SEGURIDAD EN LA NUBE

C. Daniel Giovanni Olvera Ayala

Av. Lázaro Cárdenas SN, Haciendita, 39079 Chilpancingo de los Bravo, Gro Teléfono Celular. 7471099315 Correo electrónico 13319900@uagro.mx

M.I. Rubén Rodríguez Camargo

Av. Lázaro Cárdenas SN, Haciendita, 39079 Chilpancingo de los Bravo, Gro. Teléfono Celular. 7471311223 Correo electrónico Rubenrc@uagro.mx

M.C. León Julio Cortez Organista

Av. Lázaro Cárdenas SN, Haciendita, 39079 Chilpancingo de los Bravo, Gro. Teléfono Celular 7471102752 Correo electrónico ljcortez@uagro.mx

DR. Mario Hernández Hernández

Av. Lázaro Cárdenas SN, Haciendita, 39079 Chilpancingo de los Bravo, Gro. Teléfono Celular

7471120661 Correo electrónico. 11228@uagro.mx

RESUMEN

La seguridad en la nube se ha convertido en un tema critico a considerar en la era digital actual con la creciente adopción de la nube por partes de las empresas y usuarios, es importante tener en cuenta los riesgos y proteger los datos de posibles amenazas.

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

ABSTRACT

Cloud security has become a critical issue to consider in today's digital era with the growing adoption of the cloud by companies and users, it is important to consider the risks and protect data from potential threats.

The correct implementation of the information service in the cloud will reduce the risk of security incidents that affect the image of the entity and generate irreparable damage.

PALABRAS RESERVADAS

Nube, Computadoras, Vulnerabilidad, Riesgos

KEYWORDS

Cloud, Computers, vulnerability, risks

INTRODUCCIÓN

En este artículo se dará una visión general de lo que es la seguridad en la nube, una explicación breve de los riesgos, tipos de nube y modelos de servicios.

Esta seguridad son las precauciones que se tienen en las empresas que proveen computación en la nube, de manera que la información cumpla con tres principios: la confidencialidad, la disponibilidad y la integridad. El modelo de servicio de la computación en la nube no necesariamente es una nueva tecnología más bien se pude decir que es una nueva forma de acceder a los recursos de computación.

Actualmente, toda empresa que quiera ofrecer servicios en la nube, es libre de hacerlo, pero la situación cambiará dramáticamente en diez años. Algunos de los beneficios en utilizar la nube están: reducción de costos a expensas de aspectos como hardware, software, mantenimiento, ahorro del espacio físico, potencia de cómputo, capacidad de almacenamiento, entre otros.

Sin embargo, pueden presentarse inconvenientes, como la carencia de control, dependencia de accesos a conexiones de internet, falta de portabilidad documental entre proveedores de servicios, y la más importante, la necesidad de protección de seguridad y privacidad de datos y programas.

1 Nube

Es un servicio accesible, eficiente, transformador para el procesamiento y almacenamiento de datos a través de internet mediante un modelo de precios de pago. La nube hace referencia a los servidores a los que se accede a través de internet, software y bases de datos que se ejecutan en esos servidores. Es decir, en la nube puedes guardar toda la información que es requerida en lugar de almacenarla en tu computadora, memoria usb, disco duro.

Esto se realiza en un servidor externo, para el cual se paga por dicho servicio al proveedor que lo ofrece.

1.1 Tipos de nube

Existen 3 tipos de servicio en la nube, cada tipo requiere un nivel distinto de gestión por parte del cliente y ofrece un nivel de seguridad diferente. Nube pública

La nube pública es un conjunto de recursos virtuales desarrollados a partir de un sistema de hardware que pertenece a una empresa externa encargada también de gestionarlo. La nube se pone a disposición de varios clientes a través de una interfaz de autoservicio de manera automática. Es una forma sencilla de adaptar las cargas de trabajo que sufren variaciones inesperadas de la demanda.

Por lo general, las nubes públicas actuales no se implementan como una solución de infraestructura independiente, sino como parte de un conjunto heterogéneo de entornos que mejora la seguridad y el rendimiento, disminuye los costos y aumenta la disponibilidad de la infraestructura, los servicios y las aplicaciones.

