Seguridad en la Nube

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía No. 12

MINTIC vive digital Colombia TODOS POR UN NUEVO PAÍS PAZ EQUIDAD EDUCACIÓN

HISTORIA

VERSIÓN	FECHA	CAMBIOS INTRODUCIDOS
1.0.0	20/05/2015	Versión inicial del documento
1.0.1	14/03/2016	Revisión del documento

TABLA DE CONTENIDO

PÁG.

1. DERECHOS DE AUTOR

2. AUDIENCIA

Entidades públicas de orden nacional y entidades públicas del orden territorial, así como proveedores de servicios de Gobierno en Línea, y terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea.

3. INTRODUCCIÓN

Este documento, presenta los lineamientos y aspectos a tener en cuenta para el aseguramiento de la información en la nube – Cloud; que las Entidades del Estado deben seguir, de tal manera que se conserve la seguridad de los datos en este tipo de ambientes.

La correcta implementación del servicio de información en la Nube de la Entidad, reducirá el riesgo de que se presenten incidentes de seguridad que afecten la imagen de la entidad y generen un daño irreparable.

Este documento provee a las entidades del estado recomendaciones para minimizar los riesgos, que se obtienen al tener información en la Nube, ya sea información relevante o no. Las opciones de Cloud pueden ser pública o privada almacenamiento interno y/o externo, mixto, entre otros. Los controles de seguridad variar dependiendo de las circunstancias. De igual manera las entidades deben realizar sus migraciones de información a la Nube basadas en el análisis de riesgos; esto permite tomar las decisiones apropiadas.

4. GLOSARIO

- **Cloud Computing**: Es un nuevo concepto tecnológico que se basa en que las aplicaciones software y los equipos hardware con capacidad de proceso y almacenaje de datos que están ubicado en un Datacenter que permite a los usuarios acceder a las aplicaciones y servicios disponibles a través de Internet o como se conoce coloquialmente a través “la Nube” de Internet, de una forma sencilla y cómoda.

- **Clúster**: Conjunto de servidores que trabajan como una única maquina mejorando el desempeño de las transacciones y operaciones implantadas en este sistema.

- **CPD**: Centros de Procesamiento de Datos, ubicación física donde se concentran todos los equipos electrónicos necesarios para el procesamiento de la información de una organización.

- **CRM**: “Customer Retationship Management”. Gestión de la Relación con el Cliente, son herramientas informáticas dedicadas a la gestión integrada de información sobre clientes. Estas aplicaciones permiten, desde almacenar y organizar esta información, hasta integrar, procesar y analizar la misma.

- **Data Center**: Un centro de almacenaje de datos y que provee servicios de negocio que entrega de forma segura aplicaciones y datos a usuarios remotos a través de Internet.

- **ISO27001**: Estándar para la seguridad de la información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según la metodología del Plan-Do-Check-Act (Planificar-Hacer-Verificar-Actuar).

- **Multitenancy**: Uso común entre todos los clientes y usuarios de los servicios de computación en la nube desde la misma plataforma tecnológica del proveedor contratado.

- **On-demand**: Término referido al concepto de —bajo demanda. Dentro del ámbito tecnológico se utiliza para expresar la flexibilidad de los productos cloud, basados en un modelo de pago por uso y en los cuales el proveedor pone a disposición del cliente todos sus recursos, pudiéndolos usar bajo petición previa.

- **SLA**: “Service Level Agreement” o “Acuerdo de Nivel de Servicio”. Es un protocolo plasmado normalmente en un documento de carácter legal por el que

una compañía que presta un servicio a otra se compromete a hacerlo bajo determinadas condiciones y con unas prestaciones mínimas.

5. IDENTIFICACIÓN Y ANALISIS DE RIESGOS EN LA NUBE

Con el análisis de Riesgo, los objetivos misionales y funcionales de la Entidad, así como la estrategia de TI para apoyar dichas actividades, es de vital importancia para la toma de decisiones de lo que se debe o puede migrar a la Nube. Estos pueden ser:

- ✓ Datos.
- ✓ Servicios.
- ✓ Aplicaciones.
- ✓ Funcionalidades o Procesos.

Una de las actividades más importante es la evaluación de riesgo de los activos que voy a mover a la nube, en esta la entidad identifica los datos y funcionalidades a mover. También debe tener presente el aumento de tráfico, operaciones y datos; los cuales pueden ser mayores de lo revisado.

Identificar que tan importantes son las operaciones y/o datos para la entidad; donde se determine que tan confidencial es la información, el proceso, la operación o función a migrar. La entidad puede realizar una autoevaluación a través de preguntas sencillas donde identifique el valor de los activos en términos de confidencialidad, disponibilidad, integridad y su riesgo asociado al llevar los datos a la nube parcial o totalmente.

Por ejemplo: Que impacto tendría en la entidad si:

- ✓ El activo estuviera expuesto públicamente
- ✓ Un funcionario del tercero o proveedor accediera al activo
- ✓ Un proceso fuera modificado por un externo
- ✓ Un proceso o alguna de sus funciones entregaran resultados erróneos
- ✓ Si la información o datos fueran modificados de manera inesperada
- ✓ Si se presentaran fallas de disponibilidad

6. DEFINICION DE CLOUD COMPUTING

Cloud Computing es un modelo que proporciona acceso a unos recursos de computación configurable. Por ejemplo redes, servidores, almacenamiento, aplicaciones y servicios.

