METODOS DE SEGURIDAD, COMPUTACIÓN EN LA NUBE

AUTOR: MAX JOSÉ BERMÚDEZ LEÓN

DICIEMBRE: 2020

San Marcos

Introducción

Las soluciones o aplicaciones informáticas (programas de software) han dado un importante giro en la forma en cómo se distribuyen o adquieren gracias a las necesidades de negocio que demandan cambios al mismo ritmo que los avances tecnológicos. Debido a esta necesidad es que se desea diseñar en el presente proyecto una nueva arquitectura basada en una plataforma como servicio para un sistema ya existente y que se ajuste a las nuevas tendencias digitales. Lo anterior con el único objetivo de brindar un servicio de "alquiler" de la aplicación que se pueda acceder a través de internet, obteniendo el máximo de los beneficios, los cuales garantizan un menor costo, mayor portabilidad y una mayor continuidad de negocio, entre otros.

El entorno juega un papel importante en las casusas identificadas según el análisis realizado, ya que la infraestructura requerida para cumplir con lo mínimo solicitado por los usuarios representa un desafío importante, principalmente por su costo económico, por lo que realizar los cambios para actualizar la forma en que opera el sistema resultaría muy conveniente para cumplir con dichos requerimientos.

Todas estas causas dan como efecto que la aplicación no permita implementarse bajo la modalidad de plataforma como servicio, que es lo que el cliente requiere para la evolución tecnológica del sistema y potencialización de su herramienta.

Tabla de contenido

Modelo de seguridad en la nube

Autenticación en la nube

Definir los mecanismos de seguridad correctos asociados a la gestión de usuarios es de vital importancia.

La computación en la Nube es un modelo para permitir el acceso bajo demanda a un conjunto de recursos informáticos como redes, servidores, almacenamiento de datos, servicios y aplicaciones que pueden aprovisionarse y liberarse rápidamente con un mínimo esfuerzo.

Hoy en día, las pequeñas y medianas empresas se están dando cuenta cada vez más que simplemente aprovechando la Nube pueden obtener un acceso rápido a las mejores aplicaciones comerciales o aumentar significativamente sus recursos de infraestructura, todo a un costo muy bajo.

A medida que la computación en la Nube gana popularidad, surgen preocupaciones sobre los problemas de seguridad presentados a través de la adopción de este nuevo modelo. La utilidad y la eficiencia de los mecanismos de protección tradicionales se están revisando, ya que las características de este innovador modelo de implementación difieren ampliamente de las de las arquitecturas tradicionales.

Problemas de seguridad de Computación en la Nube

Los problemas comunes en torno a la seguridad en la Nube son:

- Problemas de privacidad
- Falta de transparencia
- Filtración de datos
- Robo de identidad

Cuando se trata de computación en la Nube, los proveedores de servicios requieren que los clientes almacenen la información de su cuenta en la Nube, lo que les da acceso a estos datos. Para los clientes, esto representa un problema de privacidad.

La falta de transparencia en la Nube hace que sea difícil para los clientes garantizar que se cumplan las normas adecuadas, ya que utilizan múltiples servicios en la Nube y tienen más copias de su información en dicha Nube. Esto causa problemas de seguridad pues múltiples copias de cuentas conducen a muchos procesos de autenticación.

Mecanismos de autenticación

Autenticación a través de nombre de usuario y contraseña

El punto importante en la autenticación es proteger los datos del acceso de personas no autorizadas. Esto implica que los servidores rechazan las solicitudes de visitas de personas desconocidas y gestionan el acceso de los usuarios confirmados. En este método, el usuario debe ingresar el nombre y la contraseña para iniciar sesión en el sistema y luego puede acceder a información en la Nube.

Autenticación multifactor (MFA)

El método de autenticación tradicional a través de contraseña no puede proporcionar suficiente seguridad de la información contra la mayoría de los ataques modernos en un entorno de computación en la Nube. Un método seguro es la autenticación multifactor. No sólo confirma cualquier par de nombres de usuario / contraseña, sino que requiere un factor secundario; un token o un código por SMS son ejemplos.

Inicio de sesión único (SSO)

Es un sistema de gestión de identidad donde un usuario puede ser validado en una única autenticación y luego puede acceder a otros servicios limitados sin volver a autenticarse. En otras palabras, se genera información de autenticación mediante el uso de diferentes módulos en este método. SSO es una forma de acceder a un sistema de software múltiple independiente donde el usuario inicia sesión, así accede a todos los sistemas sin necesidad de iniciar sesión nuevamente.