Figura 1: Nube pública (Elaboración propia)

1.1.2 Nube Privada

Una nube privada es un modelo de informática de nube en el que la infraestructura se dedica a una organización de un solo usuario. Una nube privada se puede alojar en el propio centro de datos de una organización, en una instalación de cubicación de terceros o a través de un proveedor de nube privada que ofrezca servicios de alojamiento de nube privada y que pueda ofrecer también infraestructura tradicional de nube multicliente, compartida y pública..

Figura 2 Nube privada (Elaboración propia)

1.1.3 Nube hibrida

El autor Ivan Jahel Bautista García afirma que la nube híbrida es la combinación de uno o más entornos de nube privada y pública, lo que quiere decir que las empresas se benefician de las características que brindan estos dos tipos de infraestructura de cloud. La tecnología de la nube híbrida brinda a las compañías una mayor flexibilidad transportando cargas de trabajo entre soluciones de nube acuerdo con sus necesidades. Los servicios otorgados por esta suelen ser potentes y otorgan a las organizaciones más control sobre sus datos privados.

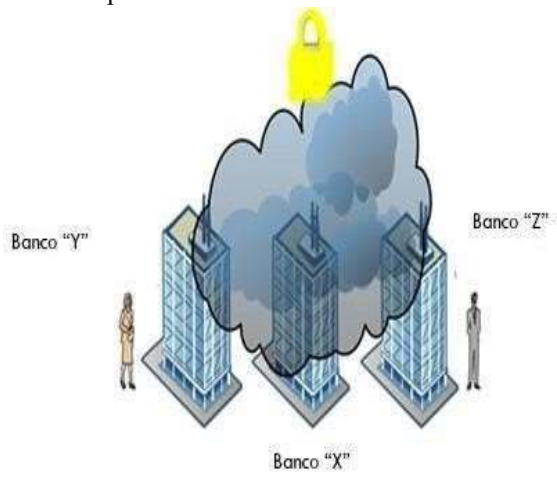

Figura 3 Nube hibrida (Elaboración propia)

1.1.4 Nube comunitaria

La nube comunitaria se define como un servicio de nube que está diseñado y es utilizado por empresas y organizaciones que tienen sus objetivos políticos, sociales o de cultura.

Es de mucha utilidad en la empresa por su flexibilidad para ilustrarlo supongamos que cierta empresa tiene un servidor web y para eso hace uso de la nube publica y para un servidor de base de datos hace uso de una nube privada.

Figura 4 Nube comunitaria (Elaboración propia)

1.2 ¿Qué es la seguridad en la nube?

La seguridad en la nube es una especialidad dedicada a proteger contra amenazas informáticas a los sistemas alojados en la nube.

De acuerdo con la página web Kasperky considera que la seguridad en la nube es toda la tecnología, los protocolos y las buenas prácticas que protegen los entornos informáticos en la nube.

Al igual que la ciberseguridad, la seguridad en la nube es un área muy amplia, y es imposible prevenir todos los tipos de ataques. Sin embargo, una estrategia de seguridad en la nube bien diseñada reduce considerablemente el riesgo de ciberataques. Estas medidas de seguridad se ponen en práctica, no sólo para proteger los datos, sino también para asegurar el cumplimiento de la normativa y garantizar la privacidad de los clientes.

1.2.1 ¿Cómo funciona la seguridad en la nube?

Un entorno en la nube es tan seguro como su punto más débil, por lo que una seguridad eficaz en la nube implica que varias tecnologías trabajen juntas para proteger los datos y las aplicaciones desde todos los ángulos. En lugar de proteger un perímetro, la seguridad en la nube protege los recursos y los datos individualmente.
La seguridad basada en la nube funciona para proteger el acceso online a los archivos, bloqueando el tráfico de usuarios sospechosos y no autorizados**.**

1.2.2 ¿Porque es importante la seguridad en la nube?

La seguridad en la nube ha evolucionado en los últimos años. Si bien en origen había ciertas reticencias al uso de estos entornos por las medidas de protección, hoy la nube es, en términos generales, un lugar seguro. No obstante, depende de las capacidades de protección implementadas por los proveedores de estos servicios. De ahí que, como usuario, deba saber en todo momento cómo va a ser tratada su información y qué medidas de seguridad van a tener.
Los ciberdelincuentes pueden ganarse la vida explotando las vulnerabilidades de la nube, por ello es importante tener una correcta seguridad ella.

1.2.3 Como asegurar la nube

Existen bastantes opciones

para asegurar o proteger la nube.

Uno de los métodos más conocidos es el cifrado ya que es una de las mejores maneras de proteger los sistemas de informática. En la nube, los datos corren más riesgo de ser interceptados cuando están en movimiento. Cuando se están trasladando entre dos ubicaciones de almacenamiento o cuando se transmiten a su aplicación local, los datos son más vulnerables. Por este motivo, el cifrado de extremo a extremo es la mejor solución de seguridad en la nube para los datos esenciales. Con el cifrado de extremo a extremo, en ningún momento su comunicación se pone a disposición de personas que no dispongan de la clave de cifrado.

1.2.4 Criptografia

Según la página web docusigb indica que la criptografía es un recurso tecnológico utilizado para codificar mensajes, para que sólo su remitente y receptor puedan acceder al contenido. En otras palabras, es una “escrita oculta”. Esta tecnología es utilizada para asegurar tus datos digitales, también es utilizada para datos confidenciales amenazas basadas en internet.

1.2.4.5 Tipos de Cifrado

Como indica la página web OSI Los dos principales tipos de cifrado es el

cifrado simétrico y asimétrico

El cifrado simétrico también es conocido como cifrado de clave secreta utiliza la misma clave para cifrar y descifrar el mensaje, que tienen que conocer, previamente, tanto el emisor como el receptor. El cifrado asimétrico es uno de los tipos de

criptografía informática más seguros y una de las técnicas de criptografía más potentes se basa en el uso de dos claves la pública y la privada
La clave pública se podrá difundir sin ningún problema a las personas que necesiten mandarle información cidrada. La clave privada jamás se debe de revelar.

1.3 Riesgos y amenazas en la nube

Uno de los mayores riesgos es perder todos nuestros datos para siempre. Las amenazas en la nube dependen del tipo de servicio contratado y de su forma de contratación y de despliegue. También será distinta la forma de afrontarlas según el grado de control sobre el servicio que recae en el proveedor y en el cliente acordado en el acuerdo de nivel de servicio. Entre las amenazas más comunes se encuentran las siguientes:
1.-Accesos no autorizados. Si el proveedor y cliente no toman conjuntamente las medidas de seguridad adecuadas, no habrá posibilidad de controlar los accesos a la información de la organización.
2.-Interfaces inseguras. Si las interfaces que proporciona el proveedor para acceder a la plataforma en la nube no son del todo seguras y presentan fallos de seguridad, estos pueden ser explotados por terceros para acceder a nuestra información.
3.-Fuga de información. Como resultado de un ataque de ingeniería social o por una infección con malware, un delincuente puede conseguir que algún usuario envíe información confidencial. También en el caso de que las operaciones de transferencia de datos no estén cifradas puede producirse una fuga de información.
4.- Suplantación de identidad. Si los ciberdelincuentes consiguen, por ingeniería social, fuerza bruta o descuido, las credenciales de algún usuario podrán acceder a la plataforma suplantando, pudiendo manipular la información, actuar en su nombre. (Stark K, 2020). [16]

5.-Abuso de servicio en la nube. Según la pagina Industrial Solutionsdice que: Los atacantes utilizan cada vez más servicios legítimos en la nube para

apoyar sus actividades. Por ejemplo, pueden usar un servicio en la nube para alojar malware encubierto en sitios como GitHub, lanzar ataques DdoS, distribuir correo electrónico de phishing, extraer moneda digital, ejecutar fraude de clics auto matizado o llevar a cabo un ataque de fuerza bruta para robar credenciales.

7.-Ataques Ddos. Los ataques DdoS continúan aumentando en frecuencia y tamaño, creando un riesgo para las empresas y los proveedores de la nube. Los actores de amenazas están utilizando servicios basados en la nube de manera fraudulenta, ya sea a través de hosts comprometidos o servicios anónimos. Después, los recursos de los proveedores de la nube se aprovechan para lanzar ataques contra víctimas.

Tabla 1 Principales amenazas en la nube (Elaboración propia

Principales Amenazas en la nube	
Orden de gravedad	Amenazas
1	Filtraciones en los datos
2	Perdida de datos
3	Interfaces inseguras
4	Ataques Ddos (Denegación de servicio)
5	Secuestro de cuentas
6	Empleados maliciosos
7	Abusos de servicio en la nube

2. Seguridad en dispositivos moviles

Los dispositivos móviles como los smartphones (teléfonos inteligentes) o tabletas son muy útiles, ya que desde ellos podemos conectarnos a internet desde casi cualquier lugar con un plan de datos o por medio de redes wifi.

Básicamente los usamos como un computador, leemos noticias, vemos videos, revisamos el correo, entre otros. Por eso, mantener seguro este tipo de aparatos es muy importante.

2.1 Riesgos de usar la nube en el movil

La nube se ha convertido en algo muy común y muy útil que está presente en todo tipo de dispositivos. Sin embargo, esto también tiene sus riesgos. Se tiene un amplio abanico de opciones, tanto gratuitas como de pago.

Algunos servicios en la nube tendrán más capacidad de almacenamiento, otros permitirán que compartas datos entre dispositivos. Pero siempre se debe Tener en cuenta posibles peligros como los programas inseguros.

El primer riesgo es toparte con programas que son inseguros. Puede que tus datos no estén protegidos, que expongan información, pero incluso podrías estar instalando software que ha sido desarrollado únicamente para estafar. Por ejemplo, esa aplicación para usar la nube que instalas en el móvil, podría estar diseñada para distribuir malware.

Otro riesgo de usar la nube en el móvil es que tus datos personales e información podrían verse comprometidos. Tal vez esa nube que utilizas, aunque la hayas bajado de fuentes oficiales y sea segura, no cifre el contenido. Esto puede suponer un problema, ya que podría quedar expuesto en la red y que accedan a esos datos.

Las copias de seguridad que generes en la nube en el móvil. Son muy útiles para guardar archivos de todo tipo, liberar espacio y poder tener acceso desde cualquier lugar. Pero también pueden suponer un problema importante si esa copia de seguridad queda desprotegida.

Por supuesto, también debes tener en cuenta que otro riesgo de utilizar la nube en el móvil es quedarte sin datos. En caso de que se realice una copia de seguridad. En estos casos lo ideal es conectarte por wi-fi para sincronizar en la nube. Así ahorrarás datos de tu tarifa y no tendrás problemas para poder usar este tipo de servicio sin agotar la tarifa que tienes contratada.

3 Servicios en la nube

El término "servicios en la nube" se refiere a una amplia gama de servicios que se prestan bajo demanda a empresas y clientes a través de Internet. Estos servicios están diseñados para proporcionar un acceso fácil a aplicaciones y recursos, sin necesidad de infraestructura o hardware internos.

3.1Nube Movil

La computación en la nube móvil (o la nube móvil) se refiere a un modelo de procesamiento que se realiza en la nube. Los datos se guardan en la nube y el acceso se realiza mediante un dispositivo móvil que actúa como terminal de presentación o pantalla. Aunque el dispositivo móvil puede ser muy variado, suele referirse al teléfono inteligente (Smartphone). La facilidad de transporte y el tamaño de las tabletas ha hecho que sean estos dos terminales los más considerados al hablar de la nube móvil.

3.2 Modelos de Servicios en la nube

No existe un modelo de servicio

de nube único para todas las empresas.

Estos modelos se clasifican básicamente en tres grupos: infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS)

3.2.1Servicio IaaS

La infraestructura como servicio (IaaS) es una infraestructura de computación en la nube que proporciona recursos de procesado, conectividad y almacenamiento a través de Internet, mediante un modelo de suscripción que puede escalar. Al ofrecerse como servicio de suscripción, se puede escalar hacia arriba o hacia abajo en función de las necesidades, lo que proporciona una mayor flexibilidad en comparación con las infraestructuras locales.

3.2.2Servicio PaaS

La página web IBM dice que: PaaS, o Plataforma como servicio, es un modelo de computación en la nube que proporciona a los clientes una plataforma de nube completa (hardware, software e infraestructura) para desarrollar, ejecutar y gestionar aplicaciones sin el costo, la complejidad y la inflexibilidad que a menudo acompañan a la creación y el mantenimiento de esa plataforma en las instalaciones.
El proveedor PaaS lo aloja todo en su centro de datos: servidores, redes, almacenamiento, software de sistema operativo, bases de datos, herramientas de desarrollo.

3.2.3 Servicio SaaS

Es un modelo de entrega de software basado en la nube en el que el proveedor desarrolla y mantiene el software de las aplicaciones en la nube, proporcionando actualizaciones automáticas del mismo y lo pone a disposición de sus clientes a través de internet con un sistema de pago por uso.

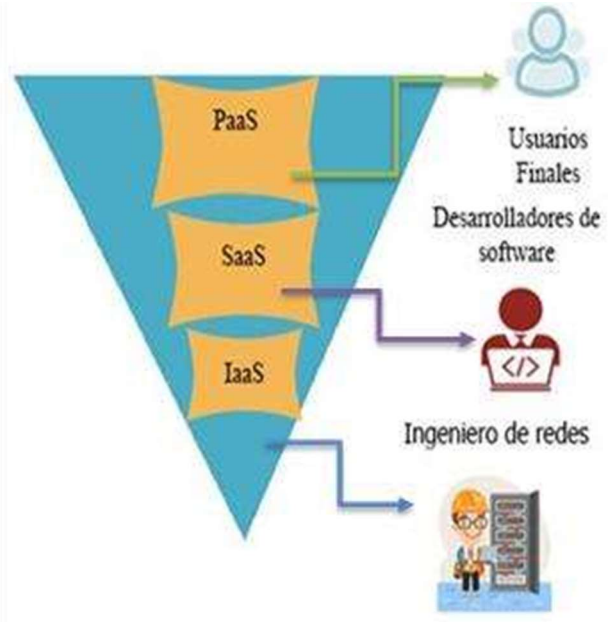

Figura 5 Modelos de servicio en la nube (Elaboración propia)

4 ¿Como identificar si un sitio web es Seguro?

De acuerdo con el autor Ivan de Souza afirma que para identificar una página web segura es necesario verificar la URL de del sitio web y observar si dice "HTTPS" al comienzo de la dirección (en lugar de "HTTP"). Esto significa que el sitio web es seguro con una certificación SSL. Es ella quien protege todos los datos que transitan del navegador al servidor del sitio web. Si aparece un candado al lado de la URL (usualmente de color verde) es señal de que la web es segura y puedes navegar libremente. Para más confiabilidad, al hacer clic en el candado, veremos el certificado SSL de la web y podremos saber si una página es oficial.

4.1 ¿Porque se crean paginas falsas?

Se denomina página web falsa a cualquier sitio web ilegítimo usado como señuelo para atraer a los usuarios hacia un fraude o un ataque malicioso. Los estafadores se aprovechan del anonimato que ofrece internet para ocultar su verdadera identidad e intereses tras diversas máscaras. Con el fin de dar una apariencia de autenticidad, pueden utilizar falsos avisos de seguridad, obsequios y otros formatos engañosos. Normalmente se crean las páginas falsas para obtener nuestros datos personales, contraseñas, números de tarjetas de crédito, número de teléfonos de celulares, correos electrónicos y cuentas de redes sociales.

4.1.2 ¿Como protegernos de las paginas inseguras?

El autor Javier Jimenez señala que es importante es tener siempre los sistemas actualizados. A veces pueden surgir vulnerabilidades que facilitan la entrada de malware y otros tipos de amenazas. Si tenemos nuestro equipo actualizado y con los parches de seguridad adecuados podemos correr menos riesgo.

Es vital tener antivirus y otros programas de seguridad. Es así como hacemos frente a posibles amenazas que comprometan nuestra seguridad y privacidad. Pero además es muy importante no descargar ningún archivo de posibles páginas fraudulentas y tampoco acceder a nuestras cuentas desde links de terceros. Con esto se refiere por ejemplo entrar en las redes sociales desde links que llegan por e-mail o vemos en otras páginas. Podría tratarse de un ataque phishing.

4.2 ¿Que amenazas se pueden encontrar en internet? Malware

La página web Argentina.gob ha afirmado lo siguiente: El malware es un programa malicioso que busca dañar a las computadoras y dispositivos móviles. El malware también se usa para nombrar distintos software hostiles, intrusivos o molestos que abren ventanas con publicidad o expulsan el CD.

Tienen como objetivo:

- Robar información personal.
- Robar tarjetas de crédito y contraseñas.
- Espiar.
- Bloquear equipos.
- Destruir información.
- Usar la computadora para impedir el acceso a sitios web.
- Mostrar publicidad no deseada.

1.-Virus

Se denomina virus a un tipo de programa informático cuya característica distintiva es la capacidad de reproducirse (auto replicarse) e infiltrarse en archivos, sectores de arranque del disco y documentos de forma inadvertida para el usuario. El nombre de virus en relación con los programas informáticos procede de la biología precisamente por su capacidad de reproducirse. Cualquier virus que se encuentre en el disco como un archivo infectado no es peligroso hasta que se abre o se ejecuta. Sólo tiene efecto cuando el usuario lo activa. Los virus están diseñados para replicarse a sí mismos, infectando los ordenadores y generalmente destruyendo los archivos.

2.- Gusanos

Los gusanos son un tipo de virus. Hacen honor a su nombre, ya que se propagan "arrastrándose" de un dispositivo a otro. Como los virus, son programas que se auto replican, sin embargo, a diferencia de los virus, los gusanos no requieren la asistencia del usuario para propagarse. Encuentra un vacío legal por sí mismo.

3.-Troyanos

Los troyanos por su parte son programas maliciosos que son implantados deliberadamente por los ciberdelincuentes para recolectar información, destruirla o modificarla, interrumpir el rendimiento del ordenador o utilizar sus recursos con fines maliciosos. Los troyanos tienen la apariencia de un software legítimo y no son sospechosos. En contraste con los virus, están diseñados para realizar sus funciones.

Con esto cuentan los ciberdelincuentes: su objetivo es crear un programa que los usuarios se atrevan a ejecutar y utilizar.

4.0 Phishing

Proviene de la palabra “fishing” (pesca).El phishing es una de las estafas más antiguas y mejor conocidas de internet. Podemos definirlo como un tipo de fraude en las telecomunicaciones que emplea trucos de ingeniería social para obtener datos privados de sus víctimas.

La información que roba son: Datos personales e información financiera.

El phishing por sitio web: también conocidos como sitios falsificados, es un tipo de fraude que consiste en el envío masivo de emails o sms con un link de ingreso a páginas falsas.

Los hackers crean estos sitios para engañarlo de modo que introduzca sus credenciales de inicio de sesión, que a continuación utilizarán para conectarse a sus cuentas. Las ventanas emergentes son otra fuente habitual de phishing por sitio web.

5.0 Ransomware

Según los autores Patrick Seguin & Nica Latto afirman que el ransomware es un tipo de malware que cifra los archivos y hasta sistemas informáticos enteros para luego pedir el pago de un rescate a cambio de devolver el acceso. El ransomware recurre al cifrado para bloquear el acceso a los archivos o sistemas informáticos infectados, lo que hace que las víctimas no los puedan usar. Los ataques que se hacen con este malware tienen como objetivo toda clase de archivos, desde documentos personales hasta aquellos que resultan esenciales para la marcha de una empresa.

Malware	Objetivos
Virus	X Espía. X bloquea equipos. X destruye información. X usa la computadora para impedir que se acceda a internet.
Gusano	X Bloquea equipos. X usar la computadora para impedir que se acceda a internet.
Troyanos	X Roba información personal. X roba tarjetas de crédito. X espía. X destruye información.
Phishing Rasonware	X Roba información. X roba tarjetas de crédito y contraseñas. X espía. X destruye información. X Bloquea Equipos X espía.

Figura 6 Ataques que utilizan los malwares (elaboración propia)

4.2.3 Robo de identidad y datos personales

Los robos de identidad obtienen información personal como contraseñas, números de identificación, números de tarjetas de crédito, datos de seguridad social con la intención de actuar de manera fraudulenta en nombre de la víctima.

Estos datos sensibles pueden ser utilizados para diversos fines ilegales, como solicitar préstamos, realizar compras en línea o acceder a los datos médicos y financieros de la víctima.

El robo de identidad está muy relacionado con el phishing y otras técnicas de ingeniería social que a menudo se usan para conseguir información sensible de la víctima. Perfiles públicos en redes sociales u otros servicios online pueden ser la fuente para adquirir la información, permitiendo a los criminales hacerse pasar por sus víctimas.

El Gobierno de Mexico menciona que para prevenir el robo de identidad se recomienda lo siguiente.

1.-Estado de cuenta

Verificarlos constantemente para identificar movimientos que no se recuerde haber efectuado, en ese caso será necesario acudir a la CONDUSEF o a la institución financiera para descartar un robo de identidad.

2.- Eliminación de documentos: Al deshacerte de los documentos que contengan información personal o financiera, o tarjetas de crédito o débito vencidas, destrúyelos perfectamente.

3.-Correos electrónico: Se debe eliminar cualquier mensaje de origen sospechoso o que solicite información personal o financiera. Es mejor no abrirlos, e informa al proveedor de internet, para ayudar a erradicarlos.
4.- Computadoras Seguras: No utilices equipos públicos para realizar movimientos bancarios o de compras por internet. La información puede quedar grabada en ellos con el uso de software maligno.
5.- Compras por Internet: Asegúrate de que el sitio que visitas sea totalmente seguro y confiable. El proveedor debe informar su identidad, denominación legal, políticas de venta y de privacidad, así como datos de su ubicación física.

CONCLUSIONES

La seguridad en la nube es un tema muy importante de conocer al momento de contratar los servicios en la nube. Los datos se deben de proteger para garantizar su privacidad. Elegir la nube adecuada no es fácil y tomar una decisión que depende de las necesidades de la empresa, de su presupuesto, del control que desee tener sobre la información y los datos.

La seguridad en la nube debería de tener mucha más importancia debido a que muchas personas desconocen los riesgos y ataques cibernéticos a que están expuestos. Hay beneficios y riesgos que deben ser analizados antes de proceder en un proyecto de computación hasta la elección de un proveedor adecuado

El desarrollo de la presente investigación es dar a cuenta que la seguridad en la nube es de suma importancia ya que facilita el trabajo y la comunicación digital y es mucho más seguro para poder almacenar nuestros documentos importantes y así podemos evitar pérdidas de información valiosa.

Recomendaciones finales:
1.- No usar la misma contraseña en todos lados 2.-Usar caracteres especiales
3.-Crear patrones
4.-Utilizar gestores de contraseñas
5.-Protege todos los dispositivos que usas para acceder a los datos en la nube, como teléfonos inteligentes, laptops y tabletas.

REFERENCIAS

1. Agendapro, B. (23 de Octubre de 2020). AgendaPro. Obtenido de Servicios en la nube: . https://blog.agendapro.com/servicios-en-la- nube

2. Argentina.gob. (15 de Septiembre de 2020). Guía para madres, padres, familias y docentesGuía para madres, padres, familias y docentes. Obtenido de Amenazas en internet: https://www.argentina.gob.ar/justicia/convose nlaweb/situaciones/guia-para-madrespadres- docentes-amenazas-internet

3. ATLASSIAN. (s.f.). Microservicios. Obtenido de Infraestructura como servicio: https://www.atlassian.com/es/microservices/cl oud-computing/infrastructure-as-a-service

4. Borreda L. (23 de Abril de 2021). Red Seguridad. Obtenido de Seguridad en la nube
¿ porque es tan importante?: https://www.redseguridad.com/actualidad/prot eccion-de-datos-actualidad/seguridad-en-la- nube-por-que-estan-importante_20210423.html

5. Cloudflare. (s.f.). Cloudflare. Obtenido de
¿Que es la nube?: .). https://www.cloudflare.com/es- es/learning/cloud/what-is-the-cloud/

6. Colaborador de DocuSign. (18 de Diciembre de 2019). DocuSign. Obtenido de Criptografia: https://www.docusign.mx/blog/que-es-la- criptografia

7. Diana Cortez Pérez . (4 de Julio de 2021). Ceupe. Obtenido de Cuales son las amenazas en internet?: https://www.ceupe.com/blog/cuales-son-las- amenazas-en-internet.html

8. Eset. (s.f.). Eset. Obtenido de Robo de identidad: https://www.eset.com/es/robo-de- identidad/

9. Ghosh. A. (26 de Julio de 2022). redpoints. Obtenido de como saber si una pagina web es falsa: https://www.redpoints.com/es/blog/como- saber-si-una-pagina-web-es-falsa/

10. Gobierno de Mexico. (07 de Noviembre de 2016). Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. Obtenido de ¿Sabes que es el robo de identidad?: Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros

11. IBM. (14 de Julio de 2021). IBM. Obtenido de Plataforma como servicio: https://www.ibm.com/mx-es/cloud/learn/paas

12. Industrial Solutions. (22 de Abril de 2021). Obtenido de https://www.indsol.com.mx/5221-2/

13. Ivan de Souza. (22 de Mayo de 2021). Rock Content. Obtenido de Como saber si un sitio web es seguro: https://rockcontent.com/es/blog/como-saber- si-un-sitio-web-es-seguro/

14. Ivan Jahel Bautista Garcia. (6 de Febrero de 2021). servnet. Obtenido de Que es una nube hibrida: https://www.servnet.mx/blog/que-es- una-nube-hibrida

15. Javier Jimenez. (30 de Mayo de 2019). RedesZone. Obtenido de Señales que indican que una web es insegura:

https://www.redeszone.net/2019/05/30/detecta r-paginas-inseguras-protegernos/

16. Javier Jimenez. (08 de Febrero de 2023). redeszone. Obtenido de https://www.redeszone.net/noticias/seguridad/ errores-evitar-usarcuenta-banco-movil/

17. Kasperky. (11 de Mayo de 2022). Kasperky. Obtenido de ¿Que es la seguridad en la nube?: https://www.kaspersky.es/resource-center/definitions/what-is-cloud-security

18. Oracle. (s.f.). Oracle. Obtenido de ¿Que es Saas?: https://www.oracle.com/mx/applications/what -is-saas/

19. OSI. (10 de Octubre de 2019). Oficina de seguridad internauta. Obtenido de Tipos de cifrado: https://www.osi.es/es/actualidad/blog/2019/07

/10/sabias-que-existen-distintos-tipos-de- cifrado-para-proteger-la-privacidad

20. Patrick Seguin & Nica Latto. (24 de Septiembre de 2021). Avast. Obtenido de la guia esencial sobre el rasonware.

21. Ramon Planet Huesa. (20 de Octubre de 2022). Cloud Master. Obtenido de Los ciberdelincuentes utilizan la nube para los ataques DDoS ¿Sabías qué…?: https://www.cloudmasters.es/los- ciberdelincuentes-utilizan-la-nube-para-los- ataques-ddos-sabias-que/

22. RedHat. (10 de Octubre de 2022). redhat. Obtenido de redhat: https://www.redhat.com/es/topics/cloud- computing/what-ispubliccloud

23. Stark K. (20 de Febrero de 2020). Evaluandocloud. Obtenido de Amenazas y riesgos de la nube: https://evaluandocloud.com/amenazas- riesgos-la-nube/

24. VMware. (26 de Enero de 2023). Que es una nube privada. Obtenido de https://www.vmware.com/latam/topics/glossary/content/private-cloud.html