"Cloud computing" es un nuevo modelo de prestación de servicios de negocio y tecnología, que permite incluso al usuario acceder a un catálogo o, de forma flexible y adaptativa, en caso de demandas no previsibles o de picos de trabajo, pagando únicamente por el consumo efectuado, o incluso gratuitamente en caso de proveedores que se financian mediante publicidad o de organizaciones sin ánimo de lucro." [1]

El NIST define Cloud computing mediante la descripción de cinco características esenciales, tres modelos de servicio en Cloud y cuatro modelos de despliegue para Cloud.

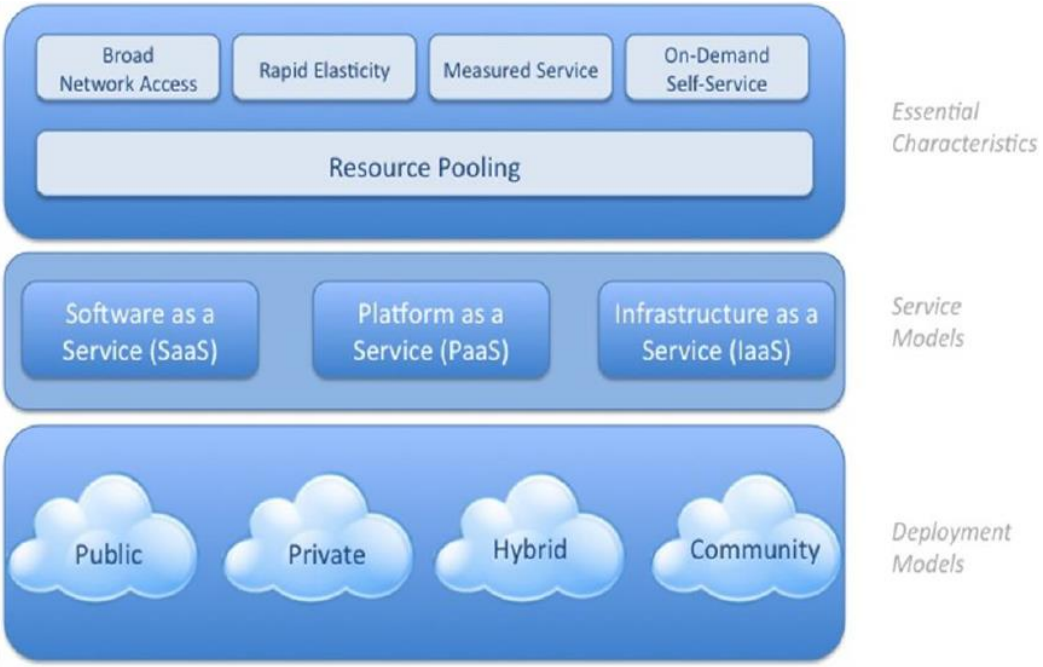

Figura 1: Modelo visual de cloud computing según NIST

[1] https://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube

7. CARACTERISTICAS DEL SERVICIO

La característica principal es la disponibilidad de la información; con el servicio de Cloud se proporciona el acceso, lo que permite un ahorro de costos en la Entidad.

7. 1 CARACTERISTICAS ESENCIALES:

- ✓ **Auto servicio a demanda**: El usuario o cliente puede ajustar la capacidad necesaria de forma unilateral, sin necesidad de involucrar al personal del proveedor. Es decir tiene acceso a la parametrización del servicio y su disponibilidad.
- ✓ **Amplio acceso a través de redes**: Acceso estándar a través de diferentes medios, habilitando todo tipo de dispositivos de acceso: teléfonos, tablets, portátiles, equipos personales, servidores, etc.
- ✓ **Recursos compartidos**: Los recursos del proveedor o tercero se agregan y se ponen a disposición de múltiples clientes para su uso compartido. La incorporación incluye equipos físicos y equipos virtuales que se asignan dinámicamente bajo demanda. El cliente o la entidad se independizan de la ubicación física de los recursos, aunque puede delimitar ubicaciones a un cierto nivel de abstracción (país, estado, etc.).
- ✓ **Aplicación inmediata**: La capacidad requerida puede provisionarse rápida y dinámicamente para seguir las variaciones de la demanda. Desde el punto de vista del consumidor, los recursos parecen ilimitados, pudiendo disponer de cualquier volumen en cualquier momento.
- ✓ **Servicio consumido**: El proveedor o tercero puede controlar el servicio prestado efectivo en cada momento, al nivel que se especifique por contrato; por ejemplo, capacidad de almacenamiento, capacidad de procesamiento, ancho de banda, cuentas de usuario, etc. El uso de recursos puede ser monitorizado, controlado y reportado, proporcionando transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

Hay que mencionar que si la entidad lleva sus servicios a la Nube, tercerizando diferentes tareas de gestión de TI; nunca debe perder el control sobre la información y sobre la seguridad. Antes de contratar este tipo de servicios es primordial evaluar las condiciones del servicio y las medidas de seguridad aplicadas; es decir, que las condiciones sean las adecuadas para garantizar el servicio y la protección de la información de la entidad.

7.2 MODELOS DE DESPLIEGUE

Los escenarios de servicios en la nube, se han clasificado en infraestructuras públicas, privadas, comunitarias o híbridas; así:

- ✓ **Nube pública**: La infraestructura de esta nube está disponible para el público en general o para un gran grupo de industria y dicha infraestructura la controla un proveedor de servicios en la nube.
- ✓ **Nube privada**: La infraestructura de esta nube es operada únicamente por y para una organización.
- ✓ **Nube comunitaria**: La infraestructura de esta nube es compartida por varias organizaciones relacionadas entre ellas y que comparten requisitos de servicio. Uno de sus miembros controla los recursos.
- ✓ **Nube híbrida**: Es la composición de dos o más modelos, por ejemplo privada y pública, que permanecen como entidades únicas pero que coexisten por tener tecnología que permite compartir datos o aplicaciones entre las mismas.

7. 3 MODELOS DE SERVICIO

- ✓ **SaaS (Software as a Service)**. El proveedor del servicio es el encargado de ofrecer al cliente o a la entidad el software como un servicio. Las aplicaciones son accesibles desde diferentes dispositivos a través de una interfaz de cliente liviano, un típico ejemplo es un servicio en un entorno Web; el cliente no administra ni controla la infraestructura en que se basa el servicio que utiliza. Las aplicaciones de ofimáticas a las que se puede acceder online son otro ejemplo.
- ✓ **PaaS (Platform as a Service)**. El proveedor del servicio se encarga de entregar una plataforma a la entidad cliente. El cliente no administra ni controla la infraestructura, pero tiene el control sobre las aplicaciones instaladas y su configuración, y puede incluso instalar nuevas aplicaciones.
- ✓ **IaaS (Infrastructure as a Service)**. El proveedor del servicio se encarga de entregar una infraestructura a la entidad, normalmente mediante una plataforma de virtualización. El proveedor se encarga de la administración de la infraestructura y el cliente tiene el control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas, así como el control de los componentes de red virtualizados.

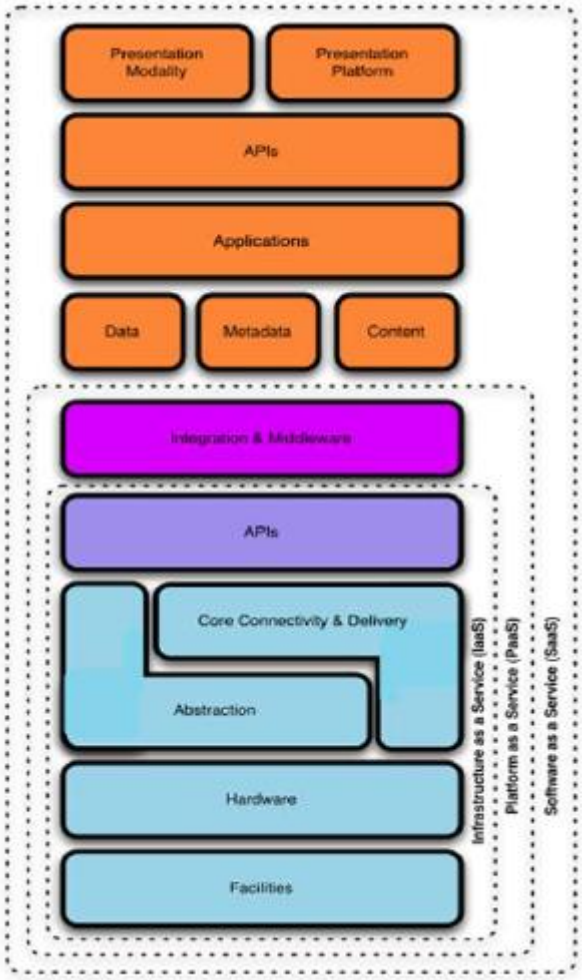

Figura 2: Modelo de servicios según CSA

En conclusión, de acuerdo al modelo de servicio contratado, conforme va incrementándose el nivel de abstracción disminuye el control que la entidad tiene sobre la infraestructura. Del mismo modo cuanto mayor control tiene la entidad sobre la infraestructura que proporciona el servicio, mayor nivel de seguridad y control puede aplicar sobre ésta y por tanto sobre la información tratada.