Autenticación biométrica

El método biométrico admite tres factores de seguridad de la información, autenticación, identificación y no repudio. Biométrico es una palabra griega antigua que comprende bio = vida y metron = medida. Este mecanismo es basado en la identificación de características fisiológicas o de comportamiento de una persona.

Existen 2 modelos distintos:

- Biometría física: tipo de autenticación basada en las características físicas del ser humano como reconocimiento de geometría de manos, reconocimiento de huellas digitales, reconocimiento de huellas de palmas, voz, reconocimiento facial, exploración retiniana y exploración del iris.
- Biometría del comportamiento: se basa en el comportamiento del usuario. Esta técnica identifica a los usuarios de acuerdo con su ubicación, patrón de mecanografía (análisis de pulsaciones de teclas) e incluso las firmas autógrafas.

API Keys

Este método aplica para la autenticación de aplicaciones. No requiere bibliotecas de cliente y es transparente para el usuario. Este método identifica a las aplicaciones con una asociación entre una clave y un proyecto.

Autenticación Auth0

Este método no sólo autentica y autoriza aplicaciones y API, sino que también es independiente de la tecnología del sistema, el dispositivo y la identidad. Este método admite varios proveedores y especificaciones de lenguaje. Por lo regular proporciona servicios de back-end, SDK y bibliotecas de interfaz de usuario para autenticar usuarios en aplicaciones web y móviles.

Autenticación de Google

Este método permite a los usuarios autenticarse iniciando sesión con su cuenta de Google. Lo mismo aplica para la autenticación con Facebook.
El activo más valioso en la computación en la Nube son los datos. La seguridad es extremadamente vital porque si los datos no están protegidos, la Nube prácticamente perderá su significado.

Seguridad en la nube

La seguridad en la nube es la protección de los datos, las aplicaciones y las infraestructuras involucradas en cloud computing. Muchos aspectos de la seguridad de los entornos de nube, ya sea pública, privada o híbrida, son los mismos que los de cuebookalquier arquitectura de TI on-premise.

Las preocupaciones de seguridad de alto nivel (como la exposición de datos no autorizada o la filtración de información, los controles de acceso vulnerables, la susceptibilidad a los

ataques y las interrupciones de la disponibilidad) afectan a la TI tradicional y a los sistemas de nube por igual. Al igual que en cualquier entorno informático, la seguridad en la nube implica mantener una protección preventiva adecuada que le permita lo siguiente:

- Estar al tanto de la seguridad de los datos y los sistemas.
- Ver el estado actual de la seguridad.
- Saber inmediatamente si sucede algo inusual.
- Hacer un seguimiento y responder ante eventos inesperados.

¿Por qué la seguridad en la nube es diferente?

Aunque muchas personas entienden los beneficios del cloud computing, les da miedo implementarlo por las amenazas de seguridad. Lo comprendemos. Es difícil comprender algo que se encuentra en algún lugar entre los recursos abstractos enviados por Internet y un servidor físico. Es un entorno dinámico donde todo cambia constantemente, incluso las amenazas de seguridad. La cuestión es que, en su mayor parte, la Modern IT security: Sometimes caring is NOT sharing. Una vez que entienda las diferencias específicas, la palabra "nube" no generará tanta inseguridad.

Seguridad de perímetros

La seguridad está muy relacionada con el acceso. Generalmente, los entornos tradicionales controlan el acceso mediante un modelo de seguridad de perímetro. Los entornos de nube se encuentran extremadamente conectados, lo que facilita el tráfico para omitir las defensas tradicionales del perímetro. Las interfaces de programación de aplicaciones (API) que no son seguras, la gestión deficiente de la identidad y las credenciales, los secuestros de cuentas y los infiltrados malintencionados pueden representar amenazas para el sistema y los datos. Para evitar el acceso no autorizado a la nube, se debe adoptar un enfoque centrado en los datos. Cifrar los datos. Fortalecer el proceso de autorización. Exigir contraseñas sólidas y autenticación de doble factor. Aplicar mecanismos de seguridad en todos los niveles.

