En las auditorías, se manejan mecanismos que documenten el cumpliendo con requerimientos externos o internos, estos reportes incluyen una lista de los problemas, riesgos y recomendaciones de remediación. La mayoría de las organizaciones son sujetos aseguran el cumplimiento mediante una mezcla de auditorías internas y externas.

El que una organización decida usar servicios en la Nube demanda de un ajuste en procedimientos sistemas y normas de esta. Hasta hace unos años, este proceso de cambio solía ser más complicado pues la empresa debía alienarse con los requisitos demandados por el proveedor. Actualmente, es un problema menos común, pues se trata de una tecnología bastante normalizada y también por las consideraciones que se aplicaron desde la aparición de la mencionada problemática donde destacan:

1. Dividir responsabilidades entre organización y servidor en base al cumplimiento de normas en un sistema.
2. Apoyar al cliente, mediante evidencias expuestas por el proveedor, en el cumplimiento normativo de dicha organización.
3. Actuar como mediador en autorías dadas entre una normativa empresarial y el proveedor.

El cumplimiento normativo resumen su análisis y propósito en:

1. Éste, sus auditorías y asesorías deben ser procesos continuos.
2. Los clientes deben entender sus obligaciones antes de migrar a la Nube.
3. Asegurar el cumplimiento de las obligaciones del proveedor.
4. Especificar en contrato el derecho al cliente de auditar al proveedor.
5. Determinar si la introducción de servicios Cloud a la organización afectara su normativa, de ser así, se debe definir un nuevo alance.
6. Identificar y probar los controles seguridad de cumplimiento del proveedor.

7. Determinar el nivel de impacto que una normativa implementada en la infraestructura del proveedor tendría.
8. Analizar el impacto que causaría el cambio de requisitos, procedimientos y políticas, el traslado de información y aplicaciones al Cloud. Independientemente del grado de cambio, se debe documentar cómo se adaptó el cumplimiento de la norma.
9. Elegir, en caso de recurrir a auditorias, a personal especializado y experimentado en el área de séricos Cloud.
10. Solicitar al proveedor una certificación de auditoria (como la ISO 27001 o SAS 70 Type II), o el proyecto de una futura certificación.

5. Gobernanza de la información

Mogull & otros (2017) definen la gobernanza de información como el uso de datos con políticas organizacionales, estándares estrategias/regulaciones y objetivos de negocio.

Al tener los datos en la Nube hay varios factores que pueden influir la información subida y su gobernanza, como lo son el almacenamiento en infraestructura compartida o responsabilidades de seguridad compartidas. Los clientes de la Nube deben incluir a su proveedor en su plan de gobernanza, pues esta entidad maneja las limitaciones juridiciales, regulaciones, políticas de privacidad y la destrucción y removida de datos (Mogull, y otros, 2017).

Dado que la gobernanza de la información es un área muy amplia, se tratarán únicamente los dominios afectados por el uso de servicios Cloud:

Tabla 12 Dominios de gobernanza de la información

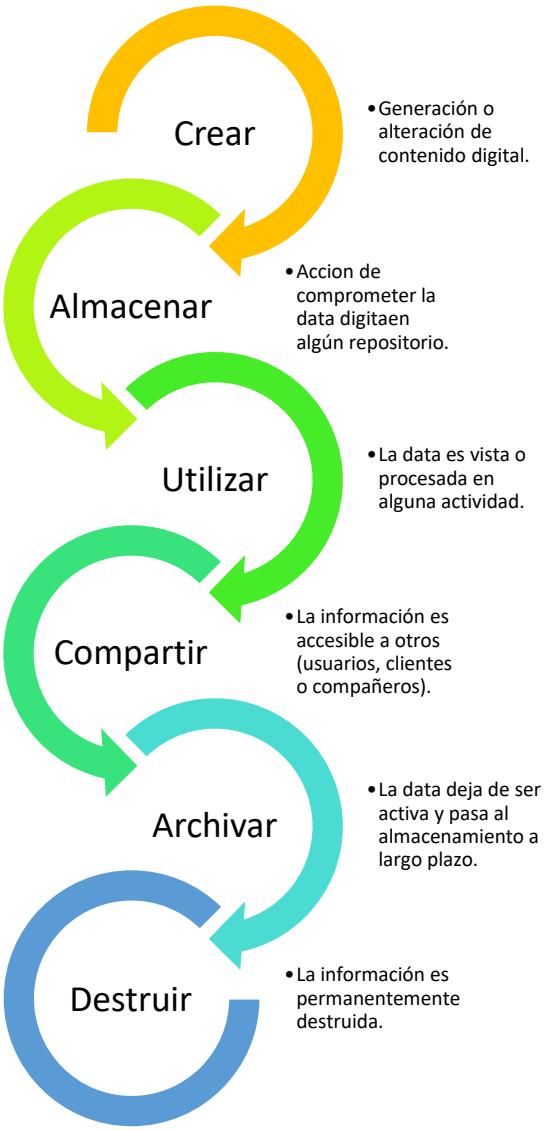
Dominios de Gobernanza de la Información	
Clasificación	En caso de contar con un programa de clasificación de data este debe ser ajustado para el Cloud Computing.
Políticas de gestión	Depende del modelo Cloud con el que se vaya a trabajar, no obstante, en todos los casos es necesario determinar la información,

	productos/servicios que estarán en la Nube y los requerimientos de seguridad que necesitan.
Políticas de localización y jurisdicción	El proveedor debe respetar y cumplir con los requerimientos de localización y jurisdicción para evitar conflictos futuros.
Autorización	Realizar únicamente los cambios necesarios para el manejo de autorizaciones en Cloud Computing sin que estos impacten al ciclo de vida.
Propiedad	La organización siempre es dueña de la información y esto no puede cambiar ni durante ni después del uso de servicios Cloud.
Custodia	El proveedor pasa a ser quien custodia la información.
Privacidad	Es el resultado de los requerimientos, acuerdos y obligaciones contractuales que se tengan con los clientes.
Control contractual	Herramienta legal que permite extender los requerimientos de gobernanza, en este caso, al proveedor de servicios.
Control de seguridad	Herramientas usadas para implementar la seguridad de data y cambian significantemente al trabajar con servicios Cloud.

Fuente: Autor, tomado de la CSA

La seguridad de la información a nivel general se centra en la protección de datos, surgen dos conceptos en base a este objetivo, siendo el primero el ciclo de vida de la información:

Gráfico 6 Ciclo de vida de la información



Fuente: Autor, basado en la definición de la guía de seguridad de la CSA

Las fases se componen de funciones de lectura, procesamiento y almacenamiento de datos. A continuación, se muestra el mapeo de estas en cada fase:

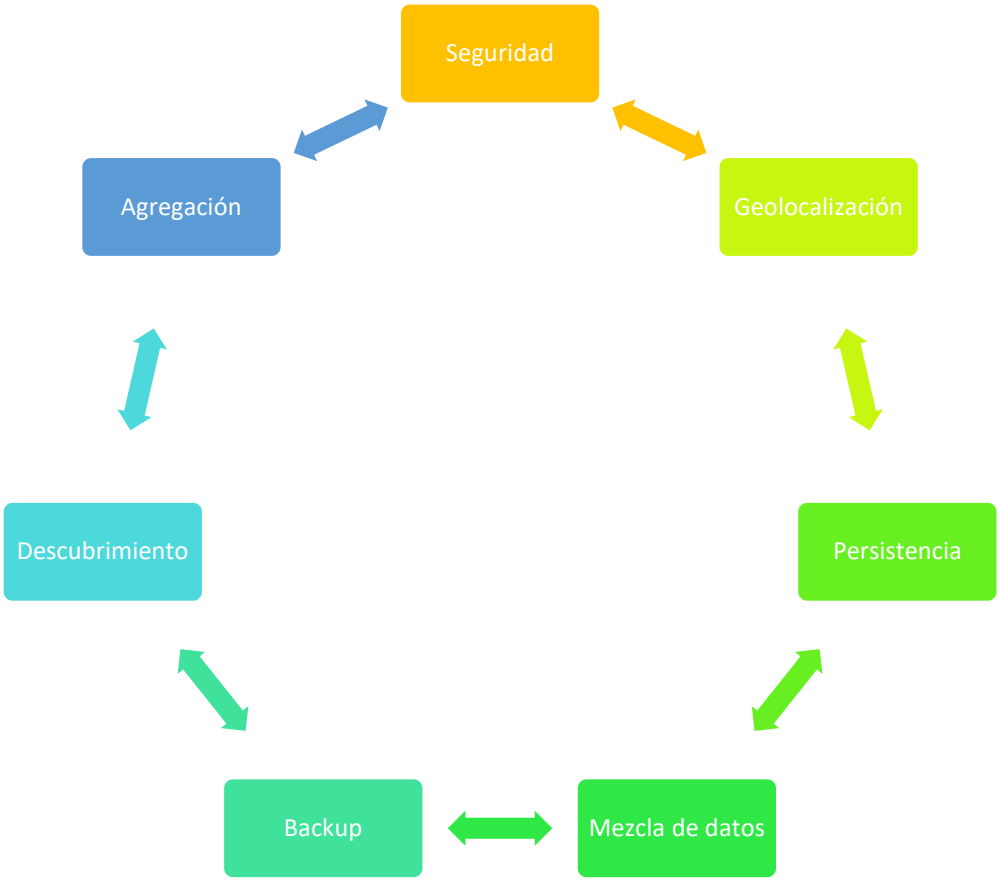
Tabla 13 Mapeo de funciones en fases del ciclo de vida de la información

	Crear	Almacenar	Utilizar	Compartir	Archivar	Destruir
Leer	x	x	x	x	x	x
Procesar	x		x			
Almacenar		x			x	

Fuente: Autor, tomado de la CSA

Por su parte, el segundo aspecto corresponde al del ciclo de vida de datos:

Gráfico 7 Ciclo de vida de datos



Fuente: Autor, basado en la definición de la CSA

- Seguridad: engloba lo referente a la confidencialidad, integridad, autenticidad y autenticación de los datos.
- Geolocalización: en el contrato se deben limitar las ubicaciones permitidas para el almacenamiento de datos, este punto se refiere a la evidencia de que esto se cumpla mediante garantías.
- Persistencia: en caso de darse la eliminación de datos, esta debe ser absoluta y efectiva.
- Mezcla de datos: la mezcla de datos entre clientes es algo que no debe ocurrir en ninguna fase con los datos sensibles.
- Backup: incluyen planes de recuperación de datos y se refiere a la restauración de estos, factor que complementa su disponibilidad.

- Descubrimiento: se relaciona con la restauración de datos, en este caso a la garantía de que los datos son en su totalidad, recuperables.
- Agregación: relacionada con la inferencia, se refiere a la implementación de técnicas y prácticas que le garanticen al cliente la protección de sus datos confidenciales de cualquier trasgresión.

Con relación a estos ciclos, las recomendaciones sugeridas incluyen:

1. Determinar los requerimientos de gobernanza de la información antes de transaccionar a la Nube.
2. Asegurar que las políticas y prácticas de gobernanza manejadas en la organización se extenderán a la Nube.
3. De ser necesario, restructurar el enfoque utilizado en la organización.
4. Conocer el tipo de controles aplicados en el ciclo de vida de datos.
5. El cliente debe tener conocimiento sobre la geolocalización de sus datos, especialmente con aquellos confidenciales.
6. En caso de que el proveedor tenga algún tipo de problema, deberá dar un informe a su cliente con respecto a lo ocurrido.
7. El cliente debe establecer los usuarios y sus privilegios, que tendrán acceso a los datos almacenados en la Nube.
8. Zhang, H., DeCleene, B., Kurose, J., & Towsley, D. han establecido la “Denegación por defecto”, una política establecida por el proveedor de servicios.
9. El contrato debe mencionar sentencias que se aplicarán al proveedor en el caso de darse alguna violación a los datos.
10. Deben existir y ejecutarse pruebas de medición a los procesos de backup.

6. Plan de gestión y continuidad del negocio

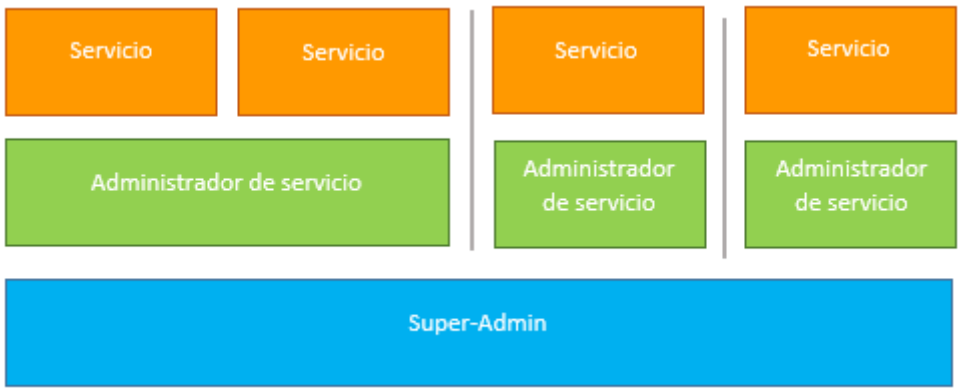
El plan de gestión se refiere a las interfaces utilizadas para el manejo de archivos en la Nube. Esta gestión controla y configura la meta-estructura (protocolos y mecanismos que proveen la interfaz entre la infraestructura y las otras capas) y que a su vez es parte de la infraestructura.

El plan de gestión es ejecutado pragmáticamente mediante consolas web (mediante DNS - Domain Name Server-) y APIs que mantienen juntos todos los componentes de la Nube haciendo posible su orquestación. Usualmente, los proveedores ofrecen también SDKs (Software Development Kits) y CLIs (Line Interfaces) a fin de facilitar aún más la integración de las APIs.

El plan de gestión va de la mano con IAM (Identity and Access Management), al ser lo que cubre los procesos de identificación, autenticación y autorización.

La plataforma del cliente se organiza mediante niveles de administración, cada uno tiene acceso y control a ciertas partes del servicio, en su base se tiene "root" o "super-admin" quien representa la entidad con privilegios totales y que tiene acceso a todo el servicio, por lo mismo, debe ser la que más restricciones tenga y la que menos se use.

Gráfico 8 Ejemplo de gestión en la Nube



Fuente, Autor basado en las descripciones de CSA

En la Nube el cliente es el responsable únicamente de la configuración de las partes que el proveedor le ha asignado mientras que la entidad se encarga de todo lo demás. El manejo de la gestión es un área demasiado amplia, por lo que únicamente se describirán los cinco factores básicos según lo establecido en la cuarta versión de Guía de Seguridad de la CSA:

- Perímetros de seguridad: protección de ataques contra el plan de gestión, incluye defesas aplicadas en todos los niveles de servicio.

- Autenticación del cliente: debe ser provista por estándares, mecanismos seguros.
- Autenticación interna y paso de credenciales: el personal de la organización debe seguir mecanismos de seguridad al momento de contactar o relacionarse de cualquier forma con el plan de gestión. El proveedor debe maneje esta fase mediante estándares, principalmente la MFA (Autenticación de múltiples factores).
- Autorización y derechos: los clientes y administradores recurrirán a sus derechos especificados en los contratos en el caso de alguna irregularidad en la autorización o privilegios.
- Registro, monitoreo y alerta: deben ser procesos extremadamente robustos, tanto para el cliente como para el administrador, a fin de cada uno pueda acceder únicamente a las partes del servicio que le correspondan.

Este dominio cubre también la continuidad de negocios y recuperación de desastres, abreviado BC/DR por sus siglas en ingles. La CSA (2017) establece que como mínimo la BC/DR debe cubrir las siguientes entradas lógicas: meta-estructura, infraestructura de Software-Definido, infraestructura, Infoestructura y estructura de aplicación

Se cubren tres aspectos básicos de la seguridad: el modelo tradicional, continuidad de la organización y planes de recuperación en caso de catástrofes. Adicionalmente, también se da énfasis a futuros cambios y a su actualización por lo que surgen las siguientes consideraciones:

1. Demandar a proveedor que limite el acceso a su información a la menor cantidad de personal posible.
2. Implementar estrictas practicas se seguridad.
3. De ser posible, revisar las instalaciones del proveedor.
4. Analizar los planes de recuperación ofrecidos por el proveedor.
5. Identificar las interdependencias presentes en la infraestructura.
6. Solicitar al proveedor toda la documentación relacionada a los controles y estándares de seguridad utilizados.

7. Revisar el plan de continuidad del proveedor y asegurar que se encuentre certificado por estándares relacionados a la rama de negocios manejada por la organización.

Las recomendaciones de este dominio se dividen en dos grupos:

Tabla 14 Recomendaciones generales del Dominio 7

Seguridad de planes de gestión	Continuidad del negocio
1. Determinar que exista una sólida seguridad perimetral en las entradas de enlace de APIs y consolas web. 2. Implementar robustos procesos de autenticación y MFA. 3. Mantener un escrito control en las credenciales de los administradores principalmente en el "root". 4. Trabajar con varias cuentas separadas y no únicamente con la de super-admin. 5. Implementar pervigilios mínimos a las cuentas que acceden a la meta-estructura. 6. Reforzar el cumplimiento constante de MFA.	1. Determinar una arquitectura para escenarios de fracaso. 2. Adoptar un enfoque basado en riesgos. 3. Acordar con el proveedor un diseño de alta disponibilidad. 4. Aprovechar la mayor ventaja posible de las características y especificaciones ofrecidas por el proveedor. 5. Considerar los factores de cruce de localidades y los costos que esto puede representar. 6. Estar preparado para fallas relacionadas con la interrupción al proveedor de la Nube.

Fuente, Autor basado en las descripciones de CSA

Si no se cumplen las recomendaciones descritas se sugiere un cambio de proveedor pudiendo ser por varios motivos: aumento de costos, una decaída en la calidad de los servicios, entre otros. Sin embargo, un cambio de proveedor podría ser tediosos y costoso, pero se garantizaría la continuidad del negocio. A fin de optimizar recursos de tiempo, dinero y esfuerzo, se recomienda:

1. Especificar en el contrato el proceso que se seguirá en migraciones.
2. Determinar el tamaño de los datos.
3. Documentar lo necesario para facilitar el proceso de migración (arquitectura y configuraciones usadas con el anterior proveedor).
4. En caso de trabajar con servicios IaaS, conocer como capturar imágenes de máquina virtual hacia el nuevo proveedor.
5. Detectar las dependencias de hardware.
6. Exigir al antiguo proveedor todos los registros del sistema que se encontraba funcionando en la Nube.
7. Consultar con el antiguo proveedor si fuese posible restablecer el contrato.
8. Determinar la compatibilidad de las APIs utilizadas en el antiguo contrato con el actual.
9. Respaldar constantemente la información en copias de seguridad.
10. Entregar registros y copias de seguridad al nuevo proveedor para que sirvan de evidencia en caso de auditorías.
11. Demandar al nuevo proveedor la realización de pruebas, y entrega de resultados, a las aplicaciones actuales.

7. Seguridad de infraestructura

Representa la base de la seguridad en la Nube; cuentan con dos capas de infraestructura:

- Recursos fundamentales que crean la Nube en conjunto: redes, almacenamiento, y computo lógico/físico usado en los recursos de servicios Cloud.
- Infraestructura virtual manejada por usuarios: el computo, redes, etc., que se usa de los recursos disponibles.

Actualmente, los servicios Cloud se manejan principalmente bajo alguna de las siguientes categorías:

- VLAN (Virtual Local Area Networks): diseñadas para un solo inquilino. Por sí solas, no se las usa para virtualización o seguridad en la Nube.

- SDN (Software Defined Networking): representan una capa de abstracción más completa y desacoplan el plano de control en redes de datos, lo que permite abstraer la creación de redes de limitaciones tradicionales de una LAN (Local Area Networks). También se caracteriza por definir ventajas de seguridad como un sencillo aislamiento o firewalls flexibles.

Dado que los clientes de los servicios Cloud operan a un nivel virtual, es necesario recurrir a la ayuda de dispositivos virtuales. No obstante, esto representa algunas preocupaciones, como, por ejemplo:

- Cuellos de botella por tráfico de datos.
- Aumento de recursos en la Nube y por ende de costos.
- Posibles problemas con el proveedor debido a licencias de uso.
- Los componentes de aplicaciones en la Nube suelen distribuirse aumentando la resiliencia, alterando el diseño de las políticas de seguridad.

Ante esta problemática la CSA introduce la microsegmentación que ejecuta redes más pequeñas y aisladas sin incurrir en costos de hardware adicionales. (CSA, 2020) y busca proporcionar el acceso dinámico a recursos y mejorar la seguridad de red.

Por su parte, la infraestructura comprende el concepto de seguridad de la carga de trabajo. Dependiendo de los niveles de aislamiento y segregación, existen varios tipos de abstracción, siendo los más comunes:

- Máquinas virtuales.
- Contenedores.
- Cargas de trabajo basadas en plataforma.
- Computación sin servidor (el usuario no administra ningún equipo virtual o hardware subyacente de la Nube, en su lugar, accede únicamente a sus funciones expuestas).

Existe una variable de máquinas virtuales denominadas inmutables, que se caracterizan por no aplicar parches o realizar cambios en una carga de trabajo que este en ejecución. Este tipo de cargas de trabajo demandan ciertos requisititos y representa algunos beneficios de seguridad:

Tabla 15 Requisitos y beneficios de máquinas virtuales inmutables

Requisitos	Beneficios
• Constante creación de imágenes y automatización en actualizaciones de soporte. • Las pruebas de seguridad deben estar integradas en la creación de imágenes y procesos de actualización. • Mecanismos que deshabiliten los inicios de sesión y restrinjan los servicios antes de desarrollar y usar imágenes en la producción de máquinas virtuales.	• Permite deshabilitar inicios de sesión remotos, evitando cambios no consistentes. • Rapidez al implementar versiones actualizadas. • Facilidad de deshabilitar servicios y aplicaciones/procesos. • Aumento de seguridad

Fuente, Autor basado en las definiciones de CSA

Finalmente se muestran algunas recomendaciones más específicas divididas en:

Tabla 16 Recomendaciones adicionales de Dominio 7

Infraestructura a nivel general
a. Conocer la infraestructura del proveedor o plataforma. b. En modelos de seguridad compartida, el proveedor debe garantizar que las capas físicas subyacentes son seguras. c. Revisar las certificaciones y atestaciones de cumplimiento del proveedor.
Redes
a. Trabajar con SDN si se diera la oportunidad y usar capacidades para incrementar el asilamiento b. Implementar restricciones en los firewalls Cloud. c. Restringir, en la manera de lo posible, el tráfico entre cargas de trabajo en una misma subred virtual.

d. Reducir la dependencia de los dispositivos virtuales limiten el rendimiento.
Computo/cargas de trabajo
a. Aprovechar las cargas de trabajos inmutables cada que se presente la oportunidad. b. Mantener controles de seguridad para largas cargas de trabajo en ejecución. c. Almacenar los registros externos de las cargas de trabajo. d. Acatar las limitaciones del proveedor en evaluaciones de vulnerabilidades y penetración.

Fuente, Autor basado en las definiciones de CSA

8. Virtualización y contenedores

Se entiende como virtualización a la abstracción de recursos entre un equipo físico y el sistema operativo de una máquina virtual, dando como resultado una versión virtual de un dispositivo o servicio (Niño Vásquez, 2020). En Cloud Computing, y tal como Niño (2020) demuestra, esto representa varias ventajas:

- Incorporar rápidamente nuevos recursos en los servidores.
- Reducir considerablemente los cotes de consumo, espacio y de hardware.
- Trabajar con una administración simple, global y centralizada.
- Facilitar la clonación y copia de sistemas.
- Aislamiento (el fallo de una máquina virtual no afecta a otras).
- Disminuir tiempos de parada.
- Posibilidad de migrar en cliente sin perder el servicio.
- Balance dinámico entre máquinas virtuales y servidores físicos, lo que representa un consumo homogéneo y optimizado de recursos.

Pese a su alto grado de satisfacción general, también hay el riesgo aumentar el grado de inconveniencias a la seguridad (si ya se tenía problemas, estos migrarán a la Nube). Los problemas más relevantes son:

- Falta de procedimientos de planificación y ejecución en el proceso de despliegue rápido de una máquina virtual.
- Manejar dispositivos de red y servidores en el mismo entorno, pues puede complicar el uso de software de gestión.
- Fácil extracción de los datos de una máquina virtual.
- Errores en la clonación de máquinas virtuales.
- Fallas de configuración en el servidor físico de las máquinas virtuales lo que afectaría a varios clientes.

Las categorías virtualización en la Nube destacan por:

- Computo: principalmente máquinas virtuales.
- Responsabilidades del proveedor: garantiza el aislamiento, asegurar la infraestructura de virtualización y dar soporte de uso seguro a los usuarios Cloud.
- Responsabilidades de usuario: especificaciones que el usuario puede direccionar en sus controles de seguridad (configuraciones de seguridad, monitoreo, inicio de sesión, gestión de activos de imagen y uso de hosting dedicado).

Las redes virtuales también forman parte de este dominio; se ejecutan en redes físicas y permiten una modificación profunda del comportamiento de la red afectando a muchos procesos y tecnologías de seguridad (Mogull, y otros, 2017), principalmente a:

- Monitoreo y filtrado.
- Gestión de infraestructura.
- Redes superpuestas (tecnología de virtualización de WAN - wide area network- que crear redes que abarcan redes base).

Este dominio también describe a los contenedores, (entorno de ejecución virtual que trabaja con un kernel compartido y un espacio de usuario aislado (Scheepers, 2015)), sus componentes y características. Se tiene:

- El entorno de ejecución
- Un controlador de orquestación y programación
- Un repositorio para las imágenes o código del contenedor

Independientemente de la plataforma, se debe garantizar la seguridad en:

- La infraestructura física subyacente.
- El plano de gestión (orquestador y el programador).
- El repositorio de imágenes.
- Las tareas/código ejecutadas en el contenedor (se requiere de una configuración segura tanto del entorno como de las imágenes).

En base a lo expuesto, las recomendaciones de este dominio se dividen en:

1. Para proveedores:

Tabla 17 Recomendaciones de seguridad en el Dominio 8

<table>
<tr><th colspan="3">A nivel general:</th></tr>
<tr><td colspan="3">• Asegurar cualquier infraestructura física subyacente usada.
• Garantizar el aislamiento de seguridad a todos los usuarios.
• Brindar las capacidades de seguridad necesarias en las capas de virtualización para que los usuarios aseguren sus activos.
• Defender las plataformas de ataques internos o externos.</td></tr>
<tr><th colspan="3">A nivel de prioridades especificas:</th></tr>
<tr><th>Computo</th><th>Redes</th><th>Almacenamiento</th></tr>
<tr><td>• Implementar hipervisores seguros y actualizarlos mediante gestión de parches.
• Aislar las máquinas virtuales mediante configuraciones de los hipervisores.
• Implantar procesos y controles técnicos que restrinjan el acceso de administradores a</td><td>• Proteger las redes subyacentes; detectar y prevenir cualquier ataque físico o virtual.
• Garantizar el aislamiento de redes virtuales, incluso las controladas por el consumidor (a menos que se solicite lo contrario).
• Implementar políticas y controles internos que eviten la alteración no</td><td>• Cifrar el almacenamiento físico subyacente para evitar la exposición de los datos.
• Evitar el acceso no autorizado a datos mediante el aislamiento de cifrado en las funciones de</td></tr>
</table>

máquinas virtuales en ejecución.	autorizada de redes de consumidores de la supervisión del tráfico.	gestión de datos.

Fuente, Autor basado en las descripciones de la Guía de Seguridad de la CSA

2. Para usuarios:
    - Comprender las capacidades de aislamiento de seguridad en la plataforma elegida y su sistema operativo subyacente.
    - Configurar los servicios de virtualización según lo establecido por el proveedor.
    - En el caso de los contenedores:
        - Aislarlos y agruparlos según a la seguridad de los hosts.
        - Asegurar su gestión y programación.
        - Implementar controles de acceso basados en roles y fuertes procesos autenticación.

9. *Notificación, respuestas y subsanación ante incidentes*

Al gestionar servicios en la Nube se debe contar con protocolos de respuesta manejados por estándares que reflejen cualquier cambio realizado. Estos planes deben definir las responsabilidades, y procesos asignados a cada parte (cliente-proveedor) del mismo.

Para el proveedor una de sus principales obligaciones es asignar medidas de seguridad a cada proceso para prevenir posibles brechas de seguridad.

Debido a los diferentes tipos de incidencias existentes, se formó la SOC (Centro de Operaciones de Seguridad), grupo que proporciona información las organizaciones optimicen sus procesos de detección, análisis y mitigación de vulnerabilidades (Alien Vault, 2015).

Este dominio se centra en el ciclo de vida de la Incidencia a Respuestas definido en el documento NIST 800-61rev2 (Cichonski, Millar, Grance, & Scarfone, 2012):

Gráfico 9 Ciclo de vida de la respuesta a incidentes según el NIST

Fuente, Autor basado en publicaciones del NIST

- Preparación:
  - Procesos para gestionar los incidentes.
  - Comunicaciones e instalaciones del gestor.
  - Documentación interna.
  - Entrenamiento de identificación.
  - Evaluar la infraestructura (escaneo proactivo, supervisión de red, análisis de vulnerabilidad y evaluaciones de riesgo)
- Detención y análisis:
  - Contar con alertas que registren cualquier irregularidad incluyendo el comportamiento de los usuarios.
  - Validar cualquier alerta de registrada.
  - Analizar el ataque según una línea de tiempo.
  - Determinar que alcance tendría la posible pérdida de datos.
  - Asignar a alguien la tarea de comunicar el estado de contención y recuperación en caso de un incidente
- Contención, erradicación y recuperación:
  - Contención; desconexión de sistemas y consideraciones de la disponibilidad del servicio en el caso de pérdida de datos.
  - Erradicación y recuperación; limpieza de los dispositivos comprometidos y su puesta en funcionamiento nuevamente. Maneja controles de seguridad y la recolección de pruebas.
- Post-Mortem: ¿Qué se puedo hacer mejor? ¿el ataque se pudo detectar antes? ¿las estrategias implementadas necesitan cambiar?

Mogull y otros analizan el impacto de la Nube en cada fase del ciclo dando:

Tabla 18 Recomendaciones generales en las fases del ciclo de respuestas incidentes

Preparación:

- SLA y gobernanza: las responsabilidades y roles entre proveedor y cliente deben ser claramente definidos.
- En cada modelo de servicio los datos/registros disponibles varían, esto es algo que debe ser documentado desde un inicio para evitar malentendidos a posteriori.
- Kit de salto al Cloud: corresponde a herramientas usadas para navegación remota.
- Diseño del entorno de la Nube: debe contar con una configuración y arquitectura que apoye las estrategias de respuesta (habilitar registros de APIs, servidores inmutables, usar mapas de pila, realizar modelos y simulaciones de ataques).

Detención y análisis:

- Capturar cualquier metadato en el momento de a alerta.
- "Pausar" la máquina virtual si el proveedor lo soporta.
- Capturar el almacenamiento de la máquina virtual.
- Determinar el alcance de la plataforma (análisis de flujo de redes, datos de configuración, registros de acceso a datos y del plano de gestión).
- En caso no usar arquitectura basada en PaaS, implementar una correlación adicional entre la plataforma y cualquier registro autogenerado de aplicación.

Contención, erradicación y recuperación:

- Es posible (especialmente en IaaS) reconstruir un entorno desde cero e incluso aislar a un atacante sin tener que eliminarlo inmediatamente.

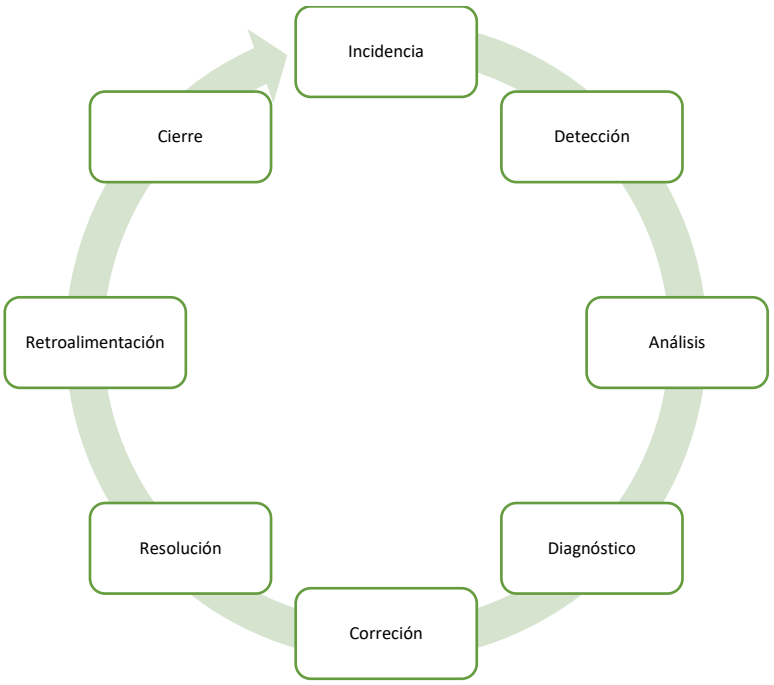
Post-Mortem:

- Analizar que funciono y que, en no, determinar las limitaciones colectadas por la data y el direccionamiento que se tomará.

Fuente, Autor basado en las publicaciones de Mogull (Mogull, y otros, 2017)

Por último, se tiene el siguiente ciclo de vida de incidencias:

Gráfico 10 Ciclo de vida de incidencias



Fuente: Autor basado en la definición del ciclo de vida de incidencias

En base a lo expuesto las recomendaciones descritas son:

1. Basar las expectativas de configuración y SLAs en un buen entendimiento de las funciones/responsabilidades.
2. Establecer vías de comunicación adecuadas con el proveedor.
3. Entender el contenido y formato de los datos suministrados por el proveedor y evaluar que los datos forenses cumplan los requisitos.
4. Supervisión continua y monitoreo de los "sin servidores".
5. Almacenar y/o copiar las fuentes de datos en ubicaciones que se mantengan disponibles incluso en incidentes.
6. Aprovechar la automatización y orquestación para acelerar los procesos de respuesta, la contención y la recuperación.
7. Planificar el enfoque de detección y gestión de incidentes en el plan de respuesta de la empresa.
8. Para el ciclo de vida incidencias surge la siguiente tabla:

Tabla 19 Recomendaciones adicionales a la respuesta a indecencias

Para el proveedor:	Para el cliente:
Permitir al cliente acceder a la plataforma en caso de análisis forenses o de incidentes.	Revisar frecuentemente el historial de incidencias.
Detectar los tipos de incidencias, frecuencia y nivel de peligro para elaborar estrategias de mitigación, soporte y recuperación.	Leer las garantías ofrecidas para usarlas en procesos de soporte.

Fuente: Autor, tomado de la CSA

10. Seguridad de aplicaciones

La seguridad requiere de cambios en las prácticas, procesos y tecnologías que no fueron diseñados para la Nube. Según CSA, esto se puede resumir en la siguiente tabla:

Tabla 20 Oportunidades y Retos de la seguridad de aplicaciones en la Nube

Oportunidades	Retos

• Mayor seguridad de base de línea • Capacidad de respuesta • Entornos aislados • Máquinas virtuales independientes • Elasticidad • Interfaz unificada • DevOps (metodología que automatiza el despliegue de aplicaciones)	• Visibilidad limitada • Mayor alcance • Menor transparencia. • Cambio en modelos de amenaza

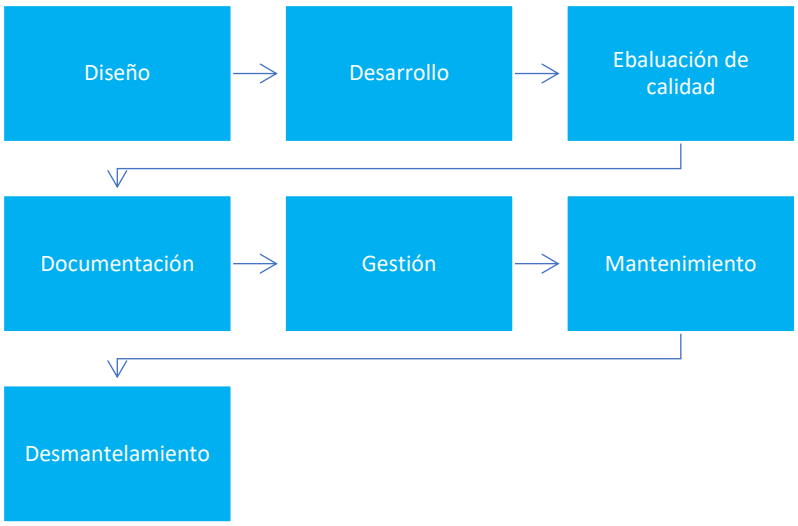
Fuente, autor basado en las descripciones de la CSA

Dada la naturaleza de las aplicaciones, su seguridad se desglosa en:

- Ciclo de vida del desarrollo de software seguro (SSDLC)
- Diseño y arquitectura
- DevOps e integración continua/despliegue continuo (CI/CD).

A fin de estar lo más preparado posible para la detección y mitigación de cualquier vulnerabilidad, se describe el ciclo de desarrollo de software:

Gráfico 11 Ciclo de desarrollo de software



Fuente: Autor basado en la definición del ciclo de vida de software

A lo largo de estas fases se pueden encontrar varas amenazas, algunas de las más destacadas incluyen:

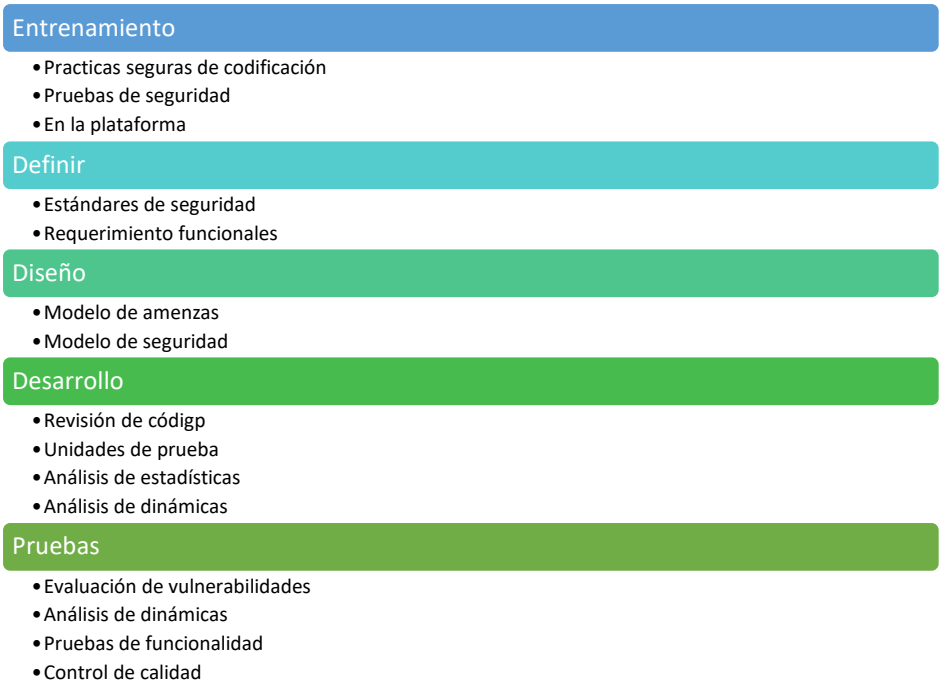
- Spoofing: tomar la identidad de otro usuario.
- Manipulación: alteración de datos en la fase de tránsito.

- Repudiación: negación al origen de una transacción.
- Revelación: dar a conocer datos sin autorización alguna.
- Denegación: si se da en un servicio alterará la disponibilidad.
- Cambio en los privilegios: alguien asume un rol que no le corresponde.

En base a este ciclo, el SSDLC sugiere el uso de frameworks (Microsoft's Security Development Lifecycle, NIST 800-64, ISO/IEC 27034, entre otros).

Existen cinco fases en el diseño y desarrollo seguro de aplicaciones, todas afectadas por el Cloud Computing:

Gráfico 12 Fases en el diseño y desarrollo seguro de aplicaciones



Fuente, autor basado en las descripciones de la CSA

El impacto más notorio del Cloud se encuentra en:

- Evaluación de vulnerabilidad: ejecución de evaluaciones completas contra imágenes o contenedores.
- Pruebas de penetración: la CSA recomienda usar pruebas experimentadas en la plataforma que aloja a la aplicación e incluir a los desarrolladores y administradores en las pruebas y permitir.

- Seguridad de la red de distribución: pueden apoyarse en infraestructura inmutable, automatización de pruebas y registro exhaustivo de la aplicación.
- Impacto de la infraestructura como código inmutable: su uso y despliegues inmutables mejoran significativamente la seguridad.

En base a todo lo expuesto, nacen las siguientes recomendaciones:

Gráfico 13 Recomendaciones del Dominio 11

Fuente, autor basado en las descripciones de la CSA

11. Seguridad de data y la información

En Cloud las tecnologías de virtualización más comunes en almacenamiento incluyen:

- Almacenamiento de objetos: se da mediante mecanismos específicos de la plataforma (usualmente a través de APIs).
- Almacenamiento por volumen: en esencia es un disco duro virtual de instancias/máquinas virtuales.
- Base de datos: se admiten varios tipos, comerciales o propietarias, y pueden ser relacionales o no relacionales (incluyen NoSQL).

- Aplicación/plataforma: como ejemplos se tienen CDN, archivos almacenados en SaaS, almacenamiento en caché, entre otros.

Inicialmente se definen las políticas y tipos de datos usados en la organización para luego determinar los repositorios de información que se tienen y finalmente decidir qué información será migrada a la Nube. El cliente puede hacer uso de las siguientes herramientas:

- CASB (Cloud Access and Security Brokers): ayuda a las organizaciones en la gestión y protección de datos almacenados. Soportan DLP (Software de prevención de pérdida de datos) e incluso ofrecen controles gestionar datos sensibles (Petters, 2020).
- Filtrado de URL: compara el tráfico web con una base de datos para evitar el acceso a sitios dañinos (Palo Alto Networks); ayuda a entender los servicios usados por los usuarios.
- DPL: estrategias que protegen los datos sensibles de la organización al mantenerlos en su red (Chistik, 2019).

El cifrado se encarga de la protección directa de los recursos mientras que la administración de claves fortalece el acceso a los mismos. Estos dos términos se subdividen respectivamente en:

Tabla 21 Cifrado y administración

Cifrado de datos	Administración de claves
Datos en tránsito de redes: deben ser protegidos en todo momento.	**Almacenamiento**: debe ser estrictamente protegido pues cualquier descuido podría exponer los datos aun si ya están cifrados.
Datos estáticos: datos protegidos en una base. El cliente debe cifrar su información en el momento de su envío y almacenamiento.	**Acceso al almacenamiento**: debe restringirse a quienes estrictamente lo necesiten.
Datos de respaldo: deben ser especialmente protegidos de	**Backup**: la perdida de alguna clave puede causar la pérdida total de la

perdidas, robos o cualquier tipo de manipulación; usualmente el proveedor se encarga de esto.	información, por ello esta fase debe implementar mecanismos seguros de recuperación de claves.

Fuente: Autor, tomado de la CSA

Ambos conceptos tienen una fase relacionada al backup, una alternativa, en caso de requerirla es el uso de protocolos ya existentes. Entre algunos ejemplos destacados se tienen:

- KMIP (Key Management Interoperability Protocol) cubre la comunicación de los sistemas usados en cifrado y administración.
- IEEE P1619-2018 (Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices), proyecto de estandarización en el cifrado de datos (IEEE SA, 2018).

En base a esto, la CSA define los siguientes controles de acceso y encriptación:

- De data: se implementan en base a planes o de gestión, controles de compartición pública e interna y controles a nivel de aplicación.
- De almacenamiento (en reposo) cifrado: protege la data y prioriza el formato de datos. Este dominio se enfoca en el primer proceso, mismo que varía según el modelo con el que se esté trabajando:

Gráfico 14 Cifrado de almacenamiento según el modelo de Nube

IaaS: Varían según la data	
En volúmenes:	Por objetos:
Gestionada por la instancia: claves gestionadas en volumen y protegidas por contraseñas. *Gestionada externamente*: las claves se emiten bajo petición.	*Del lado del cliente*: se usa como backend. *Del lado del servidor*: los datos se encriptan después de ser transferidos. *Tipo proxy*: el proxy maneja todas las operaciones de cifrado.
PaaS: Varían según la plataforma.	

Capa de aplicación: el cifrado se da en la aplicación o cliente que accede a la plataforma. *De la base de datos*: los datos cifran al ser incorporados y soportados por una base de datos (ejemplo TDE (Transparent Database Encryption)). *Otros*: capas gestionadas por el proveedor en la aplicación.
Administración de claves: destaca por
HSM (Hardware Security Module) Dispositivo virtual Servicio de proveedor en la nube Híbrido Clave gestionada por el cliente

Fuente: Autor, basado en la CSA

A nivel general, las recomendaciones de este dominio abarcan:

1. Determinar la opción de cifrado adecuada en base al modelo de amenazas, la estructura del negocio y requisitos técnicos.
2. Implementar el uso de buenas prácticas para la administración de claves y los procesos de cifrado/descifrado de datos.
3. Definir cláusulas que den a conocer los estándares usados en el cifrado y como se están gestionando las claves.
4. Determinar si las claves usadas son diferentes para cada cliente.
5. Utilizar cifrado en las fases de tránsito, almacenamiento y backup de datos (especialmente en los datos sensibles del cliente.
6. En SaaS, considerar la posibilidad de usar CASB en la supervisión de datos. En PaaS e IaaS se sugiere regirse a las políticas existentes.
7. Supervisar que las APIs, datos, y que los registros se rijan a las políticas de cumplimiento y ciclo de vida.
8. Determinar los controles de acceso que se usarán.
9. Aprovechar las capacidades de la arquitectura para mejorar la seguridad de datos.
10. Trabajar con normas que permitan establecer una buena seguridad, se tienen como ejemplos: NIST SP-800-57 y ANSI X9.69 y X9.73.

12. Accesibilidad

Cubre los mecanismos utilizados en los procesos de identidad y el control de acceso. La gestión de estos procesos abarca varias funciones, siendo las más destacadas:

- *Abastecimiento* de identidades: procesos de alta y baja de usuarios.
- *Autenticación*: verificar que el usuario sea en efecto quien dice ser.
- *Federación*: gestiona identidades federadas mediante proveedores de identidad, mejor conocidos como IdP.
- *Autorizaciones*: trabajar mediante perfiles de usuario.
- *Soporte*: asegura el cumplimiento normativo.

En la Nube, IAM (Identity and Access Management) se define como una disciplina de seguridad que determina que las personas correctas accedan a los recursos correctos en un momento determinado y por las razones adecuadas (Gartner).

La gestión de identidades y accesos es manejada por un amplio número de estándares, a continuación, se listan los más comúnmente observados en base a estudios de la CSA:

- SAML: admite autenticación autorización. Estándar basado en XML para la creación e intercambio seguro de información (OASIS , s.f.); es soportado por múltiples empresas.
- OAUTH: diseñado para trabajar sobre HTTP, es un estándar de IETF (Internet Engineering Task Force) usado para la autorización, usualmente en los servicios web (OpenID, s.f.).
- OPENID: estándar de autenticación basado en HTTP; cuenta con soporte a los servicios web.

Se debe tener ciertas consideraciones la gestión de identidades:

- Los proveedores admiten las identidades, y atributos internos para los usuarios que acceden directamente al servicio.
- Los usuarios deben decidir dónde gestionar sus identidades y los modelos arquitectónicos y tecnologías que usarán para integrarse con los proveedores.

En el área de autenticación, destaca MFA (Multifactor authentication) por los siguientes factores:

- Tokens duros: dispositivos físicos que generan contraseñas de acceso de un solo uso; son el máximo nivel de seguridad.
- Tokens blandos: similares al anterior, pero en forma de aplicaciones de software.
- Contraseñas fuera de banda: mensajes enviados al teléfono del usuario que actúan como contraseña de un solo uso.
- Biometría: protección local que representa un atributo que puede ser enviado al proveedor.

El impacto de la Nube en la autorización y gestión de acceso se visualiza en varias formas, algunas de las más importantes incluyen:

- Los proveedores y plataformas cuentan con su propio conjunto de autorizaciones potenciales.
- Los controles y autorizaciones son manejados por el proveedor.
- El usuario define los derechos y su configuración en la Nube.
- Las plataformas tienen mayor soporte para los modelos ABAC (Attribute-Based Access Control), e IAM.

Finalmente, se tiene el manejo de los usuarios privilegiados (PAM), el cual cubre las estrategias y tecnologías usadas para ejercer control sobre el acceso y permisos elevados de los usuarios; PAM ayuda a las organizaciones a prevenir o mitigar, los daños derivados de ataques externos y de negligencia interna (BeyondTrust).

En base a lo expuesto, las recomendaciones para este dominio son:

1. Facilitar el alta y baja de usuarios mediante la implementación de estándares.
2. Trabajar con esquemas SPML (Service Provisioning Markup Language).
3. Trabajar con un proveedor de identidades.
4. Implementar un sistema de identidad (Ej.: autenticaciones basadas en LDAP o conexiones VPN).

5. Implementar protocolos para la identificación de usuarios (como OpenID y sus certificaciones) y limitar sus privilegios.
6. Implementar certificaciones OAUTH, para la autenticación local.
7. Implementar fuertes sistemas de autenticación (Ej.: las contraseñas de un solo uso o los certificados digitales).
8. Verificar que el proveedor trabaje con estándares de federación, mínimamente con SAML y Web Services-Federation.
9. Establecer modelos para el control de acceso según el tipo de se servicios con el que se esté trabajando.
10. Desarrolla un plan con procesos completos y formalizados para la gestión de y autorizaciones.
11. Manejar la gestión de identidades privilegiadas con MFA.
12. Elegir los protocolos de seguridad en base a sus casos de uso y restricciones.

13. Seguridad como un servicio (SecaaS)

El uso de SecaaS representa beneficios y preocupaciones en comparación a la gestión tradicional de la seguridad, CSA considera las siguientes:

Tabla 22 Beneficios y preocupaciones de uso de SecaaS

Potenciales Beneficios	Potenciales Preocupaciones
El uso de SecaaS arrastra todas las ventajas de los servicios en la Nube.	Falta de visibilidad: el proveedor puede no revelar los detalles de implementación y gestión de seguridad y entorno.
Experiencia: cuenta con amplio conocimiento e investigaciones de seguridad.	Diferencias normativas: incapacidad de garantizar el cumplimiento de todas las jurisdicciones en las que opera una organización.
Inteligencia compartida: protección simultánea de varios clientes.	Manejo data regulada: se debe regir a los requisitos de cumplimiento.

Flexibilidad de despliegue: es un modelo nativo de la Nube con amplio acceso a red y elasticidad.	Fuga de datos: los proveedores se rigen a estándares de aislamiento y segregación.
Aislamiento de clientes: es posible interceptar ataques antes de que lleguen a la organización.	Cambio de proveedor: preocupación de organizaciones ante una posible pérdida de acceso a datos.
Escalado y coste: el consumidor paga en base a su crecimiento.	Migración a SecaaS: proceso planificado, ejercitado y mantenido.

Fuente: Autor, tomado de la CSA

SecaaS destaca en varias categorías tales como:

- Servicios de gestión de identidades, derechos y accesos: servicios que proporcionan identidad, atributos y reputación a las entidades.
- CASB: interceptan comunicaciones dirigidas a servicios en la Nube para detectar y/o prevenir problemas de seguridad. Incluyen funciones de clasificación de riesgos.
- Seguridad web: protección en tiempo real; representa una capa adicional de seguridad granular y contextual para las aplicaciones.
- Seguridad de Email: protege a la organización de ciertos riesgos (suplantación de identidad o archivos adjuntos maliciosos), aplica políticas corporativas y da opciones de continuidad del negocio y de seguridad (como firmas digitales o protección avanzada contra malware y phishing).
- Evaluación de la seguridad: auditorías, respaldadas por normas como NIST o ISO, realizadas por terceros o el cliente. Se enfoca en evaluar la seguridad tradicional, de las aplicaciones y de plataformas en la Nube.
- Firewalls de aplicaciones web: los clientes redirigen el tráfico a un servicio que analiza y filtra el tráfico antes de pasarlo a la aplicación web de destino.

- Detección/Prevención de Intrusos (IDS/IPS): monitorean patrones de comportamiento para detectar anomalías.
- Gestión de Información y Eventos de Seguridad (SIEM): datos de registro y eventos de redes, aplicaciones y sistemas que se analizan para la elaboración de informes en tiempo real.
- Cifrado y gestión de claves: incluye proxies de cifrado para SaaS, que interceptan el tráfico de SaaS.
- BC/DR: realizan copias de seguridad de datos en sistemas individuales y centros de datos a una plataforma Cloud.
- Gestión de la seguridad: reúnen las capacidades tradicionales de gestión un en un único servicio, reduciendo la necesidad de servidores locales.
- Protección contra la denegación de servicio distribuida: funcionan desviando el tráfico para absorber ataques antes de que afecten la infraestructura del cliente.

En base a todo lo expuesto nacen las siguientes recomendaciones:

1. En caso de contratar un proveedor de SecaaS, se debe comprender los requisitos específicos de seguridad, manejo y disponibilidad de datos, y el apoyo al cumplimiento.
2. Brindar especial atención a la gestión de datos regulados.
3. Entender las necesidades de retención de datos y elegir un proveedor en base a las mismas (capaz de soportar la alimentación de datos sin crear una situación de bloqueo).
4. Verificar que el servicio SecaaS sea compatible con planes actuales y futuros, de la plataforma, sistemas operativos móviles y de estaciones de trabajo admitidos, etc.

14. Tecnologías relacionadas

CSA dedica un segmento a aquellas tecnologías relacionadas a la Nube pero que no encajan en los dominios previamente mencionados. Se tienen cuatro áreas principales:

1. Big Data: conjuntos de información de alto volumen, velocidad y/o variedad que requieren nuevas formas de procesamiento para una mejor toma de decisiones y optimización de procesos (Gartner). Cubren marcos de recopilación, almacenamiento y procesamiento de datos distribuidos y se componen esencialmente por las “3 V”:

Tabla 23 3V de la Big Data

Alto volumen	Alta velocidad	Alta variedad
Tamaño de los datos	Rápida generación y procesamiento de datos/flujo.	Datos estructurados, semiestructurados o no estructurados.

Fuente, Autor basado en la CSA

Es un área extremadamente extensa, por lo que solo se mencionan sus características más esenciales:

- Seguridad y privacidad: debido al gran volumen y sensibilidad de información, la seguridad y privacidad se ven afectadas por un mosaico de diferentes herramientas y plataformas.
- Recogida de datos: proceso usado en la transferencia de datos. Los nodos de análisis/procesamientos distribuidos también requieren de seguridad extra en su almacenamiento intermedio.
- Gestión de claves: debido a la naturaleza distribuida de los nodos, depende de los mecanismos utilizados.
- Capacidades de seguridad: en algunos casos, las capacidades del proveedor ayudan a compensar las limitaciones de la tecnología de Big Data.
- Gestión de identidad y acceso: al darse a nivel de Nube y de herramientas de Big Data, puede complicar las matrices de asignación de derechos.
- PaaS: muchos proveedores extienden el soporte a Big Data mediante el aprendizaje autónomo u otras opciones.

2. Internet de las cosas (IoT): representa la variedad de dispositivos informáticos no tradicionales del mundo físico que usan la conectividad a Internet (O'Brien, 2021). Se despliegan cada vez más en los entornos empresariales tales como:
    - Seguimiento digital de la cadena de suministro.
    - Seguimiento digital de la logística física.
    - Marketing.
    - Aplicaciones de salud y estilo de vida.

3. Computación móvil: la Nube puede representar una plataforma ideal plataforma ideal la movilidad; no obstante, CSA ve algunos problemas de seguridad, los más mencionados incluyen:
    - Registro del dispositivo, autenticación y autorización
    - Las API de las aplicaciones

4. Computación sin servidor: uso extensivo de ciertas capacidades de PaaS al punto que las aplicaciones se ejecutan totalmente en el entorno del proveedor sin ningún sistema operativo gestionado por el cliente. Algunos de sus servicios incluyen:
    - Almacenamiento de objetos
    - Equilibradores de carga en la nube
    - Bases de datos en la nube
    - Aprendizaje automático
    - Colas de mensajes
    - Servicios de notificación
    - Entornos de ejecución de código
    - Pasarelas API
    - Servidores web

    Aun cuando el proveedor es responsable de la seguridad por debajo del nivel de la plataforma, el usuario sigue siendo responsable de la configuración y uso de los productos. Desde la perspectiva de seguridad, sus características clave son:
    - Alta carga de seguridad al proveedor

- El usuario no tiene acceso a los niveles de supervisión y registro habituales (como del servidor o de la red).
- No todos los servicios se ajustarán a todas las normativas.
- Altos niveles de acceso al plano de gestión del proveedor
- Se puede reducir de forma drástica la superficie de ataque, vías de acceso e integración de componentes.
- Cualquier evaluación de seguridad debe cumplir los términos de servicio establecidos con el proveedor.
- La respuesta a incidentes puede complicarse y requerir cambios en el proceso y herramientas implementadas.

Las recomendaciones de este dominio se dividen según sus grupos:

Tabla 24 Recomendaciones del dominio 14

Big Data
a. Aprovechar las capacidades del proveedor, esto garantiza una protección adecuada en la meta-estructura y aplicaciones específicas de la Nube. b. Implementar cifrado en el almacenamiento primario, intermedio y de copia de seguridad. c. Incluir las especificaciones de Big Data y gestión de identidades y accesos de la plataforma en la matriz de asignación de derechos del proyecto. d. Comprender las ventajas y riesgos (especialmente en la privacidad y cumplimiento) de usar un servicio de aprendizaje automático. e. Considerar el uso de enmascaramiento de datos en aquellos servicios que no cumplan los requisitos de seguridad y privacidad. f. El proveedor debe garantizar que los datos de los clientes no serán expuestos a empleados u otros administradores. g. El proveedor debe especificar que normas cumplen los servicios de análisis y aprendizaje automático.
IoT
a. Asegurar que los dispositivos puedan ser parcheados y actualizados.

b. No almacenar credenciales estáticas en dispositivos que puedan poner en peligro la aplicación o infraestructura de la Nube. c. Seguir las mejores prácticas en el registro de dispositivos y la autenticación en la aplicación mediante el uso de estándares. d. Cifrar las comunicaciones. e. Usar una canalización de recopilación de datos segura y desinfectar los datos para evitar la explotación de la aplicación o infraestructura. f. Asumir que todas las solicitudes de la API son hostiles.
Computación móvil:
a. Seguir las directrices del proveedor, autenticar y autorizar correctamente los dispositivos móviles. b. Implementar estándares de la ubicación para conectar las aplicaciones de los dispositivos móviles a las alojadas en la nube. c. No transferir claves o credenciales sin cifrar. d. Validar y desinfectar todos los datos de la API.
Computación sin servidor:
a. El proveedor debe indicar que servicios PaaS han sido evaluados y en base a que requisitos o normas. b. Utilizar únicamente servicios sin servidor que se ajusten a las obligaciones de cumplimiento y de gobernanza. c. Implementar arquitecturas que reduzcan la superficie de ataque y/o las vías de ataque a la red. d. Los usuarios deberán confiar más en el escaneo y registro del código de la aplicación que en los registros del servidor y red. e. Los usuarios deben actualizar o rediseñar los procesos de respuesta a incidentes.

Fuente: Autor, en base a los conceptos de la CSA

5.1. Recomendaciones legales

Tal y como se evidenció en capítulos anteriores, las preocupaciones del uso de la Nube recaen en la seguridad de datos, almacenamiento o en accesibilidad,

aspectos que a su vez forman parte del campo legal. Este capítulo cubrirá la comparativa de análisis entre dos entidades ya mencionadas, ENISA y CSA.

Según el Cloud Compliance Report (CSA, 2011) los temas legales principales que deben ser cumplidos incluyen:

1. *Establecimiento de roles*: el cliente y el proveedor representan los roles con responsabilidades que permitirán que los servicios sean cumplidos con la normativa correspondiente:

Tabla 25 Recomendaciones a los roles de cliente y proveedor

Cliente	Proveedor
Verificar que el proveedor implemente las medidas necesarias para el cumplimiento de la normativa de protección de datos.	Establecer un contrato que especifique los detalles de seguridad, protección y obligaciones necesarios.
Realizar autorías al proveedor de forma continua.	Especificar si se hará uso de subcontratos.
Analizar el riesgo del ciclo de vida de la información y de los activos colocados en la Nube.	Implementar las medidas de seguridad necesarias al modelo de despliegue.
Controlar la información durante todo el ciclo de vida.	Brindar las herramientas necesarias para el cumplimiento de obligaciones.
Comprobar que el proveedor implemente las medidas de seguridad necesarias según el modelo que se esté usando.	Considerar las medidas de seguridad que serán aplicadas (gestión de acceso, incidencias, auditorías, etc.).
Controlar que se apliquen medidas de seguridad en la gestión de accesos, incidencias, auditorias, backup y telecomunicaciones.	Delimitar las localidades donde se podría realizar el tratamiento de la información.

Fuente, Autor basado en las especificaciones de la CSA

2. *Aplicación de la legislación:* CSA considera que las leyes que se aplicaran dependen únicamente del Estado donde se encuentre independientemente de la ubicación del proveedor. No obstante, este último si debe considerar las leyes que su ubicación demande en la protección de servicios.

3. *Legislación aplicable:* Se basa en principalmente en la directiva 95/46/CE (AEPD, 1995) y representa un marco legal centrado en: la información, consentimiento, finalidad, calidad, seguridad, derechos de acceso, rectificación, cancelación/oposición, autoridad de control independiente y la limitación a las transferencias internacionales de datos.
   Las cláusulas más importantes de esta directiva se refieren al tratamiento y protección de datos personales, a la elaboración de un buen contrato y su respectivo cumplimiento, y a la gestión de telecomunicaciones.

4. *Transferencias internacionales:* son muy frecuentes en la Nube; trabajan con: el capítulo IV de la Directiva 95/46/ CE; el titulo V de la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal) y el título VI del RLOPD (Reglamento de desarrollo de la Ley Orgánica de Protección de Datos).

5. *Autoridades de control:* se define por la Directiva 95/45/CE, en resumen, delega autoridades encargadas de vigilar el cumplimiento de la normativa en un área específica. Las autoridades de control pueden aplicar más de una legislación para la resolución de inconvenientes.

6. *Comunicación a otras autoridades:* en caso de que los datos sean solicitados por una autoridad, el proveedor deberá informar al usuario sobre su entrega. Este aspecto debe definirse en el contrato para que el proveedor sepa qué tipo de información está transfiriendo.

Por su parte, el análisis de ENISA se centra en el reporte Beneficios, riesgos y recomendaciones para la Seguridad de la Información. Se presenta una tabla con los principales riesgos legales y se especifican cinco aspectos legales que deben ser cubiertos en base a la misma (ENISA, 2020).

Tabla 26 Riesgos Legales específicos de la Nube según ENISA

Nombre	Órdenes judiciales y descubrimiento electrónico	Riesgo derivado del cambio de jurisdicción	Riesgos de la protección de datos	Riesgos relativos a la licencia
Probabilidad	Alta	Muy alta	Alta	Media- alta
Impacto	Medio	Alto	Alto	Medio- alto
Vulnerabilidades	V1, V2, V3	V2, V3	V2, V3	V4
Activos afectados	A1, A2, A4, A5, A6, A8, A9			A1, A8, A10
Riesgo	Alto	Alto	Alto	Medio

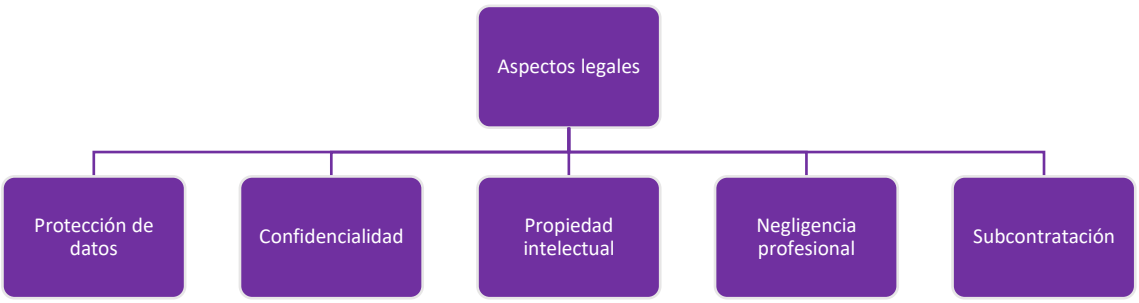
A1. Renombre de la compañía
A2. Confianza del cliente
A3. Fidelidad y experiencia de empleados
A4. Datos personales
A5. Datos personales sensibles
A6. Datos personales sensibles críticos
A7. Datos de recursos humanos
A8. Servicios en tiempo real
A9. Prestación de servicio
A10. Certificación

V1. Falta de aislamiento en recursos
V2. Almacenamiento de datos en jurisdicciones múltiples con falta de transparencia
V3. Falta de información sobre jurisdicciones
V4. Falta de integridad y transparencia en términos de uso

Fuente: Autor basado en "Beneficios, riesgos y recomendaciones para la Seguridad de la Información" (ENISA, 2020).

En base a estos riesgos, ENISA considera los siguientes aspectos legales:

Gráfico 15 Aspectos legales de ENISA



Fuente: Autor, basado en las definiciones de ENISA

1. *Protección de datos:* cubren datos: personales, datos sensibles, tratamiento de datos (registros, elaboración, modificación, etc.), responsable del tratamiento (entidad que determina los fines y medios para este), y encargado de tratamiento (entidad que trata los datos personales).

2. *Confidencialidad:* factor de riesgo, debe ser protegida por el proveedor. Las cláusulas relacionadas a este aspecto deben ser revisadas y discutidas por ambas partes del contrato.
3. *Propiedad intelectual:* dentro de Cloud Computing puede ser puesta en riesgo, de llegar a sufrir un prejuicio este puede nunca ser revertido.
4. *Negligencia profesional:* causa que el cliente experimente errores (fallas con el personal interno y/o incumplimiento de cláusulas contractuales), lo que afecta directamente a su organización.
5. *Subcontratación:* la intervención de terceros en los servicios ofrecidos por el proveedor coloca al susodicho en una posición de riesgo pues existe la posibilidad de que el cliente desconfié de la subcontratación.

En base a esto, surgen las siguientes recomendaciones legales centradas en SLA, acuerdos relacionados a la Nube (licencias, términos de uso, entre otros) y la protección de la información (ENISA, 2020):

1. Para la protección de los datos, se debe elegir cuidadosamente un proveedor en base las medidas y técnicas de seguridad y organización que sean ofrecidas.
2. Analizar las medidas obligatorias de seguridad de datos que pueden obligar al cliente a someterse a medidas regulatorias y/o judiciales que no sean abordadas en el contrato original.
3. Monitorear la información involucrada en la transferencia de datos tanto dentro como fuera de la Nube, especialmente si se relaciona directa o indirectamente con el Espacio Económico Europeo.
4. Dado que cada país cuenta con sus respectivas restricciones en acceso de autoridades policiales a datos, es obligación del cliente analizar y determinar (considerando las posibles jurisdicciones aplicables y cualquier riesgo relacionado estas) que información le entregara al proveedor.
5. Revisar las funciones y obligaciones asociadas con la confidencialidad y no divulgación de datos.
6. Tanto en IaaS como en PaaS es posible almacenar la propiedad intelectual (incluyendo obras originales creadas con la infraestructura de la Nube). Por ello, el cliente debe tener la garantía de que se respeten todos sus derechos de propiedad intelectual sin que se afecte la calidad del servicio.

7. Verificar que las capacidades del proveedor cumplan sus obligaciones contractuales con transparencia, especialmente si se diera la posibilidad de rescindir el contrato.

6. Conclusiones y recomendaciones

Conclusiones:

1. Cloud Computing es el paradigma de las Tecnologías de la información que, pese a sus riesgos, es cada vez más implementado por usuarios, compañías y entidades gubernamentales.
2. Dada la importancia del Cloud Computing y su rápido crecimiento, diferentes organizaciones globales han decidido invertir en el estudio y análisis de diferentes factores de la Nube, siendo algunos de los más destacados, modelos de servicios, las diferentes arquitecturas y el surgimiento de las nuevas tecnologías. Se han destinado entidades exclusivas que se dedican específicamente a los riesgos de la Nube, su prevención y mitigación.
3. La principal preocupación de los usuarios siempre ha sido la seguridad, privacidad e integridad de los datos que son migrados a la Nube. Los estudios han demostrado que, si bien la cantidad de empresas que usan servicios Cloud ha aumentado, esta preocupación no ha cambiado, muy por el contrario, ha aumentado debido a que los atacantes evolucionan constantemente y encuentran nuevas formas de usar la Nube y sus tecnologías a su favor.
4. La virtualización fue una de las bases que le permitió a Cloud desarrollarse, siendo que fue el instrumento que hizo posible su escalabilidad y velocidad a precios accesibles para el público, lo que a su hizo vez fue la raíz de su crecimiento.
5. Los principales riesgos de seguridad en la Nube se relacionan a: infraestructuras, compartidas, interfaces, débil protección de datos, falencias de personal interno, falta de cumplimiento de normas y/o estándares y al mal uso de recursos por parte de los usuarios.
6. El Cloud Computing se apoya en entidades legisladoras pues la manipulación y transferencia de datos conllevan varias implicaciones legales, mismas a las que los dueños de información deben estar atentos para evitar futuros problemas.
7. Los contratos entre cliente-proveedor deben incluir todos los requerimientos, derechos y obligaciones que cada tienen las partes involucradas. El usuario debe revisar meticulosamente estos documentos y, de ser necesario, negociarlos antes de acceder a fírmalos.

8. En Ecuador Cloud Computing sigue siendo un área relativamente nueva, sobre todo en comparación a otros países, en parte esto se debe a la ignorancia digital que hace que los usuarios decidan no implementar tecnologías Cloud o que lo hagan sin comprender las capacidades y riesgos de esta tecnología causando que sean vulnerables a ataques.

Recomendaciones:

1. Es necesario que se dé una capacitación masiva pretendiendo que todos los que decidan adoptar servicios virtuales comprendan los conceptos de la Nube y todas las problemáticas que conllevan.
2. Tanto usuarios comunes como especialistas deben ser conscientes de que todos estamos expuestos en la red y que somos vulnerables a ataques. Si bien no es correcto ver el desarrollo de la tecnología como un enemigo, tampoco se debe confiar ciegamente en la misma, por lo que se debe aprovechar la documentación disponible y así evitar correr riesgos innecesarios.
3. Los proveedores de Cloud Computing y sus clientes deben prestar especial atención a las amenazas, rasgos y vulnerabilidades de este entorno, se sugieren capacitaciones y la implementación de herramientas de gestión, detección y evaluación de riesgo.
4. Ante cualquier inconveniente legal, el contrato será el documento jurídico que el cliente tendrá a su favor, por lo que es necesario contar con todas las precauciones necesarias para evitar la pérdida o alteración de este.
5. El cliente debe elegir su modelo de Cloud Computing y su proveedor en base a aquel que mejor se adapte a sus requerimientos. Durante esta elección también se sugiere indagación o ayuda externa para determinar que el proveedor con el que se va a tartar cuente con estándares que ayuden a garantizar la correcta gestión de seguridad de la información.
6. Investigar con cierta frecuencia cuales son las tendencias en Cloud Computing pues sus amenazas evolucionan constantemente por lo que es necesario actualizar las medidas de seguridad tomadas.

7. Anexos

7.1. Glosario de siglas

AAA: Autenticación, Autorización y Auditoría.

ABAC: Attribute-Based Access Control.

ACL: Australian Consumer Law.

AGPD: Agencia Española de Protección de Datos.

APPI: Act on the Protection of Personal Information.

BD/CR: Business Continuity and Disaster Recovery.

CADF: Cloud Auditing Data Federation Working Group.

CAIQ: Consensus Assessments Initiative Questionnaire.

CARG: Compound Annual Growth Rate.

CASB: Cloud Access and Security Brokers.

CDN: content delivery network.

CI/CD: Continuous Integration/Continuous Deployment.

CLI: Line Interfaces.

CMWG: Cloud Management Working Group.

CRM: Customer relationship management.

CSA: Cloud Security Alliance.

CYBEX: Cybersecurity Information Exchange.

DLP: Software de prevención de pérdida de datos.

DMTF: Distributed Management Task Force.

DNS: Domain Name Server.

ENISA: European Network and Information Security Agency.

ESI: Electronically stored information.

EU: Unión Europea.

FRCP: Federal Rules of Civil Procedure.

GDPR: General Data Protection Regulation.

HSM: Hardware Security Module.

IaaS: Infrastructure as a Service.

IAM: Identity and Access Management.

IDS/IPS: Intrusion Detection/Prevention.

INEC: Instituto Nacional de Estadística y Censos.

IoT: Internet of Things.

ISO: International Organization for Standardization.

ITIL: Information Technology Infrastructure Library.

ITSM: Information Technology Service Management.

ITU: International Telecommunication Union.

LAN: Local Area Networks.

LOPD: Ley Orgánica de Protección de Datos de Carácter Personal.

MFA: Autenticación de múltiples factores.

MFA: Multifactor authentication.

MitM: man in the middle.

MV: memoria volátil.

NDA: acuerdo de confidencialidad.

NIST: National Institute of Standards and Technology

OASIS: Identity in the Cloud TC.

OSA: Open Security Architecture.

PaaS: Platform as a Service.

PAM: Privileged Access Management.

PDA: Personal Digital Assistant.

PwC: PriceWaterhouseCoopers.

PYME: pequeñas y medianas empresas.

RLOPD: Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.

SaaS: Software as a Service.

SAJACC: Standards Acceleration to Jumpstart Adoption of Cloud Computing.

SAML: Security Assertion Markup Language.

SDK: Software Development Kits.

SDN: Software Defined Networking.

SecaaS: Security as a Service

SEDM: Software Engineering and Data Mining.

SEWG: Software Entitlement Working Group.

SIEM: Security Information & Event Management.

SLA: Service Level Agreement.

SNAP: Secretaría Nacional de la Administración Pública.

SOAP: Simple Object Access Protocol.

SOC: Centro de Operaciones de Seguridad.

SSDLC: Secure Software Development Lifecycle.

SVPC: System Virtualization, Partitioning, and Clustering Working Group.

VLAN: Virtual Local Area Networks.

WAN: wide area network.

Bibliografía

AEPD. (1995). *Parlamento Europeo y Consejo de la Unión Europea. Directiva 95/46/CE del parlamento europeo y del consejo.* España.

AGPD. (2013). Guía para Clientes que contraten Servicios de Cloud Computing Agencia española˜ de protección de Datos, no. 24. 1 – 23.

Alien Vault. (2015, Agosto 12). *Guía del Técnico para establecer un Centro de Opciones de Seguridad*. Retrieved from https://learn-cybersecurity.att.com/c/5-security-controls?x=5v9G6V&utm_internal=soc-irlookbook&xs=16860

Anónimo . (2008). *ISO/IEC 27005:2008 - information technology -- security techniques --information security risk management*. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=42107

Anónimo. (2007). *ISO27000.es - el portal de ISO 27001 en español. gestión de seguridad de la información*. Obtenido de http://www.iso27000.es/glosario.html

Arminio, E., Velásquez, A., Mayor, U., & Andrés, D. S. (2013). Seguridad En La Nube.

Asamblea Nacional. (2009). Ley de Seguridad Pública y del Estado. Quito, Ecuador: Ediciones Legales.

BeyondTrust. (n.d.). *Privileged Access Management (PAM).* Retrieved from https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam

Brunette, G., & Mogull, R. (2009). *Security guidance for critical areas of focus in cloud computing v2. 1.* Cloud Security Alliance. Retrieved from Cloud Security Alliance.

Camps Sinisterra, C., & Oriol Allende, A. (2012). *La nube: oportunidades y retos para los integrantes de la cadena de valor.*

Carroll, M. (2011). Secure cloud computing: Benefits, risks and controls. *Information Security South Africa (ISSA), 2011*, (pp. 1-9).

Chen, J., Wu, X., Zhang, S., Zhang, W., & Niu, Y. (2012). A decentralized approach for implementing identity management in cloud computing," in Cloud and Green. *Cloud and Green Computing (CGC), Second International Conference*, (pp. 770-776).

Chistik, J. (2019, Diciembre 18). *Forcepoint.* Retrieved from ¿Qué es Data Loss Prevention (DLP)?: https://www.forcepoint.com/es/blog/insights/what-is-data-loss-prevention-dlp

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012, August). *SP 800-61 Rev. 2.* Retrieved from Computer Security Incident Handling Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Cisco. (2016, Noviembre 15). *Cisco Global Cloud Index 2015–2020.* Retrieved from https://www.cisco.com/c/dam/m/en_us/service-provider/ciscoknowledgenetwork/files/622_11_15-16-Cisco_GCI_CKN_2015-2020_AMER_EMEAR_NOV2016.pdf

Clemons, E. K., & Chen, Y. (2011). Making the decision to contract for cloud services: Managing the risk of an extreme form of IT outsourcing. *44th International Conference on System Sciences* (pp. 1-10). Hawaii: IEEE.

Collahuazo, J., & Alexander, J. (18 de Mayo de 2012). *Guía para el análisis de factibilidad en la implantación de tecnologías de Cloud Computing en empresas del Ecuador.* Obtenido de https://bibdigital.epn.edu.ec/handle/15000/4649

Congreso Nacional. (2002). Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Quito: Ediciones Legales.

Constitución de la República del Ecuador. (2008). Quito, Pichincha, Ecuador: Registro Oficial 449.

Creasey, J. (2015). *Cyber Security Monitoring and Logging Guide.* Retrieved from https://www.crest-approved.org/wp-content/uploads/Cyber-Security-Monitoring-Guide.pdf

CSA. (2011). *Cloud Compliance Report.*

CSA. (2019, Agosto 6). *CSA Releases New Research - Top Threats to Cloud Computing:* . Retrieved from https://cloudsecurityalliance.org/press-releases/2019/08/09/csa-releases-new-research-top-threats-to-cloud-computing-egregious-eleven/

CSA. (2020, Mayo 27). *Software-Defined Perimeter (SDP) and Zero Trust*. Retrieved from https://cloudsecurityalliance.org/research/working-groups/software-defined-perimeter-and-zero-trust/#_overview

CSA EC. (n.d.). *Cloud Security Alliance Ecuador*. Retrieved from https://www.csa-ec.org

ENISA. (2020, Noviembre 9). *Beneficios, riesgos yrecomendaciones para la Seguridad de la Información.* Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish

European Commission. (2020, noviembre 20). *Shaping Europe's digital future*. Retrieved from NIS Directive: https://digital-strategy.ec.europa.eu/en/policies/nis-directive

Evaluando Cloud. (2015, Noviembre 24). *Mercado de Cloud Computing: previsiones de adopción y crecimiento*. Retrieved from https://evaluandocloud.com/mercado-de-cloud-computing-previsiones-de-adopcion-y-crecimiento/

Franklin, D. (2015). *Security Intelligence*. Retrieved from Threat Intelligence Collaboration Leads to More Efficient, Comprehensive Cybersecurity:

https://securityintelligence.com/threat-intelligence-collaboration-leads-to-more-efficient-comprehensive-cybersecurity/

Gartner. (n.d.). *Gartner Glossary.* Retrieved from Identity and Access Management (IAM): https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam

Gartner. (n.d.). *Gartner Glossary.* Retrieved from Big Data: https://www.gartner.com/en/information-technology/glossary/big-data

Gómez Treviño, J. (2010). Aspectos Legales del Cloud Computing. *b: Secure*, 2.

Grupo EKOS. (2019). CLOUD: Eficiencia y ahorro transversal a cualquier industria. *Datta Business Innovation*, 45-47.

Herrera, P. (2014). *Propuesta para la oferta del servicio de Cloud Computing por parte de la empresa Computadores y Equipos Compuequip DOS S. A.* . Cuenca: Ph.D. Dissertation [C. A. D. E. Empresas].

IEEE SA. (2018, 10 23). *IEEE 1619-2018 - IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices*. Retrieved from https://standards.ieee.org/standard/1619-2018.html

Intersoft Consulting. (2016). *General Data Protection Regulation https://gdpr-info.euGDPR*. Retrieved from https://gdpr-info.eu

J. Chen, X. W. (2012). *A decentralized approach for.*

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. NIST Special Publication.

Kosinski, M., Stillwell, D., & Graepel, T. (2013, April 9). *Private traits and attributes are predictable from digital records of human behavior.* Retrieved from https://www.pnas.org/content/pnas/110/15/5802.full.pdf

Liou, J., & Bhashyam, S. (2010). A feasible and cost effective two-factor authentication for online transactions. *Software Engineering and Data Mining (SEDM), 2nd International Conference*, (pp. 47-51).

Mackay, M., Baker, T., & Al-Yasiri, A. (2012). *Security-oriented cloud computing platform for critical infrastructures,*. Retrieved from https://www.sciencedirect.com/science/article/pii/S0267364912001434

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing, National Institute of Standards and Technology, NIST Special Publication.*

Melorose, J., Perroy, R., & Careas , S. (2015). El derecho a la proteccion de datos de carácter personal Ecuatoriano analizado a partir de la relacion B2c en la prestacion de servicios de Cloud Computing: Caso de Políticas de Privacidad de Dropbox. *Statewide Agricultural Land Use Baseline, vol. 1*, 197.

Michigan Legal Publishing Ltd. . (2020, Noviembre 1). *Federal Rules of Civil Procedure 2021 Edition.* Retrieved from Rule 26 – Duty to Disclose; General Provisions Governing Discovery:

https://www.federalrulesofcivilprocedure.org/frcp/title-v-disclosures-and-discovery/rule-26-duty-to-disclose-general-provisions-governing-discovery/

Mogull, R., Arlen, J., Gilbert, F., Lane, A., Mortman, D., Peterson, G., & Rothman, M. (2017). *The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0.*

Montoya S., J. A., & Restrepo R., Z. (2012). *Gestión de identidades y control de acceso desde una perspectiva organizacional.* Bancolombia Medellín, Colombia: Editorial Bonaventuriana.

Niño Vásquez, D. F. (2020). *DISEÑO DE UN MODELO DE VIRTUALIZACIÓN PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE SERVIDORES EN ALTA DISPONIBILIDAD.* Bogotá D.C.

OASIS . (n.d.). *OASIS Open*. Retrieved from OASIS Security Services (SAML) TC: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

OATH. (n.d.). *OATH: Initiative for Open Authentication*. Retrieved from https://openauthentication.org/

O'Brien, L. (2021). *CSA IoT Security Controls Framework v2.*

OpenID. (n.d.). *OpenID: The Internet Identity Layer*. Retrieved from OpenID Certification: https://openid.net/certification/

Packard , H. (2015, February). *A vision for cyber security detection analytics. Business white paper.* Retrieved from https://www.ten-inc.com/presentations/HP-Cyber-Security-Detection-Analytics.pdf

Palo Alto Networks. (n.d.). *Global Cybersecurity Lider.* Retrieved from What is URL Filtering?: https://www.paloaltonetworks.com/cyberpedia/what-is-url-filtering#:~:text=URL%20filtering%20limits%20access%20by,sites%20such%20as%20phishing%20pages.

Petters, J. (2020, June 17). *What is CASB? All About Cloud Access Security Brokers.* Retrieved from https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-a-casb.html

Primorac, C. (2014). *Licenciatura en Sistemas de Información Comunicaciones de Datos Computación en Nube. Monografía Adscripción, 46.* Obtenido de http://exa.unne.edu.ar/informatica/SO/primorac_monografia_computacion_en_nube.pdf

Sabahi, F. (2011). Cloud computing security threats and responses. *Communication Software and Networks (ICCSN), IEEE 3rd International Conference,* (pp. 245-249).

Scheepers, M. J. (2015, Junio 22). *Virtualization and Containerization of Application Infrastructure: A Comparison.* Retrieved from https://thijs.ai/papers/scheepers-virtualization-containerization.pdf

Secretaría Nacional de la Administración Pública. (2013). *Acuerdo No. 166.* Retrieved from https://www.educarecuador.gob.ec/anexos/correo/Acuerdo_166.pdf

Seeborg, R., Judge, C., Soong, S., & Of Court, C. (2015, Diciembre 1). *United States District Court Northern District of California.* Retrieved from E-Discovery (ESI) Guidelines: https://cand.uscourts.gov/forms/e-discovery-esi-guidelines/

Sepúlveda, E., Salcedo, O., & Gómez, E. (2012). "Manejo del Riesgo y Seguridad en el Consumo de Servicios de TI en Cloud Computing. En *Redes De Ingenieria, vol. 1* (págs. 10-21).

SIR. (2021, Enero 25). *Red IRIS* . Retrieved from Federación de identidades: https://www.rediris.es/servicios/identidad/sir/index.html.es#:~:text=A%20partir%20de%20entonces%2C%20estos,el%20acceso%20a%20sus%20contenidos.

Telefónica. (2016, Septiembre). *Ciberseguridad, la protección de la información en un mundo digital.* Retrieved from http://www.fundaciontelefonica.com/publicaciones

Tobergte, D. R., & Curtis, S. (2013). Computación en la Nube. Journal of Chemical Information and Modeling, vol. 53, no. 9.

UNIR. (2021). El impacto del cloud computing en la era COVID. *UNIR REVISTA.*

Wentao, L. (2012). Research on cloud computing security problem and strategy. *Consumer Electronics, Communications and Networks (CECNet), 2nd International Conference*, (pp. 1216-1219).

Westmonroe. (2016). *Rain down cost savings with cloud-based business applications*. Retrieved from https://www.westmonroepartners.com/perspectives/in-brief/rain-down-cost-savings-with-cloud-based-business-applications