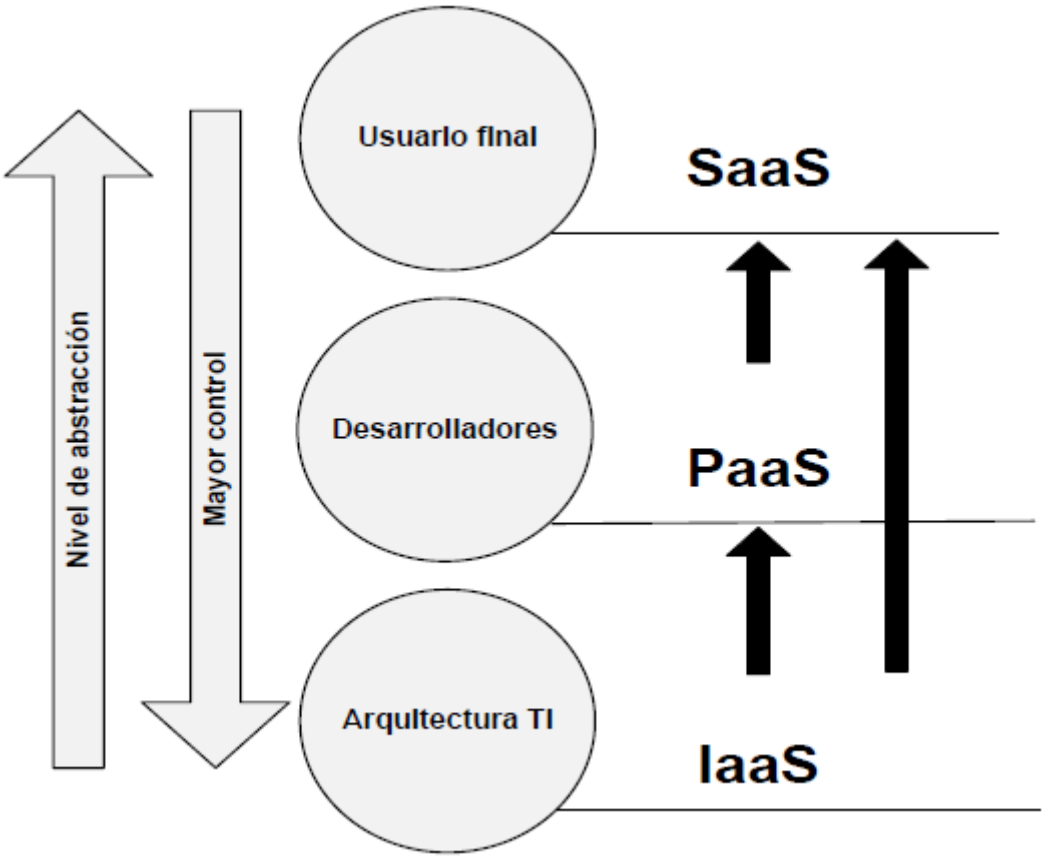

Figura 3: Control de Seguridad según CCN

8. ASPECTOS DE SEGURIDAD DE LA INFORMACION

Hay aspectos importantes que la entidad debe tener presente como la implementación de los servicios, donde se puede confundir Cloud público o privado con externo o interno. Los límites de seguridad del Cloud pueden diferir de los perímetros de seguridad de la entidad.

La implementación y el uso del Cloud deben ser evaluadas no sólo en el contexto "interno" y "externo" en lo que respecta a la ubicación física de los activos, los recursos y la información, sino también por quienes están siendo usados, así como quién es responsable de su gobierno, seguridad y cumplimiento con las políticas y estándares.

Esto no quiere decir que el hecho de que un activo, un recurso o la información estén ubicados dentro o fuera de las instalaciones no afecte a la seguridad y a la exposición al riesgo de una organización, porque sí que afecta, pero se pretende enfatizar que el riesgo también depende de:

- ✓ Los tipos de activos, recursos e información que están siendo gestionados
- ✓ Quién los gestiona y cómo
- ✓ Qué controles se han seleccionado y cómo han sido integrados
- ✓ Aspectos relacionados con el cumplimiento legal

En el ejercicio de clasificación de los activos y los servicios de la entidad se debe planificar su arquitectura de seguridad, de tal manera que se ajuste con los objetivos de la entidad, la regulación y el cumplimiento legal; es decir un ejercicio de análisis GAP. El resultado permite determinar la disposición de seguridad de un servicio y cómo se relaciona con la seguridad de un activo y los requisitos de protección.

Si la entidad es propietaria y administra la infraestructura Cloud, debe estar adecuada a la normatividad que le aplica; si dicha infraestructura es administrada por un operador, esta debe cumplir con los requisitos establecidos en la normatividad y debe cumplir con los niveles de seguridad adecuados para los servicios que presta la Entidad.

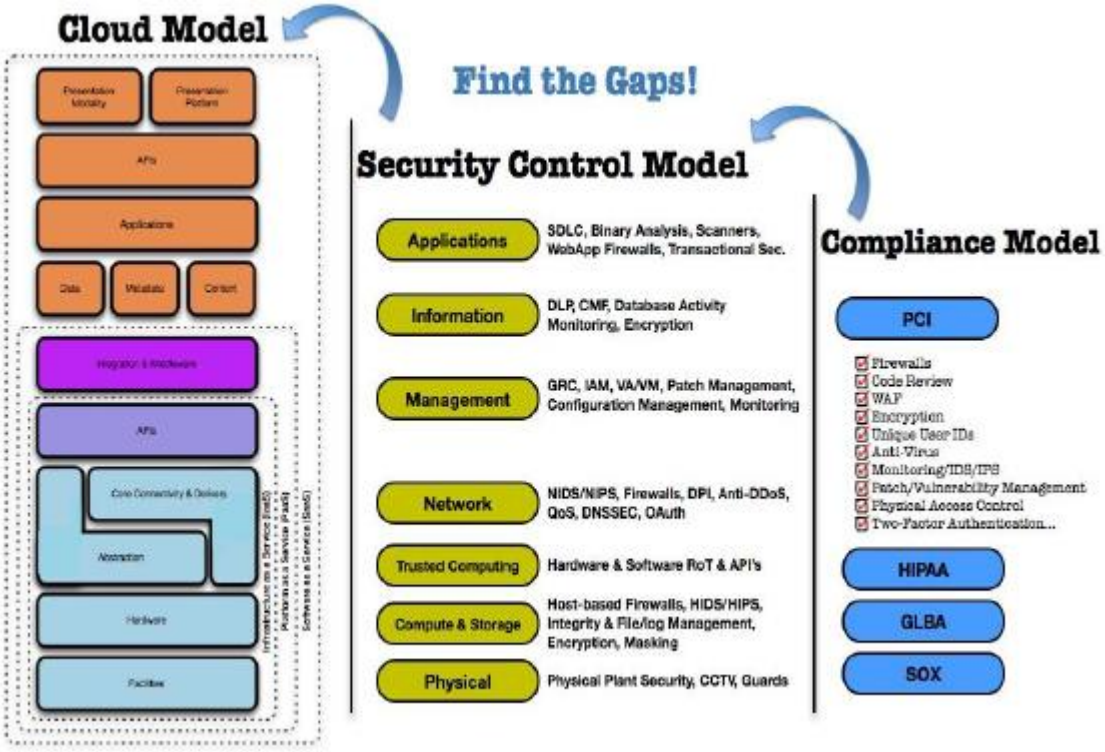

Figura 4: Modelo Cloud para el control de Seguridad y el Cumplimiento - CSA

9. CICLO DE VIDA DE LA SEGURIDAD DE LOS DATOS

El ciclo de vida de los datos es necesario para entender y gestionar la información en la entidad, dicha gestión incluye los procesos y políticas para comprender cómo se usa la información y cómo se gobierna su uso.