Ahora todo está en el software

La palabra "nube" hace referencia a los recursos alojados que llegan al usuario a través del software. Las infraestructuras de cloud computing, junto con todos los datos que se procesan, son dinámicas, escalables y portátiles. Los controles de seguridad en la nube deben responder ante las variables del entorno y acompañar las cargas de trabajo y los datos en reposo y en tránsito, ya sea como partes inherentes de las cargas de trabajo (p. ej., cifrado) o de forma dinámica a través de un sistema de gestión de nube y API. Esto permite proteger los entornos de nube de la corrupción del sistema y la pérdida de datos.

Entorno de amenazas sofisticadas

Las amenazas sofisticadas constituyen todo aquello que impacta de forma negativa en la informática moderna que, sin duda, incluye a la nube. Los sistemas malware cada vez más sofisticados y los demás ataques, como las amenazas persistentes avanzadas (APT), están diseñados para evadir las defensas de la red aprovechando los puntos vulnerables de la pila informática. Las filtraciones de datos pueden dar lugar a la divulgación de información no autorizada y la alteración de los datos. No hay una solución clara para estas amenazas, pero es su responsabilidad estar al tanto de las prácticas de seguridad en la nube en constante evolución para mantenerse al día con las nuevas amenazas.

La seguridad en la nube es una responsabilidad de todos

Independientemente del tipo de implementación de nube que utilice, usted debe encargarse de la seguridad de su propio espacio en la nube. Usar una nube cuyo mantenimiento es responsabilidad de otra persona no significa que usted pueda, ni deba, relajarse. La falta de la diligencia correspondiente es la principal causa de las fallas en la seguridad. La seguridad en la nube es responsabilidad de todos, lo cual incluye tomar las siguientes medidas:
Usar software confiable

- Entender el concepto de cumplimiento

- Administrar los ciclos de vida
- Considerar la portabilidad
- Supervisar los entornos constantemente
- Elegir al equipo de seguridad capacitado

¿Son seguras las nubes públicas?

De acuerdo. Analicemos esta pregunta. Podríamos describirle todas las diferencias de seguridad que existen entre los tres tipos de implementación (pública, privada e híbrida), pero sabemos que lo que en realidad se pregunta es si las nubes públicas son seguras. Bueno, eso depende.

Las nubes públicas son adecuadamente seguras para muchos tipos de cargas de trabajo, pero no son adecuadas para todo, en gran medida, porque no cuentan con el aislamiento de las nubes privadas. Las nubes públicas dan soporte a la arquitectura multiempresa, lo cual significa que usted alquila la potencia informática (o el espacio de almacenamiento) al proveedor de la nube junto con otras empresas. Cada inquilino firma un acuerdo de nivel de servicio (SLA) con el proveedor de la nube que documenta quién es responsable y por qué cosas se responsabiliza. Es muy parecido a alquilar un espacio físico a un arrendador. El arrendador (proveedor de la nube) promete realizar el mantenimiento del edificio (infraestructura de la nube), tener las llaves (acceso) y, en general, no estorbar al inquilino (privacidad). A cambio, el inquilino promete no hacer nada (p. ej., ejecutar aplicaciones que no son seguras) que pudiera corromper la integridad del edificio o molestar a otros inquilinos. Pero usted no puede elegir a sus vecinos, y es posible que alguno de ellos permita el acceso a algo malicioso. Mientras el equipo de seguridad de infraestructura del proveedor de la nube controla si se producen eventos inusuales, las amenazas agresivas o imperceptibles (como los malintencionados ataques distribuidos de denegación de servicio [DDoS]) pueden afectar negativamente a otros inquilinos.

Afortunadamente, hay algunos estándares de seguridad, normativas y marcos de trabajo de control aceptados en el sector, como la matriz de controles en la nube de la Cloud Security Alliance. También puede aislarse en un entorno de arquitectura multiempresa implementando medidas de seguridad adicionales (como el cifrado y las técnicas de reducción de los DDoS), que protegen a las cargas de trabajo de una infraestructura comprometida. Si eso no es suficiente, puede lanzar agentes de seguridad de acceso a la nube para supervisar la actividad y aplicar las políticas de seguridad para las funciones empresariales de bajo riesgo. Sin embargo, es posible que todo esto no sea suficiente para los sectores que operan bajo normas de estricta privacidad, seguridad y conformidad.

