**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| **PROGRAMA DE FORMACIÓN** | Implementación de auditoría técnica plataformas cloud |
| --- | --- |

| **COMPETENCIA** | 220601041 - Implementar sistemas de gestión según normativa y requerimientos técnicos. | **RESULTADOS DE APRENDIZAJE** | 220601041-03 - Aplicar los métodos de análisis y gestión del riesgo en escenarios relacionados con los servicios en nube. |
| --- | --- | --- | --- |

| **NÚMERO DEL COMPONENTE FORMATIVO** | 3 |
| --- | --- |
| **NOMBRE DEL COMPONENTE FORMATIVO** | Gestión del riesgo y seguridad en servicios en la nube |
| **BREVE DESCRIPCIÓN** | Los procesos tecnológicos de las organizaciones requieren aliarse con cambios y mejoras tecnológicas, la computación en la nube es el factor diferenciador y necesario de mayor adopción y migración de servicios, los datos en la nube traen cambios desde lo técnico, económico, legislativo y de acceso; es necesario conocer cuáles son esos riesgos que pueden afectar su integridad, confidencialidad, disponibilidad y protección. |
| **PALABRAS CLAVE** | Amenaza *(threat), compliance, hacking, malware, ransomware* |

| **AREA OCUPACIONAL** | 6 - Ventas y servicios |
| --- | --- |
| **IDIOMA** | Español |

1. **Tabla de contenidos**

**Introducción**

1. **Seguridad en la nube**
   1. Distribución de las responsabilidades en seguridad
   2. Perspectivas según los tipos de servicio y modelos cloud
   3. Estrategia y responsabilidad en protección de datos
      1. *Análisis previo antes de contratar servicios de computación en la nube.*
      2. *Implicaciones del cliente en servicios en cloud.*
      3. *Legislación aplicable.*
      4. *Obligaciones del cliente de servicios en nube.*
      5. *Medidas de seguridad exigibles.*
      6. *Garantías de cumplimiento de las medidas de seguridad.*
      7. *Garantías de recuperar los datos personales (portabilidad).*
   4. Acuerdos del nivel de servicio
      1. *Aspectos de referencia en la contratación de servicios en la nube.*
      2. *Organizaciones referentes en la contratación de servicios de cloud computing.*
2. **Gestión del riesgo**
   1. Gestión de las organizaciones basadas en el riesgo
   2. Metodología de gestión del riesgo
   3. Riesgos políticos y administrativos
      1. *Vinculación.*
      2. *Pérdida de gobernanza.*
      3. *Desafíos de rendimiento.*
      4. *Pérdida de renombre empresarial por la prestación conjunta.*
      5. *Error o cancelación de servicios en la nube.*
      6. *Falla en la cadena de suministro.*
   4. Riesgos técnicos
   5. Riesgos legales
   6. Riesgos relacionados con la nube

**Síntesis**

1. **Desarrollo de contenidos**

**Introducción**

Se da la bienvenida al componente formativo “Gestión del riesgo y seguridad en servicios en la nube”. Para comenzar el recorrido por el mismo, visite el recurso didáctico que se muestra a continuación:



1. **Seguridad en la nube**

Corresponde a la seguridad de la información, que corresponde a las políticas, tecnologías y formas de control, que están enfocadas en la protección de datos, aplicaciones e infraestructura asociadas a la computación en la nube.

* 1. **Distribución de las responsabilidades en seguridad**

A nivel mundial se han desarrollado normativas frente a la protección de los datos personales, incluso, en organizaciones mundiales como la OEA, que desde el año 1996 ha venido aprobando resoluciones enmarcadas en la protección de los datos personales, de hecho, el pasado 9 de abril de 2021 el Comité Jurídico Iberoamericano (JCI) aprobó los principios actualizados sobre la **Privacidad y la protección de datos personales**.

La computación en la nube obliga a que se establezcan acuerdos y la aplicación de la normativa jurídica en materia de la oferta de servicios en la nube, entre quienes ofrecen el servicio como proveedores y quienes consumen los servicios como clientes. Las diferentes normativas distinguen dos sujetos distintos: el responsable del archivo o del tratamiento de los datos y el encargado del tratamiento.



En estos acuerdos aparecen varios actores responsables de la protección y tratamiento adecuado de los datos, dentro de estos roles se encuentran los siguientes:





Si los servicios contratados o migrados a la nube requieren el tratamiento de datos personales su presencia es fundamental y se ha de tener en cuenta que el Oficial de Protección de Datos ODP como encargado de dirigir el Sistema de Protección de Datos Personales en la organización y responsable de velar por el cumplimiento del mismo en ella, se encarga, entre otras, de cumplir con las actividades que se aprecian a continuación:



* 1. **Perspectivas según los tipos de servicios y modelos cloud**

El cliente que contrata a un prestador de servicios de computación en la nube tiene una obligación legal de rapidez para elegir únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento esté conforme con los requisitos de la legislación aplicable y garantice la protección de los derechos del interesado.

Esta rapidez se traducirá dadas las características propias de estos servicios, en una selección de requerimientos de información al proveedor de servicios que estén direccionados a ofrecer las garantías para la protección de los datos personales de los cuales es responsable; todo esto, necesario para decidir sobre la modalidad de nube y el tipo de servicios que contrata y de esta forma, hacer la mejor elección entre sus proveedores.

En las administraciones públicas, la computación en la nube, debido al volumen y la sensibilidad de los datos que gestiona soporta unos riesgos específicos, estos deben analizarse de manera puntual, de acuerdo con los escenarios en donde se presente su uso, con lo cual se orienta para la disminución del riesgo el uso de cuidados en la implantación, evitando comprometer los derechos de autor y la seguridad de los ciudadanos. Por ello, es necesario tener presente que hay una regulación internacional en cuanto al movimiento de datos que es aplicable tanto al sector privado como al público.

|  | En particular, debe tenerse muy presente que las autoridades competentes de terceros países en los que se traten datos personales en el marco de los servicios de computación en la nube podrían solicitar y acceder a la información de la cual las administraciones públicas son responsables, en algunos casos sin que se le informe de esta circunstancia. Por esta razón, el prestador de servicios de computación en la nube debe conocer la regulación existente en los países en donde se vayan a tratar los datos, y las decisiones que serían necesarias tomar al respecto. La trascendencia de estos posibles accesos es un factor muy relevante para decidir sobre la contratación de estos servicios y el proveedor que los preste. |
| --- | --- |

* 1. **Estrategia y responsabilidad en protección de datos**

Para poder determinar una estrategia en la transferencia de responsabilidades al proveedor de servicios en la nube, a continuación, se hace referencia del estándar para clientes que contraten servicios de computación en la nube, en particular las garantías exigibles que han de ser atendidas por el proveedor previo a una contratación.