Figura 5: ciclo de vida de seguridad de los datos

El ciclo de vida tiene seis fases, desde la creación hasta la destrucción; su progreso se ve lineal pero no necesariamente pasan por todas las etapas después de su creación.

- ✓ **Creación**: Creación es la generación de nuevo contenido digital, o la alteración, actualización o modificación de contenido existente.
- ✓ **Almacenamiento**: Almacenamiento es el proceso de ubicar los datos digitales en algún tipo de repositorio de almacenamiento y normalmente ocurre de forma prácticamente simultánea a su creación.
- ✓ **Uso**: Los datos son visualizados, procesados, o utilizados de otro modo en algún tipo de actividad, no incluyendo su modificación.
- ✓ **Compartir**: La información se hace accesible a otros, tales como otros usuarios, clientes, y colaboradores.
- ✓ **Archivado**: Los datos dejan de ser usados activamente y entran en un almacenamiento de largo plazo.
- ✓ **Destrucción**: Los datos son destruidos de forma permanente usando medios físicos o digitales.

9.1 LOCALIZACION Y ACCESO

Localización: La entidad debe tener claro la ubicación de sus datos, de su información, donde se tiene un ciclo de vida no de manera lineal sino como una serie de procesos más pequeños, funcionando en diferentes entornos operativos. Los datos pueden moverse prácticamente, en cada fase, dentro, fuera o entre esos entornos. En dichos entornos se debe tener claro la regulación, los efectos contractuales y jurídicos; por esto es importante entender tanto la localización lógica como física de los datos.

Acceso: Una vez que los usuarios saben dónde residen los datos y cómo se mueven, necesitan saber quién está accediendo a ellos y cómo. Aquí la entidad debe tener en cuenta dos elementos:

1. ¿Quién accede a los datos?

2. ¿Cómo pueden acceder a ellos (dispositivo y canal)?

Hoy en día la información de la entidad es accedida mediante una variedad de dispositivos. Estos dispositivos tienen diferentes características de seguridad y pueden utilizar diferentes aplicaciones o clientes.

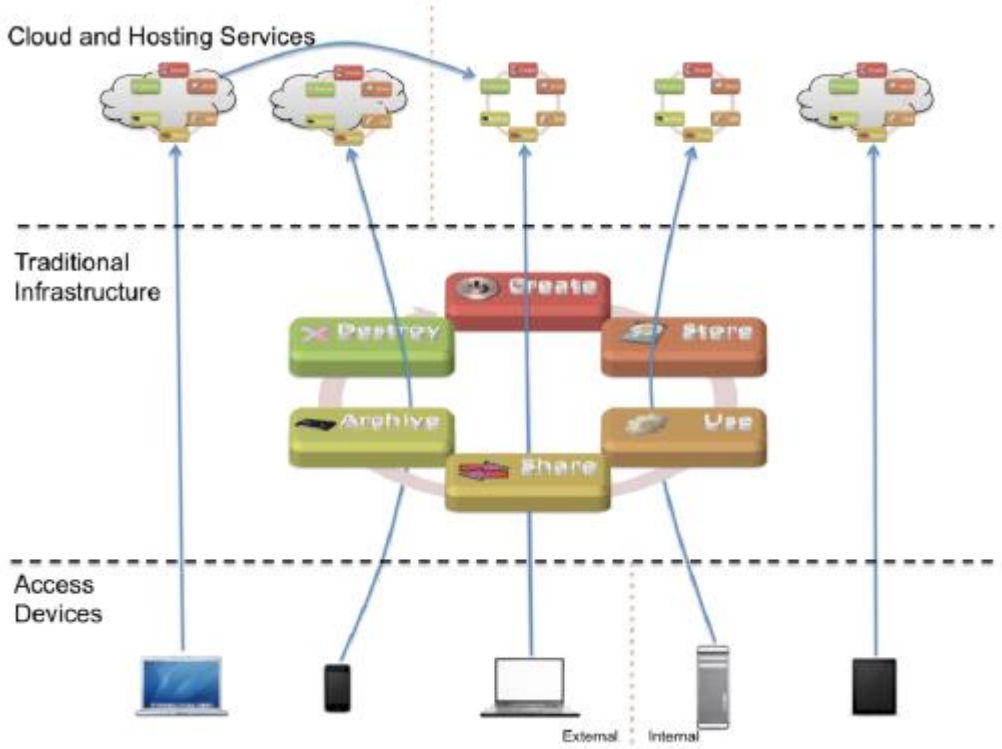

Figura 6: localización y acceso

9.2 FUNCIONES, ACTORES Y CONTROLES

La entidad debe tener claro que se puede hacer con la información y los datos, quien la accede y como la debe controlar.

Hay tres funciones que se pueden hacer con los datos:

- ✓ **Acceder**: Ver/acceder al dato, incluyendo crearlo, copiarlo, transferir el archivo, separarlo, y otros intercambios de información.
- ✓ **Tratar**: Realizar una transacción con el dato: actualizarlo, usarlo en una transacción de la entidad, etc.
- ✓ **Almacenar**: Guardar el dato (archivarlo, base de datos, etc.).

Actor: (persona, aplicación, o sistema/proceso) realizan funciones en donde se ubica la información.

Controles: Un control restringe una lista de posibles acciones a las acciones permitidas.

9.2.1 SUBCONTRATACION

Cuando el proveedor contrata a un tercero como soporte de sus servicios. Por ejemplo:

- ✓ Contratación de personal
- ✓ Contratación de instalaciones
- ✓ Contratación de servicios de comunicaciones
- ✓ Contratación de servicios de copias de respaldo

Las subcontrataciones deben ser informadas y aceptadas por la parte contratante.

Las obligaciones del proveedor en materia de seguridad se transmiten de forma transitiva a las partes subcontratadas. En particular los niveles de seguridad de la información a la que tenga acceso el proveedor, y de los servicios que de este último dependan. La parte subcontratada deberá atender a los requisitos de seguridad derivados.

10. GOBIERNO DE LA INFORMACION

La entidad debe tener gobierno sobre la información, esto incluye las políticas y procedimientos para gestionar el uso de la información. El gobierno incluye las siguientes características clave:

Clasificación de la información: Descripciones de alto nivel de las categorías principales de la información. La entidad debe definir categorías de alto nivel como “información reservada” y “clasificada” para determinar qué controles de seguridad se pueden aplicar.

Políticas de gestión de la información: Políticas para definir qué actividades se permiten para los distintos tipos de información.

Políticas jurisdiccionales y de localización: Dónde se pueden ubicar geográficamente los datos, lo cual tiene importantes ramificaciones legales y regulatorias.

Autorizaciones: Definir qué tipos de funcionario/usuarios tienen permisos para acceder a qué tipos de información.

Propiedad: Quién es el responsable final de la información.

Custodia: Quién es el responsable de la gestión de la información, a petición del propietario.

11. SEGURIDAD DE LOS DATOS

La seguridad de los datos incluye los controles y tecnologías específicas utilizadas para garantizar el cumplimiento del gobierno de la información.

Un problema frecuente es la gestión de los datos en Cloud, migraciones de datos sensibles sin aprobación o informado a las áreas necesarias para ello.

Además de los controles tradicionales de seguridad de los datos (como controles de acceso o cifrado), hay otros dos pasos que ayudan a gestionar la migración no autorizada de datos a servicios Cloud:

- ✓ Monitorizar la existencia de grandes movimientos internos de datos con herramientas de monitorización de actividad de bases de datos (DAM - Database Activity Monitoring) y de monitorización de actividad en archivos (FAM - File Activity Monitoring).
- ✓ Monitorizar la migración de datos a Cloud con filtros URL y herramientas Data Loss Prevention.

En las implementaciones de Cloud públicas y privadas, y a través de los diferentes modelos de servicio, es importante proteger los datos en tránsito. Esto incluye:

- ✓ Los datos moviéndose desde la infraestructura tradicional a los proveedores Cloud, incluyendo público/privado, interior/exterior y otras combinaciones.
- ✓ Los datos migrando entre los proveedores de Cloud.
- ✓ Los datos moviéndose entre instancias (u otros componentes) en un Cloud determinado.

Hay tres opciones:

1. **Cifrado Cliente/Aplicación**: Los datos son cifrados en el extremo o en el servidor antes de enviarse por la red o ya están almacenados en un formato de cifrado adecuado. Esto incluye el cifrado en cliente local (basado en agente), por ejemplo para archivos almacenados, o el cifrado integrado en aplicaciones.
2. **Cifrado Enlace/Red**: Técnicas de cifrado de red estándar incluyendo SSL21, VPNs22, y SSH23. Puede ser hardware o software. Es preferible extremo a extremo pero puede no ser viable en todas las arquitecturas.

3. **Cifrado basado en Proxy**: Los datos son transmitidos a un servidor dedicado o servidor proxy, el cual los cifra antes de enviarlos por la red. Es la opción escogida frecuentemente para la integración con aplicaciones legacy pero no es generalmente recomendable.

11.1 PROTECCION DE LOS DATOS EN CLOUD

La localización de contenidos incluye las herramientas y procesos para identificar aquella información delicada que esté almacenada. Permite que la entidad defina políticas basadas en el tipo de información, estructura, o clasificación y escanea los datos almacenados mediante técnicas avanzadas de análisis de contenido para identificar localizaciones y violaciones de las políticas.

La localización de contenidos es normalmente una funcionalidad de las herramientas de Data Loss Prevention; para bases de datos, está disponible en ocasiones en los productos de monitorización de la actividad de bases de datos (DAM). El escaneo puede hacerse accediendo a las carpetas compartidas o mediante un agente instalado en el sistema operativo. La herramienta ha de ser “Cloud aware”, es decir, capaz de trabajar en entorno Cloud (por ejemplo, capaz de escanear un almacenamiento de objetos). La localización de contenidos puede estar también disponible como servicio gestionado.

11.1.1 CIFRADO DE ALMACENAMIENTO DE VOLUMENES

El cifrado de volúmenes protege de los siguientes riesgos:

- ✓ Protege los volúmenes de su exposición a un clonado mediante snapshot.
- ✓ Protege a los volúmenes de ser explorados por el proveedor Cloud (y los administradores de Cloud privados)
- ✓ Protege a los volúmenes de verse expuestos ante una pérdida física de discos (un problema más de cumplimiento que de seguridad real)

Los volúmenes IaaS pueden cifrarse usando tres métodos:

Cifrado gestionado por instancias: El motor de cifrado funciona dentro de la instancia, y la clave se guarda en el volumen pero protegida por una contraseña o un par de claves.

Cifrado gestionado externamente: El motor de cifrado funciona dentro de la instancia, pero las claves se gestionan de forma externa y se proporcionan a la instancia bajo demanda.

Cifrado proxy: En este modelo el volumen se conecta a una instancia especial o appliance/software, y entonces se conecta la instancia a una instancia cifrada. El proxy maneja todas las operaciones criptográficas y puede mantener las claves de forma interna o externa.

11.1.2 CIFRADO DE ALMACENAMIENTO DE OBJETOS

El cifrado del almacenamiento de objetos protege de muchos de los riesgos presentes en el almacenamiento de volúmenes. Dado que el almacenamiento de objetos es accesible con más frecuencia desde redes públicas, también permite que el usuario implemente un almacenamiento privado virtual. Al igual que una VPN, una VPS – (Virtual Private Storage) permite el uso de una infraestructura pública compartida a la vez que los datos permanecen protegidos, dado que solo quien disponga de las claves de cifrado pueden leer los datos, aunque lleguen a estar expuestos.

Cifrado de archivos/carpetas y Enterprise Digital Rights Management. Utiliza herramientas de cifrado estándar de ficheros/carpetas o EDRM para cifrar los datos antes de ubicarlos en el almacenamiento de objetos.

Cifrado de cliente/aplicación. Cuando se usa almacenamiento de objetos como el back-end de una aplicación (incluyendo aplicaciones móviles), cifra los datos usando un motor embebido en la aplicación o el cliente.

Cifrado proxy. Los datos pasan por un proxy de cifrado antes de ser enviado al almacenamiento de objetos.

Las operaciones de cifrado deben usar el método de cifrado que sea más apropiado, lo cual puede incluir claves compartidas o pares de claves pública/privada y una estructura PKI/PKO (Public Key Infrastructure/Operations).

Dada la amplia gama de opciones y tecnologías disponibles en Cloud computing, la entidad debe analizar todas las posibles opciones de seguridad.

11.2 DATA LOSS PREVENTION

Data Loss Prevention (DLP) se define como: “Productos que, basados en políticas centralizadas, identifican, monitorizan, y protegen los datos estáticos, en movimiento, y en uso, mediante un análisis profundo de contenidos”.

DLP puede proporcionar opciones sobre cómo se han de manejar los datos cuando se detecte un incumplimiento de las políticas. Los datos pueden ser bloqueados (detener un flujo de trabajo) o permitidos para continuar tras aplicar mediante cifrado una solución utilizando métodos como DRM, ZIP, o OpenPGP.

DLP se usa normalmente para el descubrimiento de contenidos y la monitorización de datos en movimiento utilizando las siguientes opciones:

- ✓ **Appliance/servidor dedicado**. Hardware estándar ubicado en un cuello de botella entre el entorno cloud y el resto de la red/Internet o entre diferentes segmentos Cloud.
- ✓ **Appliance virtual**
- ✓ **Agente en el extremo**
- ✓ **Agente en hipervisor**. El agente DLP está embebido o se accede al mismo a nivel de hipervisor, en lugar de ejecutarse en la instancia.
- ✓ **DLP SaaS**. El DLP está integrado en el servicio cloud (por ejemplo, email en cloud) u ofrecido como un servicio independiente (normalmente de descubrimiento de contenido).

11.3 MONITORIZACION EN BASES DE DATOS Y ARCHIVOS

La monitorización de actividad en base de datos (DAM) se define como: “La monitorización de actividad de base de datos captura y registra, como mínimo, toda la actividad Structured Query Language (SQL) en tiempo real o casi real, incluyendo actividad de los administradores, a través de múltiples plataformas de base de daTos; y puede generar alertas de incumplimiento de políticas”.

DAM realiza una monitorización en tiempo casi real de la actividad de las base de datos y alerta en base a incumplimientos de las políticas, tales como ataques de inyección SQL o replicación de la base de datos sin autorización por el administrador. Las herramientas DAM para entorno Cloud se basan normalmente en agentes que se conectan a un servidor recolector central (normalmente virtualizado). Se usan con instancias dedicadas a un único cliente, aunque en un futuro puede estar disponible para PaaS.

La monitorización de actividad en archivos (FAM) se define como: Productos que monitorizan y registran toda la actividad a nivel de usuario en los repositorios de datos designados, y genera alertas de incumplimiento de políticas.

FAM para Cloud requiere el uso de agentes o ubicar un appliance físico entre el almacenamiento Cloud y los usuarios del Cloud.

11.4 ALMACENAMIENTO CON PRIVACIDAD

Casi todos los sistemas de almacenamiento basados en cloud requieren de alguna autenticación de los participantes (usuario de Cloud y/o CSP) para establecer relaciones de confianza, ya sea sólo para un punto extremo de la comunicación o para ambos. Aunque los certificados criptográficos pueden ofrecer suficiente seguridad para muchos de estos fines, no suelen cubrir la privacidad, ya que están ligados a la identidad de una persona real (usuario Cloud). Cualquier uso de uno de esos certificados muestra la identidad del titular a la parte que solicita la autenticación.

Credenciales basadas en atributos se emiten como credenciales criptográficas ordinarias (por ejemplo, las credenciales X.509) usando una clave de firma digital (secreta). Sin embargo, las credenciales (ABC) basadas en atributos permiten a su titular transformarlas en una nueva credencial que contiene sólo un subconjunto de los atributos contenidos en la credencial original. No obstante, estas credenciales transformadas pueden ser verificadas igual que las credenciales criptográficas ordinarias (utilizando la clave pública de verificación del emisor) y ofrecen el mismo nivel alto de seguridad.