Disminuir el riesgo con la nube híbrida

Las decisiones de seguridad están muy relacionadas con la tolerancia al riesgo y con el análisis de los costos y los beneficios. ¿Cuál es el impacto de los posibles riesgos y beneficios en el funcionamiento general de su empresa? ¿Qué es lo más importante? No todas las cargas de trabajo demandan el nivel más alto de cifrado y seguridad. Considérelo de esta manera: cerrar su casa con llave mantiene todas sus pertenencias relativamente seguras, pero, aun así, guarda sus cosas más valiosas en una caja fuerte. Es bueno tener opciones.

Por eso cada vez más empresas adoptan las nubes híbridas, que ofrecen lo mejor de todas las nubes. La nube híbrida es una combinación de dos o más entornos interconectados de nubes públicas o privadas.

Las nubes híbridas le permiten elegir dónde colocar las cargas de trabajo y los datos en función del cumplimiento, las auditorías, las políticas o los requisitos de seguridad; de esta manera, protegen las cargas de trabajo especialmente confidenciales en una nube privada y ejecutan las cargas de trabajo menos confidenciales en la nube pública. Hay algunos desafíos singulares en cuanto a la seguridad en la nube híbrida (como la migración de datos, el aumento de la complejidad y una mayor superficie de ataque), pero la presencia de varios entornos puede constituir una de las defensas más fuertes contra los riesgos de seguridad.

La falsa sensación de seguridad del Cloud Computing

Existe un aumento significativo de empresas que están trasladando cada vez más recursos y cargas de trabajo a la nube. Asumir que en el Cloud Computing la seguridad es intrínseca a este tipo de servicio es un error que puede complicar las cosas a muchas empresas en un futuro próximo. Porque si bien es cierto que hay que invertir en planes de ciberseguridad on-premise, también debemos hacerlo para nuestros despliegues en el Cloud.

Existen organizaciones como "*Cloud Securitty Alliance*" que se dedican a promover el uso de buenas prácticas para garantizar la seguridad en 'Cloud', porque La computación en la nube se está volviendo cada vez más popular, partiendo de sencillos repositorios de almacenamiento como OneDrive, Google Drive, Dropbox, etc. a los servicios 'SaaS' de Google asociados a las cuentas de Gmail y terminando en el hosting tradicional o los más especializados servicios de 'PaaS' e 'IaaS'.

Es conveniente conocer a grandes rasgos los distintos tipos de arquitectura y servicios que ofrece el Cloud Computing para comprender mejor las medidas de seguridad que han de adoptarse en este tipo de entornos.

Existen cuatro implementaciones de servicios de Cloud Computing en función de su tipología.

Private Cloud: La nube Privada fue precursora de este tipo de soluciones, aquí los recursos suelen estar alojados en una red privada a nivel local, en la propia infraestructura o a través de un proveedor de servicios externo especializado, que es generalmente exclusivo de la empresa u organización. Las características principales de este tipo de Cloud serian:

- Los servidores e infraestructura física son de nuestra propiedad.

- Existe un alto grado de seguridad, ya que nuestros datos no son gestionados por terceros.
- El Hardware es dedicado y adaptado a nuestras necesidades.
- La inversión inicial, los costes de mantenimiento y actualización son superiores

Este tipo de soluciones privadas son utilizadas mayoritariamente por entidades gubernamentales, organismos oficiales y entidades bancarias.

Virtual Private Cloud VPC: Esta variante del Private Cloud no es realmente un subtipo especifico, pero debido a su creciente implantación podríamos empezar considerarlo como tal. Se basa en la disposición de una serie de recursos computacionales configurables bajo demanda dentro de un ambiente de cloud público, el cual provee de un cierto grado de aislamiento entre diferentes organizaciones.

Public Cloud: La nube publica es el tipo más extendido, aquí los recursos inherentes a este tipo de servicio se encuentran alojados externamente en el proveedor de servicios. Este tipo de servicio Cloud tiene algunas implicaciones como, por ejemplo:

- Los recursos computacionales y de almacenamiento se comparten entre todos los clientes del proveedor, es decir, nuestros datos y los de otras empresas podrían estar alojados en el mismo equipo.
- Nuestra información se almacena en servidores de terceros, de los que no somos propietarios.
- No requiere de una inversión inicial en infraestructura, ni posteriormente en mantenimiento o actualización ya que esta corre a cargo al proveedor.