Es fundamental, incluso, legalmente exigible según la normativa aplicable en cada caso, la adhesión del encargado del tratamiento a un código de conducta aprobado o a un mecanismo de certificación aprobado como elemento para demostrar la existencia de las garantías suficientes.

* + 1. ***Análisis previo antes de contratar servicios de computación en la nube.***

El análisis previo a la contratación de servicios en la nube requiere tener presente condiciones específicas, como puede ver, a continuación:



* + 1. ***Implicaciones del cliente en servicios en cloud.***

El cliente que contrata servicios de computación en la nube sigue siendo responsable del tratamiento de los datos personales, aunque se contrate con una gran compañía multinacional la responsabilidad en términos de “*accountability*” no se desplaza al prestador del servicio, ni siquiera incorporando una cláusula en el contrato con esta finalidad.



* + 1. ***Legislación aplicable.***

El modelo de computación en la nube hace posible que tanto los proveedores de servicios como los datos almacenados en la nube se encuentren ubicados en cualquier punto del planeta, en cualquier caso, el cliente sigue siendo responsable del tratamiento de los datos, por lo que la normativa aplicable al cliente y al prestador del servicio es la local del país del cliente.

La aplicación de dicha normativa no puede modificarse contractualmente y aunque le informen acerca de la disociación de los datos personales, no cambia la ley aplicable, ni la responsabilidad del cliente y del prestador del servicio.



* + 1. ***Obligaciones del cliente de servicios en nube.***

Se debe ser diligente en la elección del prestador del servicio para que le ofrezca garantías suficientes en el cumplimiento de la ley de protección de datos aplicable y en la protección de los derechos de los interesados.

Se debe formalizar un contrato con las garantías indicadas en el apartado “las garantías contractuales”.

En particular, debe solicitar y obtener información sobre si intervienen o no terceras personas (subcontratistas) en la prestación de servicios de computación en la nube, esta es una condición muy habitual entre proveedores de servicios, de ser así se requiere:



Para la protección de los datos personales y en relación con las cláusulas contractuales es necesario:

* + Relevancia de la ubicación de los datos personales.
  + La localización de los datos es necesaria porque las garantías exigibles para su protección rigen de diferente forma, según los países en que se encuentren.
  + Existen acuerdos bilaterales o reglamentos vinculantes para diferentes regiones geográficas, estas ofrecen garantías suficientes y no se considera legalmente que exista una transferencia internacional de datos.
  + Si los datos están localizados en países que no pertenecen al mismo espacio o región amparada por acuerdos en este nivel, al tener una transferencia internacional de datos, dependiendo del país en que se encuentren, deberán proporcionarse garantías jurídicas adecuadas.
  + Las garantías consideradas adecuadas para las transferencias internacionales de datos regulan bajo consideraciones como:



Es preciso resaltar que la regulación sobre datos personales en Colombia impone cargas probatorias en cabeza de los responsables del tratamiento. Es así como en el siguiente recurso educativo se explican en brevedad:





* + 1. ***Medidas de seguridad exigibles.***

Las medidas de seguridad son indispensables para garantizar la integridad de los datos personales, evitar accesos no autorizados y recuperar la información en caso de que se produzcan incidencias de seguridad.

En la **Guía para la implementación del principio de responsabilidad demostrada** (*accountability*), establecida por las Superintendencia de Industria y Comercio se indica que las garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales serán los resultantes de un sistema de administración de riesgos asociados al tratamiento de datos personales, con el fin de que permitan “identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales”.

Por su parte, la evaluación del riesgo o impacto en la privacidad debería incluir, al menos:

* Una descripción detallada de las operaciones de tratamiento de datos personales que involucra el proyecto de comercio electrónico.
* Una evaluación de los riesgos específicos para los derechos y libertades de los titulares de los datos personales.
* La identificación y clasificación de los riesgos, así como la adopción de medidas para mitigarlos.
* Las medidas previstas para afrontar los riesgos, incluidas las garantías, los controles de seguridad, el diseño de *software*, las tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los titulares de los datos y de otras personas eventualmente afectadas.

Los resultados de este estudio, junto con las estrategias para mitigar los riesgos, hacen parte de la aplicación del principio de privacidad desde el diseño y por defecto.

En la gestión de los encargados del tratamiento en las transmisiones internacionales de datos personales, los sujetos obligados deben tomar las medidas necesarias para asegurar la protección de los datos personales, cuyo tratamiento es realizado por los encargados, a través de transmisiones internacionales de datos personales. Para ello, se deben tener en cuenta:



No se debe olvidar las garantías de cumplimiento y adherencia continua de estas medidas con base al programa integral de gestión de datos personales.

* + 1. ***Garantías de cumplimiento de las medidas de seguridad.***

| La Nube ¿Es segura para guardar tu información? Grupo Garatu - Soluciones TI | Como cliente se debe tener la opción de comprobar las medidas de seguridad, incluidos los registros que permiten conocer quién ha accedido a los datos de los que es responsable.  El proveedor de servicios cloud debe poner a su disposición toda la información necesaria para demostrar el cumplimiento de las medidas de seguridad.  El proveedor le puede acreditar que dispone de una certificación de seguridad adecuada mediante un tercero independiente que audite la seguridad. En este caso, debe conocerse la entidad auditora y los estándares reconocidos que aplica. |
| --- | --- |

Se debe solicitar información al proveedor sobre cómo se auditarán las medidas de seguridad, el cliente debe ser informado sin dilación indebida por el proveedor sobre las incidencias de seguridad que afecten a los datos de los que el propio cliente es responsable, así como de las medidas adoptadas para resolverlas o de las medidas que el cliente ha de tomar para evitar los daños que puedan producirse, por ejemplo, informar a sus propios clientes sobre cómo proteger su información personal.