11.5 DIGITAL RIGHTS MANAGEMENT (DRM)

basicamente, Digital Rights Management cifra el contenido, y entonces aplica una serie de derechos. Los derechos pueden ser tan simples como copiar, o tan complejos como especificar restricciones por grupo o usuario en actividades como cortar y pegar, enviar correos, cambiar el contenido, etc. Cualquier aplicación o sistema que trabaja con datos protegidos con DRM debe ser capaz de interpretar e implementar los derechos, lo cual normalmente implica integrarse con un sistema de gestión de claves.

Hay dos categorías en Digital Rights Management:

- ✓ **DRM de consumidor** se usa para proteger contenido de amplia distribución como audio, video, y libros electrónicos destinados a audiencias masivas.

Hay diversas tecnologías y estándares, y el énfasis está en la distribución unidireccional.

- ✓ **DRM corporativo** se usa para proteger el contenido de una organización de forma interna y con sus colaboradores de negocio. El énfasis se pone en derechos más complejos, políticas, e integración con entornos de negocio y particularmente con los servicios de directorio corporativo.

El DRM corporativo puede proteger correctamente el contenido almacenado en Cloud, pero requiere una integración profunda de la infraestructura. Es sobre todo útil para la gestión y distribución de contenido basado en documentos. El DRM de consumidor ofrece una buena protección para proteger y distribuir contenido a los clientes, pero no tiene una buena trayectoria dado que, para la mayoría de las tecnologías desarrolladas hasta la fecha, se ha encontrado la forma de romper los mecanismos de protección que aplican.

12. CONCLUSIONES

- ✓ Entiéndase que la arquitectura de almacenamiento Cloud empleada, lo cual ayudará a determinar el riesgo de seguridad y los controles posibles.
- ✓ Elija almacenamiento con dispersión de los datos cuando esté disponible.
- ✓ Utilice el ciclo de vida de seguridad de los datos para identificar riesgos de seguridad y determinar los controles más adecuados.
- ✓ Monitorice las bases de datos clave internas y los repositorios de archivos con DAM y FAM para identificar grandes migraciones de datos, que podrían indicar que se están migrando datos al Cloud.
- ✓ Monitorice el acceso de los empleados a Internet con filtrado de URL y/o herramientas DLP para identificar datos delicados que se estén migrando al Cloud. Escoja herramientas que incluyan categorías predefinidas para servicios Cloud. Considere el uso de filtros para bloquear la actividad no autorizada. Cifre todos los datos delicados que se mueven hacia o dentro del Cloud en la capa de red, o en los nodos antes de la transmisión por red. Esto incluye todos los servicios y modelos de despliegue.
- ✓ Cuando use algún tipo de cifrado de datos, preste especial atención a la gestión de claves.
- ✓ Use el descubrimiento de contenido para escanear el almacenamiento Cloud e identificar los datos confidenciales expuestos.
- ✓ Cifre volúmenes con información delicada en IaaS para limitar la exposición debida a los snapshots o acceso no autorizado por administradores. La técnica específica variará en función de las necesidades operativas.
- ✓ Cifre los datos delicados en el almacenamiento de objetos, generalmente con agente cifrado de archivo/carpeta.
- ✓ Cifre los datos delicados en las aplicaciones PaaS y el almacenamiento. El cifrado a nivel de aplicación es la opción preferida habitualmente, sobre todo porque pocas bases de datos Cloud dispone de cifrado nativo.
- ✓ Al utilizar el cifrado de aplicación, las claves deben ser almacenadas externamente a la aplicación cuando sea posible.
- ✓ Si el cifrado es necesario para SaaS, trate de identificar un proveedor que ofrezca cifrado nativo. Utilice cifrado de proxy si no está disponible y/o se han de asegurar niveles de confianza.
- ✓ Utilice DLP para identificar los datos delicados que se estén filtrando de despliegues Cloud. Por lo general sólo está disponible para IaaS, y puede no ser viable para todos los proveedores de Cloud pública.

- ✓ Monitorice las a bases de datos con datos delicados con DAM y genere alertas de vulneraciones de política de seguridad. Utilice una herramienta preparada para el Cloud.
- ✓ Considere un almacenamiento que preserve la privacidad cuando ofrezca infraestructura o aplicaciones en las que el acceso normal pueda revelar información delicada del usuario.
- ✓ Recuerde que las brechas más grandes de seguridad son el resultado de una seguridad escasa en las aplicaciones.
- ✓ La eliminación o de datos de un proveedor Cloud, ya sea debido a la expiración del contrato o cualquier otra razón, se debe cubrir en detalle en la creación del ANS. Esto debe abarcar la eliminación de cuentas de usuario, la migración o la eliminación de datos desde el almacenamiento primario/redundante, entrega de claves, etc.
- ✓ Utilice el ciclo de vida de la seguridad de los datos para identificar riesgos de seguridad y determinar los controles más adecuados.
- ✓ Debido a todos los potenciales problemas regulatorios, contractuales y jurisdiccionales de otro tipo, es extremadamente importante entender tanto las ubicaciones lógicas como las físicas de los datos.

13. BIBLIOGRAFIA

- CSA, Cloud Security Alliance., (2011).Guías de Seguridad de Áreas Criticas en Cloud Computing V 3.0.
- CCN, Centro Criptologico Nacional, Guía de Seguridad de las TIC., (2014). Utilización de Servicios en la Nube.
- NIST, National Institute of Estandards and Technology, SP-800-30.
- NIST, National Institute of Estandards and Technology, SP-500-292
- ISO/IEC 27000, Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary
- ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements
- www.revistacloudcomputing.com.