Este tipo de servicios son los ofrecidas por empresas como Amazon, Google, Microsoft etc. que se encargan a nivel global de su gestión y mantenimiento.

Hybrid Cloud: El Cloud hibrido supone Una combinación de los casos anteriores, donde coexisten recursos locales y externos que configuran la arquitectura final del entorno.

Podemos disponer de una arquitectura de sistemas on-premise y paralelamente utilizar la nube pública para funcionalidades específicas o conexiones con herramientas externas.

Modalidades del tipo de servicio: A la hora de contratar los servicios en 'Cloud', también hay que tener en cuenta otras consideraciones en relación a las modalidades del tipo de servicio. Éstas se clasifican en tres:

- Software como Servicio ('SaaS'): De las siglas en inglés Software as a Service, suele ser el más utilizado y consiste en que el 'software' permanece alojado en el servidor del proveedor y el cliente accede al mismo a través de un navegador web. El mantenimiento, soporte y disponibilidad es gestionada por el proveedor. Un ejemplo de este tipo de servicio podría ser las herramientas de correo electrónico tipo Gmail. En este caso no controlaremos aspectos propios del servidor de Cloud Computing como el sistema operativo o la infraestructura.
- Plataforma como servicio('PaaS'): En este tipo de servicio, Platform as a Service, el proveedor ofrece acceso a un entorno basado en la nube en el cual los usuarios pueden crear y distribuir sus propias aplicaciones. El proveedor proporciona la infraestructura subyacente que nos permitirá interactuar con algunos servicios básicos ya preinstalados, como bases de datos, teniendo cierto grado de libertad a la hora de instalar software.
- Infraestructura como Servicio ('IaaS'): Con la Infraestructure as a Service tendremos control prácticamente total del servidor, aunque existen algunas variantes, podremos administrar recursos asignados al mismo, así como aspectos fundamentales como la instalación del sistema operativo.

Amenazas relativas a servicios Cloud

El factor humano ocupa la parte más amplia en la pirámide de riesgo, es la más importante en cuanto a volumen, pues la amenaza que suponen los usuarios es con diferencia el factor de riesgo más importante. Definir los mecanismos de seguridad correctos asociados a la gestión de usuarios es de vital importancia.

Otra de las grandes amenazas actuales son los secuestros de sesión. Este tipo de ataques permiten que se puedan obtener las credenciales de acceso en los trascursos de inicio de sesión, con lo que se aconseja aplicar técnicas de autenticación de doble factor siempre que sea posible y monitorizar las sesiones en búsqueda de actividades maliciosas o inusuales.

Respecto al 'hardware' compartido empleado por los proveedores de servicios de Cloud, es también un vector a tener en cuenta pues se emplean los mismos servidores físicos para prestar servicio a múltiples clientes a través de la virtualización. El hecho de compartir la misma máquina implica que el acceso a la misma o a uno de los servidores virtuales podría facilitar la entrada a todos los recursos presentes. Es por este motivo que debemos tener garantías suficientes que las plataformas de virtualización están debidamente protegidas en este respecto.

En cuanto a los repositorios de información y sistemas de copias de seguridad, aparte de una especifica gestión de amenazas y la auditoria de acceso a los recursos a de establecerse con el proveedor una correcta estrategia de salvaguarda de la información, porque los problemas físicos también suponen amenazas. En este caso, es importante que el proveedor ofrezca las garantías suficientes frente ante cualquier tipo de contingencia como incendio, robo, e inundación, ya que al fin y al cabo se trata de una infraestructura física la que está soportando la plataforma virtual y por tanto el servicio ofrecido.

Sobre los problemas de cumplimiento y de cara a poder estar alineados con el Reglamento General de Protección de Datos (RGPD) europeo, al tratarse de un servicio en el cual puede estar alojada todo tipo de información sensible, información de carácter personal, etc, debemos asegurarnos de que el proveedor cumple con todos los requisitos exigidos por la normativa solicitándole un certificado de cumplimiento, que garantice que el lugar donde se alojan los datos se encuentren en país con que forme parte de un marco seguro como la Unión Europea o Estados Unidos.