En cuanto a los compromisos de confidencialidad de los datos personales, el proveedor debe comprometerse a garantizar la confidencialidad utilizando los datos solo para los servicios contratados. Asimismo, debe garantizar que el personal autorizado a tratar datos personales haya suscrito compromisos de confidencialidad o esté sujeto a obligaciones de confidencialidad estatutarias.

* + 1. ***Garantías de recuperar los datos personales (portabilidad).***

La portabilidad significa que el proveedor está obligado a resolverse el contrato o a la terminación del servicio, de entregar toda la información al cliente en el formato previamente acordado, de forma que este pueda almacenarla en sus propios sistemas o bien optar porque se traslade a los de un nuevo proveedor en un formato que permita su utilización, a la mayor brevedad posible, con total garantía de la integridad de la información y sin incurrir en costos adicionales.

| En particular, el cliente debe tener la opción de exigir la portabilidad de la información a sus propios sistemas de información o a un nuevo proveedor cuando considere inadecuada la intervención de algún subcontratista o la transferencia de datos a países que estime no aportan las garantías adecuadas. Estas condiciones son también particularmente importantes en los casos en que el proveedor modifique unilateralmente las condiciones de prestación del servicio dado su poder de negociación frente al cliente. Por tanto, se debe solicitar información y garantías al proveedor sobre la portabilidad de los datos personales. | Que debes saber al portar tu número. |
| --- | --- |

Asimismo, debe preverse mecanismos que garanticen el borrado seguro de los datos cuando lo solicite el cliente y, en todo caso, al finalizar el contrato. Un mecanismo habitual y apropiado es requerir una certificación de la destrucción, emitido por el proveedor de computación en la nube o por un tercero.

* 1. **Acuerdos de nivel de servicio**

Cualquier actividad empresarial, incluyendo la contratación de servicios de computación en la nube se debe regular mediante un contrato la relación entre el proveedor de servicios (en este caso el proveedor de servicios cloud CSP) y el cliente (en este caso, el contratante). A continuación, se mostrarán de manera genérica algunas cláusulas que deberían ser consideradas:

* Las cláusulas del contrato que deben definir claramente la posición de cada una de las partes, así como sus responsabilidades y obligaciones.
* Los términos de uso que se encargan de definir las especificaciones técnicas más importantes relacionadas con la entrega y la calidad del servicio. Suelen estar recogidas en documentos llamados SLA (Acuerdos de Nivel de Servicio) y entre otras cosas establecen los niveles de rendimiento y disponibilidad garantizados por el proveedor.



La falta de regulaciones específicas, así como de las funciones y obligaciones recíprocas, conllevan a que estas sean incorporadas en el pliego estándar de condiciones generales, las cuales son elaboradas de forma unilateral por el proveedor del servicio y en su defecto aceptadas por los clientes, sin que medie modificaciones a la medida, o mediante negociaciones o acuerdos. Para lo cual es necesario establecer una diferencia entre el caso de una pequeña o mediana organización, quienes seguramente escogerán entre los diferentes contratos ofrecidos, y una organización grande, quien tendrá mayor libertad de negociar las cláusulas. Las recomendaciones para cláusulas contractuales específicas deben entenderse como preferencias entre ofertas del mercado.

* + 1. ***Aspectos de referencia en la contratación de servicios en la nube.***

Existen algunos aspectos relevantes a tener en cuenta al llevar a cabo un contrato de servicios en la nube, que permiten amparar a la organización, a la vez que posibilitan exigir a los prestadores de servicio mayor control en la negociación, estos aspectos clave se detallan, a continuación:



* + 1. ***Organizaciones referentes en la contratación de servicios de cloud computing.***

Más allá de la propia legislación específica aplicable en materia de protección de datos se explican, a continuación, una serie de documentos que acreditan los focos de atención en cada uno de estos, con el fin de hacer un análisis un poco más detallado de aquellos más significativos:



1. **Gestión del riesgo**

En los últimos años, las estrategias corporativas se han centrado en dedicar los recursos propios en las actividades consideradas “*core*” o esenciales para mantener la competitividad en los mercados, externalizando aquellas otras actividades necesarias desde el punto de vista logístico u operativo, pero difíciles de entender por ser ajenas a la cultura de la organización y de la dirección, además de costosas de mantener por ser adquiridas y consumidas en un volumen reducido.

El desarrollo de la tecnología en los últimos veinte años ha impulsado la prestación de los servicios relacionados con las TIC, de forma acelerada hasta un nivel de madurez que no solo permite su externalización alineada con las actividades “*core*” del negocio, sino que son parte integral del negocio y forman parte de su cadena de valor, tal y como se referencia en ITIL 4, atendiendo a la denominada cuarta revolución industrial y la transformación digital relacionada.

* 1. **Gestión de las organizaciones basadas en el riesgo**

Ante la gran variedad de posibles opciones de despliegue de los servicios de nube (XaaS) en entornos públicos, privados o híbridos el enfoque de aplicar un conjunto de controles de seguridad preestablecido no es viable desde el punto de vista técnico, ni económico.

Hay que considerar que lo que puede funcionar en un proveedor o en un cliente puede ser ineficiente, inviable o directamente no cobra ningún sentido en otra organización distinta.

Además, la aplicación de controles necesita de recursos para su implementación, mantenimiento y que finalmente se verán reflejados en cifras económicas de gastos operativos.

Otro enfoque habitual es la aplicación de controles técnicos individuales según se van descubriendo situaciones de riesgo que puedan comprometer la información entre el sistema de información proporcionado por el proveedor, los sistemas y las redes de comunicación de los usuarios del cliente de servicios web.

| La nube: un camino ineludible para las empresas | Gestión | Inicialmente, este enfoque puede dar la sensación de un avance progresivo y proporcionado a las necesidades requeridas por la organización, pero ya ha quedado ampliamente demostrado que conduce finalmente a una falta de control y al desgobierno por ser un enfoque reactivo; pero además, por la incertidumbre de cómo los nuevos controles que se implementan acaban afectando la eficacia de aquellos previamente implementados. |
| --- | --- |

El proceso de análisis y evaluación de riesgos habilita a las gerencias a tomar en consideración todos los aspectos de riesgo que son pertinentes al contexto de la actividad de la organización y a sus objetivos estratégicos de modo que, con base en el resultado del proceso que aporta una identificación completa del escenario de riesgos en un informe puedan decidir en su experiencia como gestores (ahora sí) qué situaciones de riesgo no son asumibles, priorizando unas acciones respecto a otras según el impacto financiero, económico, operativo, reputacional y los recursos requeridos para su control efectivo.

* 1. **Metodología de gestión del riesgo**

En primer lugar, se introducirá en este momento algunos términos y definiciones esenciales para poder entender los fundamentos de las metodologías en gestión del riesgo.

Las referencias en este caso están tomadas de la ISO 27000, norma de consenso y alcance internacional, que toma referencias anteriores como la Guía ISO 72:2009 y amplía adicionalmente, proporcionando una visión general de las normas que componen la serie 27000 (como ISO 27017 y 27018 relacionadas con la prestación de servicios de computación en la nube) y que recopila todas las definiciones relevantes a la seguridad de la información de las publicaciones, de manera que en el siguiente recurso didáctico encontrará una explicación al respecto:

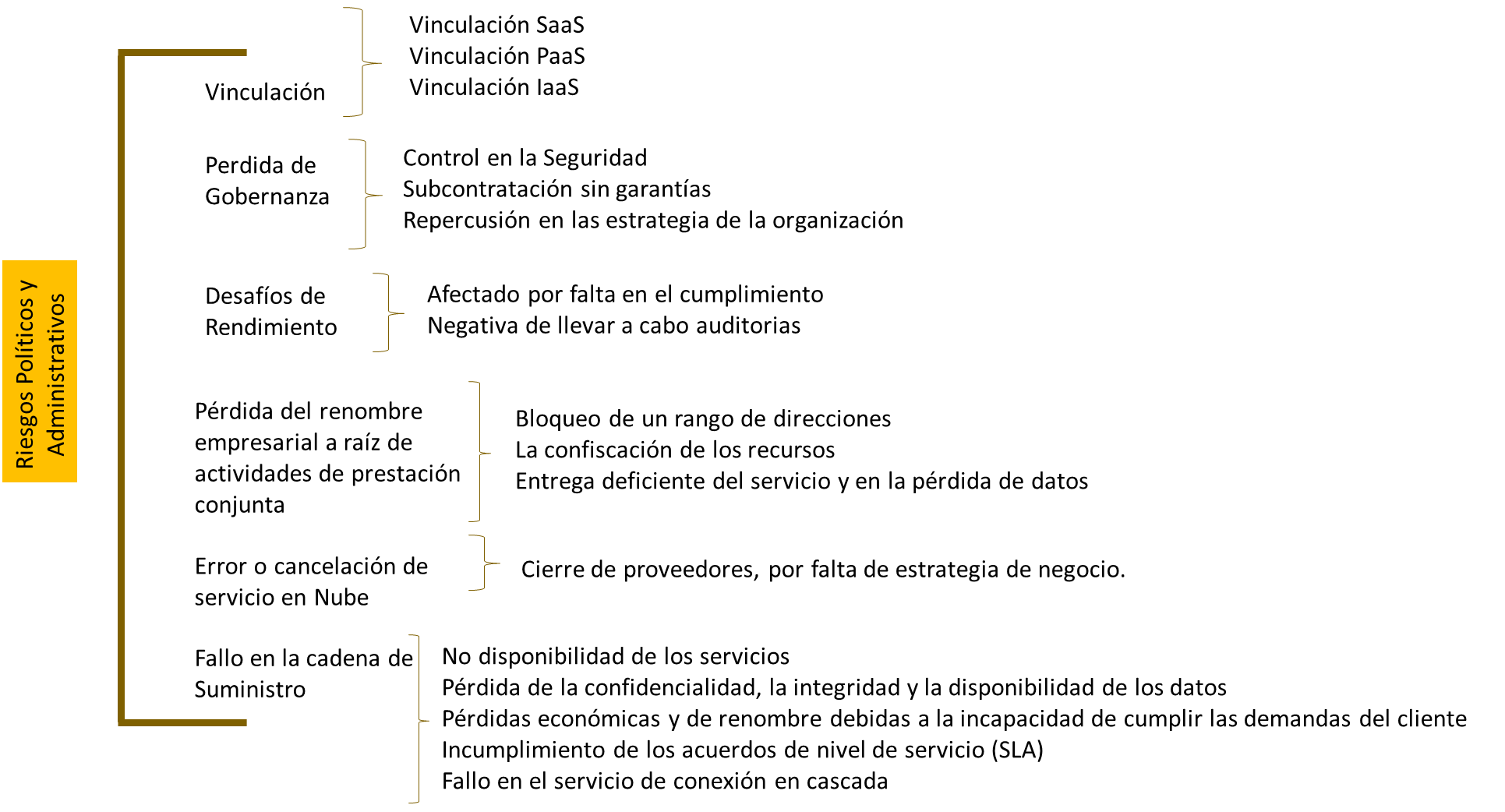


* 1. **Riesgos políticos y administrativos**

A continuación, se presentan los riesgos más comunes que desde el punto de vista administrativo y político se pueden tener al adquirir servicios en la nube; una presentación condensada de estos se aprecia en la siguiente figura:

**Figura 1**

*Riesgos políticos y administrativos*



Un mayor detalle de los aspectos correspondientes a los riesgos políticos y administrativos presentes en la gestión del riesgo se muestran a continuación:

* + 1. ***Vinculación.***

La oferta actual en cuanto a herramientas, procedimientos o formatos de datos normalizados o interfaces de servicio que puedan garantizar la portabilidad del servicio y de los datos es aún escasa, aunque existen algunas iniciativas de estandarización.

Por este motivo, la migración del servicio de un cliente a otro o la migración de datos y servicios desde un entorno de tecnologías de la información interno o al mismo puede ser muy compleja. Además, los proveedores de servicios cloud pueden tener un incentivo para impedir (directa o indirectamente) la portabilidad de los datos o los servicios de sus clientes.

Esta dependencia potencial de la prestación del servicio de un proveedor de servicios cloud concreto, en función de los compromisos del mismo, puede generar un fracaso catastrófico del negocio si el proveedor va a la quiebra y la ruta de migración de la aplicación y el contenido a otro proveedor es demasiado costosa (en términos económicos o temporales) o no se proporciona una alerta suficiente (no hay alerta temprana).

Es importante entender que el grado y la naturaleza de la vinculación varían en función del tipo de nube, que se describe a continuación:



* + 1. ***Pérdida de gobernanza.***

Al utilizar las infraestructuras de nube, el cliente necesariamente cede el control de una serie de cuestiones que pueden influir en la seguridad al proveedor de servicios cloud, por ejemplo, los términos de uso pueden prohibir el escaneado de puertos, la evaluación de vulnerabilidades y las pruebas de penetración. Además, pueden surgir conflictos entre los procedimientos de refuerzo del cliente y el entorno en nube. Por otra parte, puede ocurrir que los acuerdos de nivel de servicio no incluyan la prestación de dichos servicios por parte del proveedor de servicios cloud, dejando así una laguna en las defensas de seguridad.

| Asimismo, el proveedor de servicios cloud puede subcontratar o externalizar servicios a terceros (proveedores desconocidos) que podrían no ofrecer las mismas garantías (como la prestación del servicio de manera legal), ofrecidas por el proveedor o que se produzcan cambios en el control del proveedor de servicios cloud, de modo que provoquen una modificación de los términos y condiciones de sus servicios. | Fullcloud600 - Pérdida De Gobernanza En La Computacion De La Nube, HD Png  Download , Transparent Png Image - PNGitem |
| --- | --- |

La pérdida de gobernanza y control podría repercutir gravemente sobre la estrategia de la organización y por tanto, sobre la capacidad de cumplir su misión y sus objetivos. La pérdida de control y gobernanza podría generar la imposibilidad de cumplir los requisitos en materia de seguridad, la falta de confidencialidad, integridad y disponibilidad de los datos, el deterioro del rendimiento y de la calidad del servicio, por no mencionar la introducción de desafíos de cumplimiento.

* + 1. ***Desafíos de rendimiento.***

Determinadas organizaciones que migran a la nube han realizado inversiones considerables para alcanzar la certificación, bien para lograr una ventaja competitiva o para ajustarse a los requisitos normativos o reglamentarios del sector. Esta inversión puede verse amenazada por la migración a la nube en:



En determinados casos, también significa que el uso de una infraestructura pública de nube implica que no pueden alcanzarse determinados niveles de cumplimiento y por ello, los servicios de alojamiento en la nube no pueden utilizarse para los servicios que los necesitan.



* + 1. ***Pérdida de renombre empresarial por la prestación conjunta.***

Los recursos compartidos implican la posibilidad de que las actividades maliciosas de un prestador puedan afectar el renombre de otro, por ejemplo, el *spam*, el escaneado de puertos o la prestación de contenido malicioso de la infraestructura en nube puede ocasionar:





* + 1. ***Error o cancelación de servicio en la nube.***

Como en cualquier mercado nuevo, la presión de la competencia, una estrategia de negocios inapropiada, la falta de apoyo financiero, etc., pueden provocar el cierre de algunos proveedores o como mínimo, obligarles a reestructurar su oferta de cartera de servicios.

Dicho de otro modo, es posible que a corto o mediano plazo finalicen algunos servicios de computación en la nube. El impacto de esta amenaza para el cliente de servicios cloud es sencillo de entender, ya que puede dar lugar a una pérdida o al deterioro del rendimiento y de la calidad del servicio, así como a una pérdida de la inversión.

Además, los errores en los servicios subcontratados al proveedor de servicios cloud pueden repercutir considerablemente sobre la capacidad del cliente de estos servicios para cumplir sus funciones y obligaciones para con sus propios clientes. Así, este puede encontrarse expuesto a la responsabilidad contractual y extracontractual frente a sus clientes, basándose en la negligencia de su proveedor.

* + 1. ***Fallo en la cadena de suministro.***

Un proveedor de servicios cloud puede subcontratar determinadas tareas especializadas de su cadena «de producción» a terceros. En esta situación, el nivel de seguridad del proveedor de servicios cloud puede estar supeditado al nivel de seguridad de cada enlace y al grado de dependencia de terceros de este.

Cualquier interrupción o corrupción de la cadena, así como la falta de coordinación de las responsabilidades entre las partes implicadas puede ocasionar:



Un ejemplo importante al respecto es la existencia de una dependencia crítica de un servicio de gestión de identidad o de un inicio de sesión único de un tercero. En este caso, la interrupción del servicio del tercero o de la conexión del proveedor de servicios cloud al servicio o las deficiencias de sus procedimientos de seguridad pueden poner en entredicho la disponibilidad o la confidencialidad de un cliente de servicios cloud, o de hecho, de toda la oferta en la nube.

* 1. **Riesgos técnicos**

La seguridad de cloud computing presenta los mismos problemas que los sistemas propios (infraestructura no externalizada), pero adicionalmente han surgido otros nuevos, resultado del uso de nuevas tecnologías implementadas como es la virtualización, las arquitecturas orientadas a servicios o las nuevas aplicaciones, que afectan la prestación del servicio desde lo técnico. Algunos de estos riesgos son:

* **Agotamiento de recursos (prestación excesiva o insuficiente).** Un modelado inadecuado del uso de recursos que pudiera concluir en un agotamiento de recursos, debido a un fallo en los algoritmos de provisión de recursos, en donde se presentan varias características, estas son:



* **Fallo de aislamiento.** La multiprestación y los recursos compartidos son dos de las características que definen los entornos de la computación en nube: la red, el almacenamiento y la capacidad de computación son compartidos entre múltiples usuarios.

| Almacenamiento en la nube, qué nos preocupa y cómo se puede solucionar |  SMiD Cloud, secure encryption solutions | Este tipo de riesgos incluye los errores de los mecanismos que separan el almacenamiento, la memoria, el enrutamiento e incluso el renombre entre distintos arrendatarios de la infraestructura compartida (por ejemplo, los denominados ataques de «*guest-hopping*», los ataques por inyección SQL que exponen los datos de múltiples clientes almacenados en la misma tabla y los ataques por vía alternativa).  Cabe señalar que la probabilidad de que se produzca este escenario de incidentes depende del modelo de nube considerado; es probable que sea bajo para las nubes privadas y algo mayor en el caso de nubes públicas. El impacto puede ser una pérdida de datos sensibles o valiosos, perjuicios para el renombre e interrupción del servicio para el proveedor de servicios cloud y sus clientes. |
| --- | --- |

* En relación a los **miembros maliciosos de un proveedor de servicios cloud, abuso de funciones privilegiadas.** Es de anotar que las actividades maliciosas pueden repercutir sobre la confidencialidad, la integridad y la disponibilidad de todos los tipos de datos, IP, todos los tipos de servicios y, por tanto, indirectamente sobre el renombre de la organización, la confianza del cliente y las experiencias de los empleados.

Este aspecto puede considerarse especialmente importante en el caso de la computación en la nube, debido a que las arquitecturas en la nube necesitan determinadas funciones de alto riesgo. Entre los ejemplos de estas funciones se incluyen los administradores de sistema de los proveedores de servicios cloud y los proveedores de servicios de seguridad gestionada que se ocupan de los informes de detección de intrusiones y de las respuestas a los incidentes.



* **Compromiso de interfaz de gestión (manipulación, disponibilidad de la infraestructura).** Las interfaces de gestión de cliente de un proveedor de servicios *cloud* público son accesibles a través de Internet, y canalizan el acceso a conjuntos de recursos más grandes (que los proveedores tradicionales de alojamiento), por lo que plantean un riesgo mayor, especialmente cuando se combinan con el acceso remoto y las vulnerabilidades del navegador de web.

Aquí se incluyen las interfaces de cliente que controlan una serie de máquinas virtuales, y lo que es más importante, interfaces de proveedor de servicios cloud que controlan el funcionamiento de todo el sistema en la nube. Es evidente que los proveedores pueden mitigar este riesgo incrementando la inversión en seguridad.

* **Interceptación de datos.** Al ser una arquitectura distribuida, la computación en la nube implica más datos en tránsito que las infraestructuras tradicionales, por ejemplo, los datos deben transferirse para sincronizar múltiples imágenes de máquinas distribuidas, imágenes distribuidas entre múltiples máquinas físicas, entre la infraestructura de la nube y los clientes remotos de web, etc.

| Además, la mayor parte del uso del alojamiento de los centros de datos es implementada a través de un entorno de conexión segura de tipo VPN, una práctica que no siempre se sigue en el contexto de la nube. | PELIGRO EN LA WEB: Articulo 269C |
| --- | --- |

Los programas espía, la falsificación de IP, los ataques con intermediarios (MITM – Man in the Middle), los ataques por vía alternativa y los ataques en repetición deben considerarse posibles fuentes de amenaza. Además, en ocasiones, el proveedor de servicios cloud no ofrece una cláusula de confidencialidad o de no divulgación o si lo hace, dichas cláusulas no ofrecen garantías suficientes de protección de la información secreta y los conocimientos del cliente que circularán por la nube.

Asociado a este tipo de riesgo se puede presentar otro llamado **Fuga** **de datos** durante la carga/descarga dentro de la nube que se puede ocasionar durante la transferencia de datos entre el proveedor de servicios cloud y el cliente.

* **Eliminación de datos no segura o no eficaz.** Cuando se cambia de proveedor los recursos se escalan de forma descendente, el *hardware* físico se reubica, etc., y los datos pueden estar disponibles más allá de la vida indicada en la política de seguridad.



Cuando se realiza una solicitud para suprimir un recurso en nube, en ocasiones el proceso no elimina definitivamente los datos (al igual que con la mayoría de los sistemas operativos). Si se requiere una supresión total de los datos es necesario seguir procedimientos especiales, y puede que la API estándar no soporte esta función (o no pueda realizarse de ningún modo). Si se utiliza una codificación satisfactoria, el nivel de riesgo puede considerarse inferior.

* **Denegación de servicios.** En los últimos años hemos visto un aumento en el uso de ataques de Denegación de Servicio (DOS) y Denegación de Servicio Distribuido contra varias organizaciones. El ataque de DOS es cuando los atacantes envían algo de tráfico a los sistemas de destino que ya no pueden proporcionar el servicio a los usuarios legítimos. Las organizaciones de clientes deben determinar qué herramientas de mitigación y protección requieren para garantizar el acceso al servicio de cloud.
* **Denegación económica de servicio.** Existen distintos escenarios en los que los recursos del cliente de servicios cloud pueden ser utilizados por terceros de forma maliciosa, ocasionando repercusiones de índole económica, entre las consecuencias están:



* **Pérdida de las claves o certificados de seguridad.** Aquí se incluye la divulgación de las claves secretas (SSL, codificación de archivos, claves privadas del cliente, etc.) o las contraseñas a las partes maliciosas, la pérdida o corrupción de dichas claves o su uso indebido para la autenticación y el no repudio (firma digital).
* **Realización de escaneos o mapeos de redes y servicios.** El escaneado o la detección maliciosa, así como el mapeo de redes, son amenazas indirectas a los activos en cuestión, pueden utilizarse para recabar información en el contexto de un intento de piratería. Uno de los posibles resultados podría ser la pérdida de la confidencialidad, integridad y disponibilidad de los servicios y datos.
* **Compromiso del motor de servicio.** Cada arquitectura de nube descansa en una plataforma altamente especializada: el motor de servicio que se sitúa por encima de los recursos físicos de *hardware* y gestiona los recursos del cliente con distintos niveles de abstracción, por ejemplo, en la nube IaaS, este componente del *software* puede ser el hipervisor.

Este motor de servicio está desarrollado y soportado por los distribuidores de la plataforma en la nube y la comunidad de código abierto en algunos casos. Los proveedores de computación en la nube pueden personalizarlo todavía más.

| Ilustración de concepto abstracto de motor basado en la nube | Vector Gratis | Como cualquier otra capa de *software*, el código del motor de servicio puede tener vulnerabilidades, y es proclive a sufrir ataques o errores inesperados. Un atacante puede poner en peligro el motor de servicio, accediendo a él sin autorización desde dentro de una máquina virtual (nube IaaS), el entorno de ejecución (nube PaaS), el conjunto de la aplicación (nube SaaS) o a través de sus API. |
| --- | --- |

El acceso no autorizado al motor de servicio puede servir para escapar al aislamiento entre distintos entornos de cliente (*jailbreak*) y acceder a los datos contenidos en los mismos, controlarlos y modificar la información almacenada dentro de los mismos de forma transparente (sin que haya una interacción directa con la aplicación dentro del entorno del cliente) o reducir los recursos asignados a los mismos, ocasionando una denegación del servicio.

* 1. **Riesgos legales**

Además de la pérdida de información o la intervención malintencionada de terceros, existen otros riesgos que amenazan seriamente los datos almacenados de las organizaciones, bien sea por la intervención directa de una orden judicial, por la pérdida de autonomía de ejecución dentro del territorio, la intrusión a la privacidad de los usuarios e incluso al caducar las licencias. Algunos de estos riesgos de orden legal se explican a continuación:



* 1. **Riesgos relacionados con la nube**

Durante este componente se identifican las siguientes amenazas no específicas de la computación en la nube, pero que deben considerarse detenidamente a la hora de evaluar el riesgo de un sistema típico basado en la nube, de igual manera, se identifican una serie de vulnerabilidades que pueden ocasionar amenazas y riesgos que afectan los datos y servicios a través de la nube, vea esta información a través de los siguientes puntos:



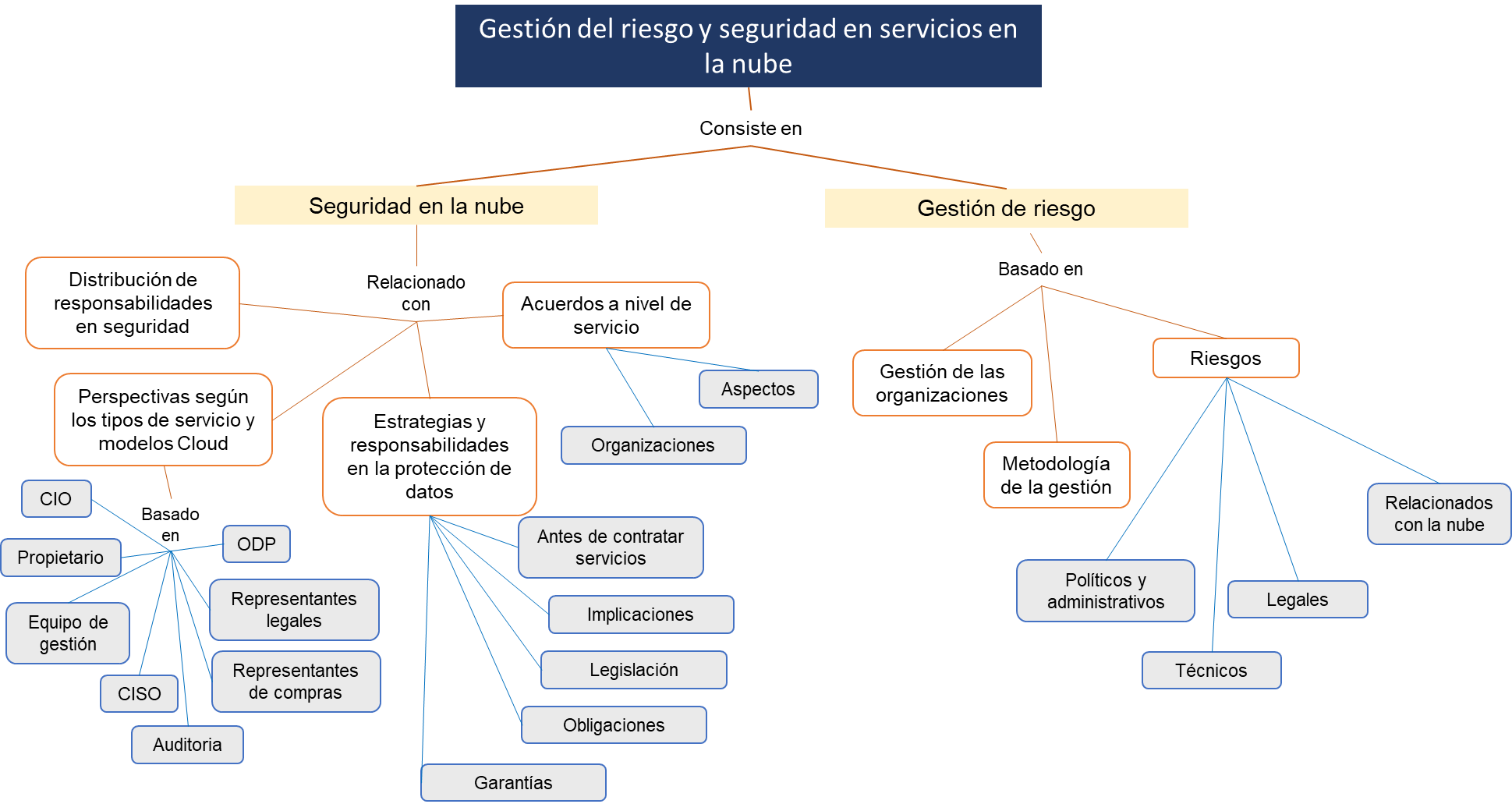
**Síntesis**

El uso de diversas tecnologías que ofrezcan disponibilidad de múltiples combinaciones, acordes con los cambios que se ven en la economía, la administración e incluso en las políticas públicas, no siempre van de la mano, aunque en la actualidad las organizaciones pequeñas y grandes cada vez demandan más su implementación. Vea que un término en boga es el cloud computing o computación en la nube, que permite entre otras cosas gestionar información de manera remota, su demanda cada vez va en aumento, en donde un conjunto de recursos informáticos configurables se encuentran dispuestos, con un mínimo de esfuerzo e incluso algunas veces sin proveedor de servicios en la nube.

No obstante y pese a la reducción de costos de operación, escalabilidad, reducción de costos de obsolescencia tecnológica, acceso a tecnología de punta e incluso rápida recuperación de información se encuentran algunos riesgos de cuidado que, si no son atendidos de manera temprana, pueden afectar el objetivo y propósito de la empresa al no contemplarlos cuando se lleva a cabo la implementación.

Todos los temas de seguridad tradicionales permanecen, pero la naturaleza de los riesgos, roles, responsabilidades y la implementación de los controles cambian, aunque el alcance general de la seguridad y el cumplimiento no lo haga, pueden agregarse nuevos actores o se hace redistribución de responsabilidades, pero es el controlador el de la información quien deberá estar presente y pendiente de minimizar los fallos, con el fin de generar un óptimo servicio.

Basado en lo anterior, en el siguiente mapa conceptual, podrá tener un repaso breve de los contenidos vistos en este componente formativo:



1. **Actividades didácticas (opcionales si son sugeridas)**

| **Descripción de la actividad didáctica** | |
| --- | --- |
| **Nombre de la actividad** | Sopa de letras |
| **Objetivo de la actividad** | Afianzar algunos de los conceptos más importantes de los riesgos y la seguridad en servicios cloud. |
| **Tipo de actividad sugerida** | Buscar las palabras ocultas en la sopa de letras. |
| **Archivo de la actividad**  **(Anexo donde se describe la actividad propuesta)** | Anexos / Actividad\_didáctica\_3 |

1. **Material complementario**

| **Tema** | **Referencia APA del material** | **Tipo de material**  **(video, capítulo de libro, artículo, otro)** | **Enlace del recurso o**  **archivo del documento o material** |
| --- | --- | --- | --- |
| Seguridad en la nube | Decreto 1377 de 2013. [Presidencia de la República de Colombia]. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Junio 27 de 2013. <http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1276081> | Decreto | <http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1276081> |
| Seguridad en la nube | Red Iberoamericana de Protección de Datos. (2021). *Legislación.* Red Iberoamericana. <https://www.redipd.org/es/legislacion?nid=83> | Página web | <https://www.redipd.org/es/legislacion?nid=83> |
| Seguridad en la nube | Superintendencia de Industria y Comercio. Colombia. (s.f.). *Guía para la implementación del principio de responsabilidad demostrada.* Superintendencia de Industria y Comercio. <https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf> | Documento | <https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf> |

1. **Glosario**

| **Término** | **Significado** |
| --- | --- |
| ***Accountability*** | Habilidad de asumir responsabilidades y su importancia en las empresas. |
| **Amenaza (*Threat*)** | Es la causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. |
| ***Blockchain*** | Economía de bloques es una tecnología que permite crear redes de dispositivos sin la necesidad de un servidor central y localizado para conectarlos entre sí. Podría decirse que funciona como un libro de cuentas donde se registran las operaciones de compra, venta o cualquier transacción. |
| ***CIO (Chief Security Officer*** | Responsable del área de informática. |
| **CISO** | Responsable de la seguridad de la información, su función principal es evaluar las prácticas de seguridad del proveedor de servicios en la nube, en relación con el tipo de datos que se trate y la criticidad del servicio para el negocio. |
| ***Compliance*** | Es, según el Comité de Basilea, “una función independiente que identifica, asesora, alerta, monitorea y reporta los riesgos de cumplimiento en las organizaciones”. Además, también se entiende como el riesgo de recibir sanciones, sufrir pérdidas financieras o de reputación. |
| **DDoS** | Ataques de denegación de servicios distribuidos. |
| ***Hacking*** | Es el conjunto de técnicas a través de las cuales se accede a un sistema informático, vulnerando las medidas de seguridad establecidas originalmente. |
| **ISO 27000** | Las normas que forman la serie ISO/IEC-27000 son un conjunto de estándares creados y gestionados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC). Ambas organizaciones internacionales están participadas por multitud de países, lo que garantiza su amplia difusión, implantación y reconocimiento en todo el mundo.  Las series 27000 están orientadas al establecimiento de buenas prácticas en relación con la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI). |
| ***Malware*** | *Software* malicioso. |
| **ODP** | Oficial de datos personales, persona o área responsable de la atención de peticiones, consultas y reclamos, ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización. |
| ***Randsomware*** | El *malware* de rescate o *ransomware*, es un tipo de *malware* que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. |
| **Riesgo** | Se define como el efecto de la incertidumbre sobre los objetivos. |
| **Vulnerabilidad (*Vulnerability*)** | Es la debilidad de un activo o control que puede ser explotada por una o más amenazas. |
| **XaaS** | Despliegue de servicios en la nube. |

1. **Referencias bibliográficas**

Aspectos profesionales: protección de datos, cloud computing y sistemas de gestión. (2012). *Cláusulas contractuales en entornos de cloud computing.* [Blog]. <http://www.aspectosprofesionales.info/2012/10/clausulas-contractuales-en-entornos-de.html>

Brun, L. y Bellanova, R. (2018). *The role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity*. Université Catholique de Louvain.

Ferma. (2003). *Estándares de gerencia de riesgos.* Ferma. <https://www.theirm.org/media/6836/rm_standard_spanish_15_11_04-1.pdf>

ISO/IEC 27005:2018(en) Information technology — Security techniques — Information security risk management. (2021). *Foreword*. <https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en>

ISO 31000. (2021). *Risk management*. <https://www.iso.org/iso-31000-risk-management.html>

Samarati, P., Di Vimercati, S., Murugesan, S. & Bojanova, I. (2016). Cloud security: Issues and concerns. *Encyclopedia on cloud computing*, p. 1-14.

Swain, B., Pohlman, M. y Posey, L. (2010). *Cloud Security Alliance GRC Stack Training*.

1. **Control del documento**

|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** |
| --- | --- | --- | --- | --- |
| **Autor (es)** | Henry Eduardo Bastidas Paruma | Instructor experto temático | Regional Cauca - Centro de Teleinformática y Producción Industrial | Noviembre 2021 |
| María Inés Machado López | Diseñadora instruccional | Regional Distrito Capital - Centro de Diseño y Metrología | Diciembre 2021 |
| Andrés Felipe Velandia Espitia | Revisor metodológico y pedagógico | Regional Distrito Capital – Centro de Diseño y Metrología | Diciembre 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor pedagógico Ecosistema RED | Regional Santander - Centro Industrial del Diseño y la Manufactura | Diciembre 2021 |
| Julia Isabel Roberto | Diseñadora y evaluadora instruccional | Regional Distrito Capital – Centro para la Industria de la Comunicación Gráfica | Diciembre 2021 |

1. **Control de cambios**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** | **Razón del cambio** |
| --- | --- | --- | --- | --- | --- |
| **Autor (es)** |  |  |  |  |  |