LA APUESTA POR LA NUBE PÚBLICA ESTÁ MUY ENFOCADA AL ÁMBITO DOMÉSTICO Y A LA PEQUEÑA EMPRESA POR DOS RAZONES: ECONÓMICA Y DE GESTIÓN

La apuesta por la nube pública en este sector es una tendencia, pero está muy enfocada al ámbito doméstico y a la muy pequeña empresa especialmente, las razones son principalmente dos:

- Económica: gracias a las economías de escala son más baratas.
- De gestión: no disponer de un equipo IT dedicado y formado que pueda asumir este rol hace que empresas, especialmente las pequeñas recurran a este tipo de soluciones.

A la hora de escoger hay que balancear y optar por la solución que mejor se adapte a cada compañía o institución.Los retos del Cloud Computing en materia de seguridad. Como hemos visto en los puntos anteriores existen varios aspectos que definirán la solución de Cloud Computing se mejor se adapta a nuestras necesidades, ya sea al contar con un equipo de IT en plantilla, de nuestro presupuesto o del grado de seguridad y control sobre nuestros datos.

El Cloud Computing ha resuelto muchos de los problemas de las empresas, debido sobre todo a la facilidad de uso y al bajo coste de las soluciones, por este motivo el uso de la computación en la nube aumenta día a día. Pero este hecho puede ser un arma de doble filo si no se establecen los procedimientos de ciberseguridad adecuados, se invierte en formación y se realizan acciones pedagógicas para que los usuarios dejen de ser la brecha de seguridad más importante.

Y es por este motivo fundamentalmente por el cual todavía existen multitud de empresas que se resisten a los considerables atractivos de la nube debido sobre todo a las persistentes preocupaciones en materia de seguridad de la información, porque una implementación insegura, puede poner en grave riesgo los activos e incluso la viabilidad de la empresa.

Conclusiones y recomendaciones

Sin duda la nube computacional ha llegado para establecerse cada vez de manera más formal, aportando con soluciones que van aumentando de tal manera que día a día son más usuarios los que se integran a este modo de trabajo. ¿Podrán los riesgos presentados arruinarle el negocio a la computación en nube? Esto parece muy improbable, ya que la computación en nube es conveniente para los usuarios y es rentable para los proveedores. Un total rechazo a utilizar los servicios en la nube haría que una empresa termine aislada (e incapaz de hacer negocios), tal como sucedería si hoy se rechazara de pleno el uso del correo electrónico. En vez de boicotear esta tecnología, un enfoque más productivo consistiría en la creación de una nueva legislación y estrictos reglamentos para los proveedores, así como tecnologías que hagan (casi) imposible que los empleados de un proveedor husmeen la información del usuario. Actualmente, toda empresa que quiera ofrecer servicios en la nube, es libre de hacerlo, pero la situación cambiará dramáticamente en unos diez años. Los proveedores tendrán que regirse por normas si quieren ofrecer sus servicios. Por otro lado, podemos decir que siempre habrá detractores, los enemigos del progreso pedirán tiempo para analizar, y luego propondrán planes pilotos, mientras piensan en otros motivos para atrasar.

Referencias bibliográficas

- Ahmad,Shabir and Ehsan Bilal. IJSER. (2013). The Cloud Computing Security Secure User Authentication Technique (Multi Level Authentication) https://www.ijser.org/researchpaper/The-Cloud-Computing-Security-Secure-User-Authentication.pdf consultado mayo, 2020.

- EL KAMOUN, Najib. ResearchGate. (2017). Authentication mechanisms in cloud computing environments. https://www.researchgate.net/publication/319522315_AUTHENTICATION_MECHANISMS_IN_CLOUD_COMPUTING_ENVIRONMENTS consultado mayo, 2020.

- KioNetworks. (2020). MECANISMOS DE AUTENTICACIÓN DE LA NUBE. https://www.kionetworks.com/blog/nube/mecanismos-de-autenticacion-de-la-nube

- RedHat. (2020). Seguridad en la nube. https://www.redhat.com/es/topics/security/cloud-security

- Edward Jones. (2020). Una guía completa de Cloud Security en 2020 (Riesgos, mejores prácticas, certificaciones). https://kinsta.com/es/blog/seguridad-nube/

- Antonio Marco. (2020). La falsa sensación de seguridad del Cloud Computing. https://cuadernosdeseguridad.com/2020/05/cloud-computing-seguridad-lanaccess/

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica