

ANÁLISIS DE LAS AMENAZAS CIBERNÉTICAS MAS REPRESENTATIVAS QUE
ENFRENTAN LOS SERVICIOS DE NUBE PUBLICA

CRISTIAN ANDRES CAÑÓN RECALDE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA, CAQUETÁ
2022

ANÁLISIS DE LAS AMENAZAS CIBERNÉTICAS MAS REPRESENTATIVAS QUE
ENFRENTAN LOS SERVICIOS DE NUBE PUBLICA

CRISTIAN ANDRES CAÑÓN RECALDE

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director:
MIGUEL ANDRES AVILA GUALDRON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
FLORENCIA, CAQUETÁ
2022

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con amor dedico este trabajo a mis padres, que, me acompañaron en esta etapa tan importante en mi vida y por la cual puedo estar orgulloso de tenerlos en mi vida. De igual forma agradezco a mi novia por su apoyo, motivación y colaboración para el desarrollo de esta especialidad.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

De manera especial a las orientaciones del Ingeniero Miguel Andrés Ávila Gualdron, quien estuvo desde principio a fin en el desarrollo del proyecto, compartiéndonos sus conocimientos en el tema.

CONTENIDO

	Pág.
1 GLOSARIO	6
INTRODUCCIÓN	10
2 DEFINICIÓN DEL PROBLEMA	11
2.1 ANTECEDENTES DEL PROBLEMA	11
2.2 FORMULACIÓN DEL PROBLEMA	11
3 JUSTIFICACIÓN	13
4 OBJETIVOS	15
4.1 OBJETIVO GENERAL	15
4.2 OBJETIVOS ESPECÍFICOS	15
5 MARCO REFERENCIAL	16
5.1 MARCO TEÓRICO	16
5.1.1 Las nubes.	16
5.1.2 Análisis forense digital.	19
5.2 MARCO CONCEPTUAL	21
5.3 MARCO HISTÓRICO	23
5.4 antecedentes o estado actual	24
5.4.1 Ranking de amenazas	25
5.4.2 Clientes y casos de éxito.	26
5.5 MARCO LEGAL	29
6 DESARROLLO DE LOS OBJETIVOS	31
6.1 amenazas CIBERNÉTICAS que enfrentan los servicios de almacenamiento DE NUBES PÚBLICAS	31
6.1.1 AMENAZAS Y RIESGOS CONTRA LOS SERVICIOS EN LA NUBE	36
6.1.2 AMENAZAS Y RIESGOS PARA LOS SERVIDORES	39
6.1.3 AMENAZAS Y RIESGOS CONTRA LOS USUARIOS	39
6.2 TÉCNICAS Y táCTICAS UTILIZADAS POR LOS CIBERCRIMINALES.	40
6.2.1 METODOLOGIAS UTILIZADAS POR LOS CIBERDELINCIENTES	43
6.2.2 HERRAMIENTAS UTILIZADAS POR LOS CIBERDELINCIENTES	50
6.3 RECOMENDACIONES Y BUENAS PRACTICAS ENFOCADAS A LOS USUARIOS	51
7 CONCLUSIONES	54
8 RECOMENDACIONES	56
9 DIVULGACIÓN	57
10 ANEXO	58
BIBLIOGRAFÍA	59

LISTA DE ILUSTRACIONES

	Pág.
Ilustración 1 Nuevas tecnologías en Japón	27
Ilustración 2 Ataque DDoS.....	32
Ilustración 3 Ataque Man in the Middle	36
Ilustración 4 Matriz ATT&CK.....	41
Ilustración 5 Clasificación de tácticas, técnicas y mitigaciones.....	41
Ilustración 6 Matriz PRE-ATT&CK	42
Ilustración 7 Modelo OSSTMM	44
Ilustración 8 Modelo ISSAF.....	45
Ilustración 9 Evaluación de una vulnerabilidad por OWASP	46
Ilustración 10 Identificación de amenazas Offensive Security	49

1 GLOSARIO

ANÁLISIS DE LOS RIESGOS: “Procesos sistemáticos para identificar y estimar la magnitud del riesgo sobre un sistema de información”¹.

ARTEFACTO FORENSE: “Mecanismos de registro sobre actividades por el usuario en el sistema, programas utilizados, accesos que realizan, conexiones, aplicaciones, etc.”²

CLÚSTER: Servidores que trabajan en conjunto de una sola máquina, para mejorar el rendimiento de las operaciones implantadas en el sistema.

CSP (CLOUD SERVICE PROVIDER): Es una organización dedicada a proveer servicio y tecnología en infraestructura en la nube.³

DATA CENTER: Un centro de almacenamiento de datos y que provee servicios de negocio, siendo de forma segura con respecto a sus aplicaciones y datos a usuarios remotos a través de la web.⁴

CLOUD O NUBE: Es un símbolo que se usa para representar al internet.

COMPUTING O COMPUTACIÓN: Congrega conceptos sobre la informática, la lógica coordinada y almacenamiento.

HARDWARE COMO SERVICIOS (Haas, Hardware As A Service): Son centro de datos con todo tipo de máquinas proporcionando para la computación, catálogos y almacenamiento.

WEB PLATAFORMAS: Son plataformas que se una en la web para la publicación de aplicaciones o páginas web orientadas a servicios donde se interactúan con otros sitios web para presentar información y en un solo sitio

¹ MELL GRANCE. (2011). THE NIST DEFINITION OF CLOUD COMPUTING RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.(EN LINEA)

² AREOS, I. (2015). ARTEFACTOS FORENSES.(EN LINEA) Obtenido de <http://insecuredata.blogspot.com/2015/03/artefactos-forenses-i.html>

³ CSA. (2011). CLOUD SECURITY ALLIANCE (EN LINEA). GUÍAS DE SEGURIDAD DE ÁREAS CRÍTICAS EN CLOUD COMPUTING V3.0.

⁴ CCN. (2014). CENTRO CRIPTOLOGICO NACIONAL (EN LINEA). GUÍA DE SERGURDAD DE LAS TIC.

COMMUNITY SOURCE: Se proporciona a vendedores independientes de software y hardware la oportunidad de desarrollar tecnología de virtualización avanzada.⁵

MALWARE: “Software malicioso. Código de software informático cuyo objetivo es provocar daño a un sistema”⁶

CIBERCRIMEN: Es una actividad delictiva que afecta a una computadora por ejemplo su red informática o su dispositivo en red.

DELITO INFORMÁTICO: El delito informático es una implantación de virus, la suplantación de sitios web, violando los derechos de autor entre otros.

⁵ CHANG, F., DEAN, J., GHEMAWAT, S., HSIEH, W. C., WALLACH, D. A., BURROWS, M., Y OTROS. (NOVIEMBRE DE 2006). BIGTABLE: A DISTRIBUTED STORAGE SYSTEM FOR STRUCTURED DATA. SEVENTH SYMPOSIUM ON OPERATING SYSTEM DESIGN AND IMPLEMENTATION. SEATTLE, WA.

⁶ RIVERO, MARCELO. S.F. ¿QUÉ SON LOS MALWARES? [EN LÍNEA].
<[HTTPS://WWW.INFOSPYWARE.COM/ARTICULOS/QUE-SON-LOS-MALWARES/](https://www.infospymware.com/articulos/que-son-los-malwares/)>.

RESUMEN

Los nuevos avances de las tecnologías han permitido que las actividades cotidianas dependan de los servicios TI (Tecnologías de la información), lo que ha dado paso a la necesidad de adquirir espacios virtualizados para almacenar la información y de esta manera, acceder a los datos de forma más ágil, en diferentes ubicaciones geográficas sin tener un dispositivo físico.⁷

Con este auge tecnológico, se han creado diferentes servicios, denominados nube pública, privada o híbrida, en los cuales, se utilizan recursos de varios servidores interconectados a la red, facilitando la suma de capacidades relacionadas con el procesamiento de cómputo y el almacenamiento de información. Esta unión facilita la masificación del uso del internet para la creación de aplicaciones web, el almacenamiento de datos y el desarrollo en general de miles de negocios que favorecen el mundo social, económico y personal de los seres humanos.⁸.

Teniendo en cuenta estos avances, es importante mencionar los diversos riesgos que también se plantean con ellos, a los que se enfoca la atención de este trabajo, realizando un análisis de las amenazas cibernéticas más típicas que enfrentan los servicios de nube pública, enfocando sus resultados en la creación de TI, recomendaciones de seguridad para los usuarios finales de estas tecnologías. Sin embargo, la asignación de responsabilidades entre el proveedor de la nube pública y la organización del cliente varía mucho según el modelo informático: SaaS, PaaS o IaaS.

Palabras clave: SaaS, PaaS, IaaS,

⁷ Ortiz Chimbo, K. M., Luna Aveiga, H., Yanez, R. M., & Parra, M. A. (2016). LA IMPORTANCIA DEL USO DE LAS CLOUD COMPUTTING EN LAS EMPRESAS PUBLICAS Y PRIVADAS.(EN LINEA). *CONTRIBUCIONES A LA ECONOMÍA*.

⁸ Orozco, I., & Jacobs, O. (2017). LA NUEVA ERA DE LOS NEGOCIOS: COMPUTACIÓN EN LA NUBE.(EN LINEA). *REVISTA ELECTRÓNICA DE ESTUDIOS TELEMÁTICOS*, 21.

ABSTRACT

The new advances in technology have allowed daily activities to depend on IT services (Information Technology), which has given way to the need to acquire virtualized spaces to store information and thus access data from more agile way, in different geographical locations without having a physical device.

With this technological boom, different services have been created, called public, private or hybrid cloud, in which resources from several servers interconnected to the network are used, facilitating the sum of capacities related to computing processing and information storage. . This union facilitates the widespread use of the Internet for the creation of web applications, data storage and the general development of thousands of businesses that favor the social, economic and personal world of human beings. .

Taking into account these advances, it is important to mention the various risks that are also posed with them, to which the attention of this work is focused, carrying out an analysis of the most typical cyber threats faced by public cloud services, focusing on their results. in creating IT, security recommendations for end users of these technologies. However, the allocation of responsibilities between the public cloud provider and the customer organization varies greatly depending on the computing model: SaaS, PaaS, or LaaS.

Keywords: SaaS, PaaS, Laas,

INTRODUCCIÓN

La nueva era de las tecnologías de la información ha facilitado a las plataformas que cuenten con una disponibilidad 24/7 (24 horas al día, 7 días a la semana), así como, una mayor eficiencia por un bajo costo. Esta evolución tecnológica ha creado la necesidad de tener acceso a la información en cualquier parte del mundo, definiéndose como “Cloud Computing o computación en la nube”, convirtiéndose en servicios apetecidos por las empresas debido a que en la mayoría de sus configuraciones solo se paga por los servicios requeridos evitando los costos de adquisición, administración y manejo de la infraestructura tecnológica a nivel físico.

Si bien los proveedores de servicios en la nube se esfuerzan por garantizar un alto nivel de seguridad en el acceso y el control de la información que manejan de sus clientes, las debilidades o las malas prácticas pueden ser descubiertas por sus clientes y usuarios conducen a incidentes cibernéticos, por esta razón es importante generar conciencia de las amenazas y riesgos que ocurren en el ciberespacio para reducir la posibilidad de que los ciberdelincuentes afecten los servicios, extraigan información o dañen el sistema.

En este documento, se aborda un tema relacionado con las amenazas cibernéticas más representativas que enfrentan los servicios de la nube pública y la seguridad de la información, así como algunas vulnerabilidades de los servidores.

2 DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

Día a día los avances tecnológicos han hecho que las organizaciones y los clientes puedan tener acceso a la información y alternativas de fácil alcance. Esto ha ocasionado, que las empresas afronten la necesidad de transformar sus actividades para cumplir con los actuales requerimientos de sus clientes; aprovechando para esta tarea la innovación digital, así como los nuevos esquemas de trabajo que se han venido desarrollando en los últimos años.

De acuerdo con lo anterior esta investigación parte de una serie de hechos y situaciones que se han venido presentado en algunas empresas con la implementación de nuevas tecnologías, las cuales han acrecentado las amenazas cibernéticas en sus activos informáticos y sobre todo el riesgo de exfiltración en los datos almacenados en servidores de nube pública⁹.

Estos riesgos mencionados, requieren un análisis del entorno de los sistemas de la nube, que permita poner en contexto el funcionamiento de este tipo de herramientas para las organizaciones, incluyendo su definición con respecto a las variables que pueden influir en su implementación, y de esta forma brindar algunas recomendaciones que pretendan minimizar las vulnerabilidades asociadas con este tipo de tecnologías, al igual que, buenas prácticas para facilitar la detección de los riesgos alineados con las normas vigentes.¹⁰ Por otra parte, dar a conocer recomendaciones generales para los usuarios de estas tecnologías, con el fin de prevenir incidentes cibernéticos que pongan en riesgo la seguridad de la información.

2.2 FORMULACIÓN DEL PROBLEMA

Algunos de los proveedores de Cloud proporcionan a las organizaciones la infraestructura con capacidad para el almacenamiento de información y seguridad porque en ella se ejecutan diferentes aplicaciones, en donde los usuarios solo deben contar con un servicio de internet, ya que los servidores y el software que ofrecen solo se gestionan bajo el esquema del servicio que ofrecen. Además, se tiene como expectativa la seguridad de la información ya que se encuentran en repositorios y como se debe tener control adecuado de los datos puesto en internet. Debido a las amenazas

⁹ (CHAKI & CHAKI, 2014)

¹⁰ BROW ANDERSON. (2018). SECURITY RISKS AND COUNTERMEASURES (EN LINEA). ATHABASCA UNIVERSITY.

y riesgos que se puedan acarrear debido al acceso de la información o el mal manejo que puedan darle a ese uso.

Las amenazas en la nube pueden ocasionar incidentes y provoca daños en la reputación y pérdidas económicas. Debido a esta circunstancia se debe efectuar un análisis de posibles riesgos que se encuentran en la nube, afectando a los servicios que se contratan para poner medidas adecuadas para tratarlos.

De esta manera, se realiza el análisis a un modelo investigativo que contenga evidencias sobre sistemas Cloud haciendo énfasis a los usuarios finales, asimismo, establecer hipótesis de investigación y seleccionar elementos a estudiar.

Con el tiempo han surgido una serie de nuevas advertencias que afectan a las arquitecturas Cloud. La regulación o el monitoreo de seguridad constante es de ayuda para identificar las posibles amenazas en la que se enfrentan las nubes públicas, para ello es importante evaluar las prevenciones convencionales

Teniendo en cuenta lo anterior, surge el planteamiento de este proyecto, centrándose en ¿Cómo el análisis de las amenazas cibernéticas más representativas que enfrentan los servicios de nube pública puede aportar buenas prácticas de seguridad informática orientadas a los usuarios?

3 JUSTIFICACIÓN

En la actualidad las empresas quieren estar en una posición competitiva, siendo esto complejo y costoso. Por esta razón las tecnologías ofrecen en gran parte tener menos costo con respecto a su infraestructura, generando mayor y mejor funcionalidad, por esta razón se proponen modelos de servicios tecnológicos a través de los servicios de la nube, respondiendo a las necesidades de cada empresa, siendo flexible y adaptiva¹¹

Fábrega¹² dice que la computación en la nube libera recursos que podrán direccionarse hacia otros puntos estratégicos de la organización. En el sentido de la infraestructura tecnológica para ser un servicio más. De igual forma se involucran aspectos de análisis forense siendo una necesidad por los incidentes de seguridad que pasa a diario. Como, por ejemplo: pérdida de información debido a virus.

En esta propuesta tecnológica se considera de importancia para el funcionamiento de los diferentes tipos de servicios de la nube con respecto a sus modelos, siendo impacto que causa a las organizaciones en relación con reducción de costos destinados a infraestructura, pero también implica más seguridad en la información de sus datos¹³. Debido que en la actualidad se dan ataques de grupos hackers afectando la Infraestructura informática de organizaciones. Identificando las amenazas y dependiendo del tipo de ataque que usen así mismo se podrá saber el servicio afectado como, por ejemplo, los servicios financieros, el comercio electrónico, software y servicios basados en la nube.

Esto lleva a determinar la seguridad es uno de los principales problemas en el ámbito de la transmisión de datos y eso ha generado que la aparición de Cloud Computing crezca conforme a los servicios en la nube. Debido a que la seguridad se convierte en punto relevante, pues los datos del usuario se encuentran almacenados en servidores gestionados por proveedores que no garantiza el cien por ciento de confiabilidad.¹⁴ Actualmente, un ataque bien organizado por parte de un grupo de piratas informáticos puede afectar la infraestructura del sistema TI de una organización. Los piratas informáticos que utilizan DDoS (ataques de denegación de servicio) pueden atacar

¹¹ BURNS, A., HERRING, C., & PETERSON, K. (2007). PROVABLE DATA POSSESSION AT UNTRUSTED STORES. (EN LINEA).

¹² FABREGA, A. (2012). UN CONCEPTO TECNOLÓGICO REVOLUCIONARIO Y DE GRAN IMPACTO ECONÓMICO. (EN LINEA). *INNOVACION*.

¹³ PASTRANA PERALTA, F. S., MUÑOS RAMOS, J. S., & RUIZ RUIZ, R. A. (2016). IMPLEMENTACIÓN DE UNA NUBE PRIVADA PARA LOS SERVICIOS INTERNOS DE LA DIRECCIÓN DE PROMOCIÓN A LA INNOVACIÓN Y CREATIVIDAD DEL MINISTERIO DE LA JUVENTUD DE MANAGUA. (EN LINEA). *UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA*.

¹⁴ CONTRACTOR PATEL. (2012). TRUT MANAGEMENT FRAMEWORK FOR ATTENUATION OF APPLICATION LAYER DOS ATTACK INCLOUD COMPUTING. (EN LINEA).

servicios financieros, comercio electrónico, juegos en línea, agencias gubernamentales, software y servicios basados en la nube.

La importancia de conocer las características de los servicios en la nube y las amenazas donde se derivan los riesgos y así darle el tratamiento adecuado. Ya sea ataques indirectos o directos, también los Hackers y actores estatales, errores de los empleados y personas malintencionadas.

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Analizar las amenazas cibernéticas más representativas que enfrentan los servicios de almacenamiento en nubes públicas para la generación de buenas prácticas de seguridad informática orientadas a los usuarios

4.2 OBJETIVOS ESPECÍFICOS

- Establecer las amenazas cibernéticas que enfrentan los servicios de almacenamiento en nubes públicas para la identificación de los riesgos más representativos.
- Comparar las técnicas y tácticas utilizadas por los cibercriminales para la materialización de las amenazas cibernéticas que enfrentan los servicios de almacenamiento en nubes públicas.
- Proponer recomendaciones y buenas prácticas de seguridad informática enfocadas a usuarios de los servicios de almacenamiento en nubes publicas

5 MARCO REFERENCIAL

Para el desarrollo de la investigación se tiene en cuenta algunos conceptos teóricos que ayuden a entender el problema planteado.

5.1 MARCO TEÓRICO

5.1.1 Las nubes.

5.1.1.1 La Evolución de la nube.

La nube computacional permite acceder fácilmente a la petición del usuario, siendo un recurso informático compartidos y configurados para suministrar información o interacción del proveedor de servicios¹⁵.

Entre 1997 y 2001, fue denominado “Explosión de la burbuja.com”. Impulsando a nuevas compañías como Amazon.com a modernizar el desarrollo de su Nube informática como su Data Center. Amazon fue uno de los “que comenzó a proveer acceso a sus sistemas a través de su plataforma “Amazon Web Services” mediante servicios Simple Storage Service (S3) y Elastic Compute Cloud (EC2) en el 2006”¹⁶.

5.1.1.2 Arquitectura general de la informática en la nube.

Cuatro modelos de despliegue, el público, privado, híbrido y comunidad, contando con unos modelos de servicio como Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS). Una de las características esenciales que lo conforma es su amplio acceso a la red, elasticidad y rapidez, servicios supervisados y autoservicios a la carta.

5.1.1.3 Tipos de nube

Nube Pública

Según Pastrana, la nube pública “Es el modelo estándar de la computación en la nube en el cual un proveedor de servicios pone sus recursos tales como aplicaciones y almacenamiento disponibles al público en general a través de Internet. Los servicios de

¹⁵JOYANES AGUILAR, L. (2010). COMPUTACIÓN EN LA NUBE NOTAS PARA UNA ESTRATEGIA ESPAÑOLA EN CLOUD COMPUTING.(EN LINEA). UNIVERSIDAD PONIFICIA COMILLAS.

¹⁶ PRIMORAC, C. R., & LA RED, D. L. (2014). COMPUTACIÓN EN LA NUBE (MONOGRAFIA DE ADSCRIPCIÓN DE LICENCIATURA EN COMPUTACIÓN).(EN LINEA).

la nube pueden ser libres (gratuitos) o bien ofertados mediante un modelo de pago por uso”¹⁷.

Pastrana, describen una nube pública como “aquellas abiertas al público y son propiedad de un proveedor de Cloud Computing que, adicionalmente, se encarga de gestionarlas con todas las garantías de privacidad, seguridad y disponibilidad, así como las penalizaciones por incumplimiento, deben estar expresadas en el contrato de servicio. También proporcionan ahorros en costes y gran flexibilidad de seguridad de los datos de los que hace uso”¹⁸.

Ventajas que ofrece la nube pública:

- Precios accesibles en contar con una nube privada, con posibilidades de pagar por horas, se puede pagar por el consumo.
- Su servicio disponible 24 horas.
- Es adaptable a cualquier empresa para su uso.
- Capacidad de procesamiento y almacenamiento sin instalar maquinas locales.

Desventajas son:

- El funcionamiento de las aplicaciones está ligadas al acceso a internet debido a que no están almacenadas de forma local por ende el rendimiento puede ser menor.
- Los datos sensibles del cliente pueden verse en riesgo de cualquier robo de información dado que depende de la seguridad que proporciona el proveedor.
- A medida que mas usuarios hagan uso de la infraestructura en la nube, está no proporciona un optimo esquema de crecimiento o escalabilidad, esto conlleva a degradaciones en el servicio.
- En caso de fallar el servicio que ofrece el proveedor, existen diferentes dificultades al momento de restablecer el servicio o en el peor de los casos, migrar el servicio para otro proveedor o establecerlo de forma local.¹⁹

¹⁷ Pastrana Peralta, F., Muñoz Ramos, J., & Ruiz Ruiz, R. (2016). Servicios en la Nube [En línea]. Obtenido de Implementación de una nube privada para los servicios internos de la Dirección de Promoción a la Innovación y Creatividad del Ministerio de la Juventud de Managua, en el segundo semestre de 2016 [En línea].

¹⁸ Ibid., p. 8

¹⁹ Kezherashvili, B. (s.f.). Computación en la Nube [En línea]. Obtenido de Disponible en: http://www.adminso.es/recursos/Proyectos/PFM/2011_12/PFM_cloud_beka.pdf

Nube Comunitaria:

Carlos R, Primorac. & Dr. David Luis La Red, M. (2014). "Nos describen que la nube comunitaria es una infraestructura en nube que está preparada para el uso de una comunidad específica de consumidores de organizaciones que tienen intereses compartidos (por ejemplo, misión, requerimientos de seguridad y políticas). Puede ser de propiedad, administrada y operada por una o más de las organizaciones en la comunidad, por un tercero o una combinación de ambos y puede existir dentro o fuera de las instalaciones"²⁰.

Nube Híbrida:

"Se trata de una combinación de nubes públicas y privadas. El cliente está en posesión de unas partes y comparte otras, esto además puede ser de manera controlada. Las nubes híbridas ofrecen la ventaja del escalado proporcionado externamente, bajo demanda, se añade la posibilidad de determinar cómo distribuir las aplicaciones a través de los ambientes diferentes. Las nubes híbridas pueden resultar atractivas ya que, por ejemplo, se puede poseer el entorno de aplicaciones y medios de almacenamiento propios y usar la nube para distribuir y compartir datos además de las capas de infraestructura en las que ejecutar las aplicaciones"²¹.

Nube Privada:

En esta nube, es distinta a las demás por el siempre hecho de que su uso es exclusivo para su organización comprendiendo varios consumidores, Su principal característica son:

- Sus recursos agrupados, permitiendo la agrupación de unidades para impulsar la eficacia y estabilidad de sus recursos. Elasticidad, cuando los recursos se encuentran agrupados, se pueden expandir o contraerse por medio de flujo de trabajo.
- Autoservicio, por medio de un portal o sistema interactivo podrán configurar ya sea quien administra los servicios TI, proveedores o los clientes de servicio permitiendo la automatización de los recursos.
- Control y personalización, significa que tendrán mayor control y personalización de la arquitectura o modelos de servicios de la nube²².

²⁰ PRIMORAC, C. R., & LA RED, D. L. (2014). *COMPUTACIÓN EN LA NUBE (MONOGRAFIA DE ADSCRIPCIÓN DE LICENCIATURA EN COMPUTACIÓN)*.(EN LINEA).

²¹ OSCAR AVILA. (2012). DIRECCIÓN GENERAL DE POLÍTICAS INTERIORES (EN LINEA). *COMPUTACIÓN EN LA NUBE*.

²² BUYYA, B., & GOSCINSKI, A. (2014). *PRINCIPIOS Y PARADIGMAS DE LA NUBE COMPUTACIONAL*.(EN LINEA).

5.1.1.4 Modelos de servicios en la nube.

IAAS (Infraestructura como servicio): Es un servicio que suministra el debido espacio en el disco duro, tiempo en CPU, transferencia de datos y base de datos. Comúnmente conocida como solución basada en virtualización de servidores²³.

PASS (Plataforma como servicio): “El cliente es el que contrata la plataforma TI, para implementar aplicaciones desde internet, es un nivel superior a IAAS porque tiene más dependencia del proveedor. Algunos ejemplos son como Google engine, Microsoft Azure, INV- computación en la nube, Force de Salesforce.com.”²⁴

SAAS (Software como servicio): El proveedor ofrece un software para el uso del cliente, es un nivel completo y alto entre los 3 modelos. Ya que el proveedor y administrador instala una infraestructura de tipo software o aplicación. Mediante internet, sin necesidad de contar una infraestructura TI o licencias de software para su uso^{25,26}.

5.1.2 Análisis forense digital.

Son técnicas científicas y analíticas especializadas a infraestructura tecnológica permitiendo identificar, preservar, analizar y mostrar datos que sean validos con respecto a los procesos legales.

Esta disciplina no solo usa las tecnologías de punta para la integridad de datos, sino que requiere de conocimientos avanzados en materia informática y sistemas. Esto abarca el hardware, con respecto a sus redes, seguridad, hacking y recuperación de información.

5.1.2.1 Metodología de Análisis Forense:

Se enumeran:

La identificación de fuentes para capturar la información para la investigación.

²³ CONTRACTOR PATEL. (2012). TRUT MANAGEMENT FRAMEWORK FOR ATTENUATION OF APPLICATION LAYER DOS ATTACK INCLOUD COMPUTING.(EN LINEA).

²⁴ GARFINKEL ROSENBLUM. (2013). VIRTUAL MACHINE INTROSPECTION BASED ARCHITECTURE FOR INTRUSION DETECTION.(EN LINEA).

²⁵ GROBAUER, W. (2012). UNDERSTANDING CLOUD COMPUTING VULNERABILITIES.(EN LINEA). *IEEE COMPUTER SOCIETY*.

²⁶ HARAUZ KAUFMAN. (2010). POTTER DATA SECURITY IN THE WORL OF CLOUD COMPUTING (EN LINEA). *IEEE COMPUTER AND RELIABILITY SOCIETIES*.

La realización de una recolección de la información conservando su cadena de custodia, no alterando sus datos de origen.

La realización de una imagen con su información original, siendo analizada y documentada para cada uno de los hallazgos obtenidos.

Luego de obtener los resultados, se procederá a realizar unas conclusiones, las cuales ayudaran a la toma de decisiones legales o correctivas dependiendo del caso.

5.1.2.2 Análisis Forense en la Nube:

Es un subconjunto de la ciencia de forense de la red. Es una disciplina transversal entre computación en la nube y análisis forense digital, a continuación, se mencionan las tres dimensiones de la nube forense:

La dimensión técnica: Siendo un conjunto de herramientas necesarias para llevar a cabo el proceso forense, en la computación de la nube.

La dimensión organizacional: En la investigación forense en los entornos computacional de la nube, se encuentran divididos en dos, involucrando al consumidor de la nube y el CSP.

La cadena de dependencia: Proveedores de servicios de nube con aplicaciones de la nube con dependencia de otros CSP. Los problemas pueden derivarse o interrumpirse en numerosas cadenas o por falta de coordinación entre todas las partes involucradas.²⁷

5.1.2.3 Análisis Forense en la Nube:

Impulsores

Dichos autores²⁸ han identificado promotores sobre el Cloud Computing.

Tercerización: Ahora las organizaciones quieren que sus procesos de negocio se expandan cada vez más, incluyendo toda la parte de computacional en ciertas aplicaciones por parte de los terceros.

²⁷ LLEIXA, A. (2015). *LA EVIDENCIA DIGITAL ANTE RIESGOS Y AMENAZAS EN EL CLOUD COMPUTING. ASPECTOS PROFESIONALES: PROTECCIÓN DE DATOS, CLOUD COMPUTING Y SISTEMAS DE GESTIÓN*. (EN LINEA). Obtenido de <http://www.aspectosprofesionales.info/2015/06/la-evidencia-digital-ante-riesgos-y.html>

²⁸ SULLIVAN, F. (2009). GUEST EDITOR'S INTRODUCTION: CLOUD COMPUTING FOR THE SCIENCES. (EN LINEA). (I. C. SOCIETY., ED.) *COMPUTING IN SCIENCE AND ENGINEERING*, 11 (4), 10-11. <http://www.savvis.net/en-US/Pages/Home.aspx>.

Tiempo de Valoración y Desempeño: La computación en la nube está orientada a presentar servicios con mayor desempeño y la entrega de aplicaciones que cumpla las necesidades de cada empresa. Siendo los Data Centers un medio para proveer una mayor capacidad de almacenamiento y alta disponibilidad de acceso.

Ubicación: Facilidad de acceso para todo el mundo en todo lugar, los empleados o usuarios pueden tener acceso dentro de las oficinas o desde sus casas, permitiendo estar en cualquier lugar.

Maduración de las tecnologías de virtualización: Esto ha permitido a la Cloud computing a la asignación de recursos y que los servicios son eficientes, dinámicos. Esta propuesta se ha desarrollado más de 50 años. Pero gracias a la virtualización, su acceso y uso son accesibles.

Obstáculos

Algunos de los obstáculos identificados con la dificultad la implementación del Cloud Computing²⁹:

Percepción de la seguridad: Una de las preocupaciones es el tema de la seguridad. Ya que existen desconocimiento sobre los parámetros que superan los centros de datos. Ya que en cualquier lugar pueden tener acceso a información. Por esa razón se deben seguir los lineamientos de las prácticas de seguridad para protegerlos 24/7. Con su encriptación de los datos de los usuarios que tenga acceso.

Restricciones de Internet: El tráfico del internet puede ocasionar retrasos o pérdida de información debido a los nodos por donde pasan.

Pérdida de Control: Debido a la previa pérdida de información, pues no se tiene accesos a los servidores físicamente, dejando a la responsabilidad de su almacenamiento y su control a manos del proveedor del servicio.

5.2 MARCO CONCEPTUAL

Computación en la nube es un modelo de acceso a la red desde cualquier parte del mundo. Permitiendo compartir recursos informáticos, fácil de acceso, su configuración puede ser provisional e interacción con los proveedores de servicios.³⁰

²⁹ SULLIVAN, F. (2009). GUEST EDITOR'S INTRODUCTION: CLOUD COMPUTING FOR THE SCIENCES. (EN LINEA). (I. C. SOCIETY., ED.) *COMPUTING IN SCIENCE AND ENGINEERING*, 11 (4), 10-11. <http://www.savvis.net/en-US/Pages/Home.aspx>.

³⁰ ORIOL FITO Y JORDI GUITART. (2015). *INTRODUCING RISK MANAGEMENT INTO CLOUD COMPUTING (EN LINEA)*.

Este método de la computación en la nube y el almacenamiento brinda información y funcionalidades en línea. Sin embargo, algunos servidores en la nube se dirigen en aplicar servicios y funcionalidades de compras, redes sociales, protección de documentos digitales etc. De igual forma está enfocado para negocios o empresas pequeñas, grandes e instituciones³¹.

Uno de los propósitos de la nube son las herramientas de software, que también son importantes para la creación de servicios y soluciones, e incluyen API, middleware, bases de datos, aplicaciones, un supervisor para crear máquinas virtuales (VM) e infraestructura de escritorio virtual (VDI), así como software de pila en la nube como OpenStack y herramientas de administración relacionadas.

Ejemplos de hipervisores VMs y VDI incluyen Citrix/Xen, KVM, Microsoft Hyper-V, Oracle, VMware ESX/vSphere y PROMOX que permite crear una infraestructura completa de virtualización³²

La Cloud es una herramienta de software donde se pueden crear servicios, concretar soluciones incluyendo APIS, también base de datos, hipervisores para la creación de máquinas virtuales y aplicaciones.

En la actualidad se encuentra una lista de proveedores de servicios públicos y servicios Cloud debido al crecimiento constante. Debido a los servicios especializados de la red. Se dará a conocer algunos proveedores de la nube computacional:

Amazon EC2: Es un servicio web que provee capacidades de cómputo elásticas, su infraestructura cloud diseñada con la finalidad de proveer computación para entornos web, con un modelo comercial de pago por uso.³³

Google: Google App Engine es una plataforma para la creación y alojamiento de aplicaciones web.³⁴

Salesforce.com: Es un proveedor de Customer Relationship Management (CRM), ofrecen software como servicio, incluyendo aplicaciones a la venta, soporte y servicios.

Force.com: Permite a los desarrolladores externos crear aplicaciones adicionales que les permita integrar en las aplicaciones de CRM.

³¹ AZEEM KHALIL KHREISHAH. (2014). CLOUD COMPUTING SECURITY: A SURVEY COMPUTERS (EN LINEA).L

³² (CHOW GOLLE & MOLINA, 2009). CONTROLLING IN THE DATA CLOUD.

³³ AMAZON WEB SERVICES. (2019). AMAZON SIMPLE QUEUE SERVICE (AMAZON SQS) (EN LINEA). Obtenido de [HTTP://AWS.AMAZON.COM/SQS/](http://AWS.AMAZON.COM/SQS/)

³⁴ GOOGLE. (209). GOOGLE APP ENGINE (EN LINEA). Obtenido de [HTTP://CODE.GOOGLE.COM/](http://CODE.GOOGLE.COM/)

Microsoft: Servicios Azure, permite alojar en centro de datos de Microsoft, ofreciendo servicios de sistemas operativos y pueden usar servicios individualmente o de conjunto.³⁵

5.3 MARCO HISTÓRICO

En el transcurso del tiempo se ha recorrido un largo camino desde que se empezó el concepto de la computación en la nube por parte de algunos investigadores. Inicialmente ese concepto llega a finales del siglo XX, remontando el concepto de J.CR.LICKLIDER Y JHON McCARTHY.³⁶

El término de la nube se mostraba por medio de dibujos para simbolizar la red telefónica y luego de ellos representaban por medio de diagramas la red de los equipos. Esto ha sido una evolución para generalizar la virtualización, está orientada en los servicios y utilidad del equipo.

El concepto básico que atribuye John McCarthy es del término “Inteligencia Artificial”. Fue uno de los primeros en compartir el concepto de la tecnología de tiempo compartido de computadoras. Por ejemplo, alquilar tiempo y servicios de cómputo, proporcionando un ambiente operacional.

Luego el concepto de una red conectada por una computadora para el acceso o comunicación de varios usuarios fue formulado por J.C.R. Licklider de Bolt, Beranek and Newman en agosto 1962.³⁷

En los años 90, se empezó el ancho de banda para soportar la computación en la nube. Desde ese momento se empezaron los primeros intentos para el diseño de esa tecnología. En 1996 se usó Ejecutivos de Compaq Computer por primera vez se usa el término.

En el 2002, lanzan Amazon Web Services, un sistema de almacenamiento en la nube permitiendo la ejecución de todo tipo de aplicaciones e información dentro de la nube.³⁸ Luego de un tiempo, se empieza a ofrecer servicios a pequeñas y medianas empresas del alquiler de servidores, mejorando la capacidad del procesamiento e invirtiendo en

³⁵MICROSOFT. (209). *MICROSFT SQL AZURE DATABASE (EN LINEA)*. Obtenido de [HTTP://WWW.MICROSOFT.COM/WINDOWSAZURE/SQLAZURE/](http://www.microsoft.com/windowsazure/sqlazure/)

³⁶ GARFINKEL ROSENBLUM. (2013). *VIRTUAL MACHINE INTROSPECTION BASED ARCHITECTURE FOR INTRUSION DETECTION*.(EN LINEA).

³⁷ BUITRAGO, Y., & SILVA, D. (2009). *HACIA UNA ONTOLOGÍA UNIFICADA DE LA COMPUTACIÓN EN LA NUBE*.(EN LINEA).

³⁸ MELL GRANCE. (2011). *THE NIST DEFINITION OF CLOUD COMPUTING RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY*.(EN LINEA).

avances tecnológicos. Con el paso llegaron sistemas a unirse al mundo de la nube para empezar a construir un presente. Como Google, Gmail y iCloud. Todas se caracterizan por ser computación en la nube.

5.4 ANTECEDENTES O ESTADO ACTUAL

Anteriormente la demanda era baja por los recursos de cómputo configurables, por ejemplo, están las redes, los servidores, el almacenamiento, aplicaciones y servicios configurados. Siendo esto herramientas de fácil disposición para el cliente siendo un mínimo esfuerzo y de interacción con el proveedor del servicio. Además, sus diferentes tipos de nube, como el público, privado, híbrido y comunitario.³⁹

Las nubes que consumen servicios muestran los esquemas cifrados asegurando que los datos que se almacenan estén protegidos de acceso no permitidos, su copia de seguridad es programada y segura siendo un medio de respaldo.⁴⁰

También se conocen otras definiciones sobre la nube computacional, la cual es capacitado de proporcionar infraestructuras flexibles adquiriendo modelos de implementación en servicios SaaS, permitiendo usar dos tipos de servidores en el cual uno es principal y el otro es de dominio.⁴¹

La nube multiinquilino es un modelo de amenaza informática que desafía la seguridad, debido que los datos confidenciales, la seguridad del cliente. Actualmente, enfrenta algunas fuentes principales como amenaza de la infraestructura virtualizada del servicio que explotan vulnerabilidades grande y complejo, son ataques sigilosos de datos confidenciales operados en la nube.⁴²

Bloqueo de cuentas por denegación de servicio: una verificación de seguridad de uso común, especialmente la autenticación de nombre de usuario/contraseña, es bloquear las cuentas que han recibido múltiples intentos fallidos de autenticación.

Mecanismo de restablecimiento de credenciales débiles: cuando los proveedores de la nube administran las credenciales de los usuarios por sí mismos en lugar de utilizar la autenticación asociada, deben proporcionar un mecanismo de restablecimiento de las credenciales de los usuarios en caso de olvido o pérdida de datos. En el pasado, los mecanismos de recuperación de contraseñas han demostrado ser particularmente débiles.

³⁹ JENSEN SCHWENK, GRUSCHKA IACONO. (2010). ON TECHNICAL SECURITY ISSUES IN CLOUD COMPUTING (EN LINEA).

⁴⁰ ALCALDIA MAYOR DE BOGOTÁ. (2009). LEY 1341 DE 2009 (EN LINEA).

⁴¹ NORMA ISO 27001(SEGURIDAD DE LA INFORMACIÓN),ISO 31000(RIESGO),9001(CALIDAD),ISO 27018(PROTECCIÓN INFORMACIÓN PERSONAL NUBE)(EN LINEA). (s.f.).

⁴² NORMA ISO 27001(SEGURIDAD DE LA INFORMACIÓN),ISO 31000(RIESGO),9001(CALIDAD),ISO 27018(PROTECCIÓN INFORMACIÓN PERSONAL NUBE)

Verificaciones de autorización insuficiente o defectuosa: Las ofertas de servicios web y aplicaciones web son vulnerables porque muchos de ellos su verificación de autorización son insuficientes o defectuosas que pueden poner a disposición de los usuarios información o acciones no autorizadas. Las comprobaciones de autorización faltantes, por ejemplo, son la causa raíz de los ataques de adivinación de URL. En tales ataques, los usuarios modifican las direcciones URL para mostrar información de otras cuentas de usuario.

Control de autorizaciones basto: Las interfaces de administración de servicios en la nube son especialmente susceptibles de proporcionar modelos de prueba de autorización demasiado crudos. Como resultado, las medidas de seguridad estándar, como la segregación de tareas, no se pueden realizar porque no es posible otorgar a los usuarios solo los privilegios que necesitan para realizar su trabajo.

Vulnerabilidades de Inyección: Ejemplos claros, es la inyección de SQL, donde la entrada contiene código de SQL que se ejecuta erróneamente en el black-end de la base de datos. La inyección de comandos, los scripts entre sitios web donde tienen acceso al código por el navegador de la víctima.

Vulnerabilidades de Autenticación: Comportamiento inseguro del usuario, como elegir contraseñas débiles, reutilizar contraseñas, etc. Cuando la autenticación de factor cruzado es limitada.

Vulnerabilidad en la recuperación de datos: Las características de las nubes implica recursos asignados para un usuario. Ahí es donde entra la memoria de almacenamiento (El cache), generando recuperar datos escritos por el usuario anterior.

5.4.1 Ranking de amenazas

La seguridad para todos los negocios, se enfrentan a riesgos como le denegación de servicio, el malware, la inyección SQL, la pérdida de datos, entre otros.

Muchos proveedores de nubes introducen el acceso a recursos de seguridad con respecto a herramientas altamente sofisticados para no tener acceso. Así que, estos son algunos riesgos de seguridad de la computación en nube.

5.4.1.1 Pérdida de visibilidad

La mayoría de las empresas accederán a servicios de nube, por medio de dispositivos, departamentos y geografías. Sin las herramientas apropiadas en su lugar, puede causar la pérdida de visibilidad del acceso a su infraestructura. Ya que, si no se puede ver, no puede protegerlo. Ocasionando riesgo de violación y pérdida de datos.

5.4.1.2 Violación de Incumplimiento

Con el control reglamentario, es necesario cumplir con una serie de requisitos estrictos, para no entrar al riesgo de violación de cumplimiento si no se tiene cuidado. Por ejemplo, Una transferencia descuidada de datos a la nube, o el traslado al proveedor equivocado, puede poner a su empresa en el estado de incumplimiento, generando repercusiones legales y financieras.

5.4.1.3 Falta de Estrategia y Arquitectura de Cloud Security

En su prisa por migrar los sistemas y datos a la nube, muchas empresas empiezan a funcionar sin antes de la estrategia de seguridad esté en funcionamiento para proteger su infraestructura.

5.4.1.4 Amenazas internas

No tiene por qué tener un propósito malicioso para causar daños a su negocio. De hecho, pasa esos incidentes internos por la falta de información o a la negligencia.

5.4.1.5 Interfaz de Usuarios de Aplicaciones Inseguras (API)

Se debe tener en cuenta que cualquier API incorporada a sus aplicaciones web o móviles pueden accederse tanto interno por parte de la persona lo externo por parte de los consumidores. Generando una puerta de entrada que ofrece acceso no autorizado a los ciberdelincuentes buscando robar datos y manipular servicios.

5.4.1.6 Desconfiguración de los Servicios de la Nube

La configuración errónea de los servicios en la nube puede ocasionar la manipulación de datos o incluso la eliminación de ellos.

5.4.1.7 Denegación de servicios (DoS)

Están diseñados para evitar que los usuarios de un servicio puedan acceder a sus datos o aplicaciones. El proveedor de DNS Dyn es un ejemplo clave de un ataque DoS. Siendo que un grupo externo se apoderó de los dispositivos IoT para lanzar la denegación de servicios distribuida, usando el malware Mirai.

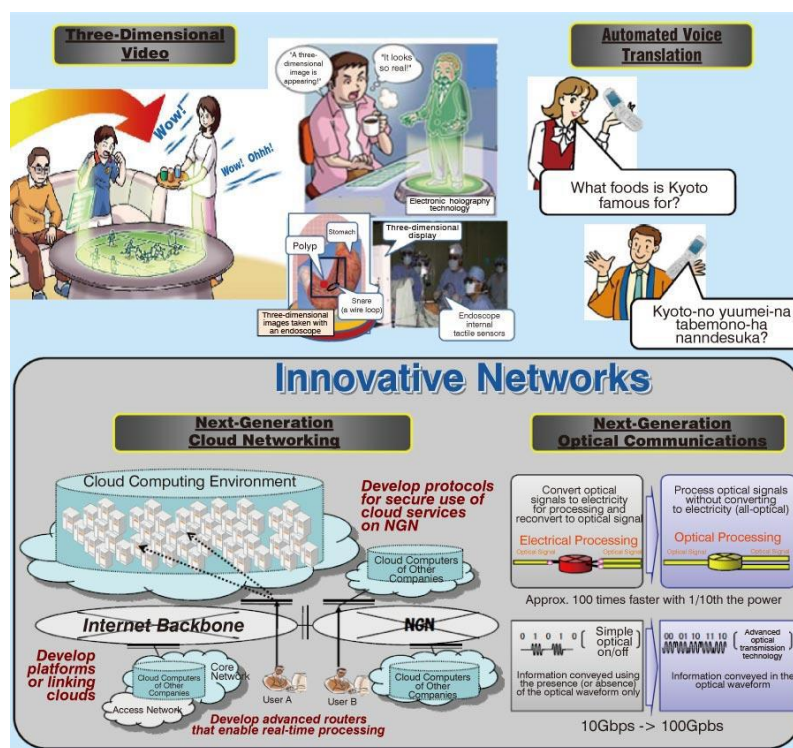
5.4.2 Clientes y casos de éxito.

Japón

En Japón los tics tienen un crecimiento del 40% en economía de la nación, en este mercado en la actualidad tiene inversiones de cerca de mil millones de dólares. El

Ministerio de Asuntos internos y Comunicaciones (MIC), crearon un proyecto sobre el plan ICT Hatoyama (Digital Japan Creation Project (ICT Hatoyama Plan): Outline, 2009), con el fin de crear nuevos mercados TIC, para la generación de nuevos empleos, en este proyecto se cuenta con nuevos temas como la generación de tecnologías Cloud.

Ilustración 1 Nuevas tecnologías en Japón



Fuente: Ministerio de Asuntos internos y comunicaciones del Japón

Los sistemas de información de este gobierno indica que las tecnológicas innovaran para las tecnologías Cloud. Siendo esto que para el 2018 este en una etapa madura con el desarrollo de la Nube Kasumigaseki (Lo bautizaron provisional), esto es para dar tiempo a la integración y conciliación de las plataformas.

Su manera de hacer que la Cloud tenga funcionalidad de Archivos Nacional Digital, en ella se almacenara documentos oficiales, libros, sus bienes culturales, sus datos estadísticos. Para la estandarización de los formatos para el acceso al público.

Reino Unido

Durante el año 2017, Ofcom ⁴³ realizó un estudio sobre la identificación sobre las áreas para el desarrollo y el impacto de aplicaciones con las nuevas tecnologías. En el estudio que realizaron incluyeron las siguientes revisiones:

Para determinar las necesidades no satisfechas, se realiza la revisión de las posibles tecnologías que se encuentran disponible en a actualidad. En la accesibilidad de las comunicaciones se realiza la revisión de las recientes aplicaciones con respecto a los avances tecnológicos para tener una mejora de ella misma.

A partir de ese estudio, se hacen dos recomendaciones para seguir y llevar las regulaciones:

La realización de proyectos, que logren la voz IP (VOIP) para usuarios con deficiencia auditiva para mayor facilidad de su uso. La implementación de servicios de entretenimiento, WebTV, los servicios de radio y su tecnología Cloud.

Caso de Éxito

Algunos casos sobre la implementación del uso Cloud Computing:

Caso New York Times

Como lo detalla⁴⁴, “el periódico The New York Times genera la necesidad de convertir 11 millones de artículos e imágenes desde su archivo en un formato PDF. El departamento TIC hizo un promedio y decían que se demoraban entre cinco a siete semanas. Mientras un desarrollador una de las instancias de Amazon EC2 como interface para el servicio web que operaba Hadoop donde se completó el trabajo en 24 horas”.

Caso Animoto Productions

⁴³ ASSISTIVE TECHNOLOGIES IN COMMUNICATIONS: (EN LINEA) UNMET NEEDS, NEW TECHNOLOGIES AND ONGOING RESEARCH AND DEVELOPMENT PROGRAMMES, 2008)

⁴⁴ GARTNER, INC. (26 DE JUNIO DE 2008). *GARTNER SAYS CLOUD COMPUTING WILL BE AS INFLUENTIAL AS E-BUSINESS*. (EN LINEA). 20 DE OCTUBRE DE 2009, DE [HTTP://WWW.GARTNER.COM/IT/PAGE.JSP?ID=707508](http://www.gartner.com/it/page.jsp?id=707508)

En este caso fueron los creadores de mash-up para la creación de videos a partir de imágenes y música. Utilizando como herramienta los servicios Cloud Computing de Amazon. Escalando en tan solo tres días para la utilización de los servidores. Siendo uno de los casos de éxito más importante de los servicios web de Amazon, por ser unas de las instancias más activas.

Caso SmugMug

Como se detalla en ⁴⁵, a principio de 2010 la compañía SmugMug inicio una investigación para la solución de su almacenamiento de información, para un nuevo repositorio de mil millones de imágenes. Luego de una semana cuando se inicio la utilización de los servicios de Amazon Simple Storage Service, los clientes han añadido hasta 10 terabytes de imágenes nuevas cada mes. Esto ha generado un ahorro de 500.000 dólares en gastos de almacenamiento.

Caso Linden Lab

En este caso utilizaron Amazon Simple Storage Service para almacenar la mayoría de los elementos usados. Tras el lanzamiento de Amazon CloudFront, el cual Linden Lab migro la parte de descargar para que se pueda generar hasta 40 mil veces cada día por usuario en todo el mundo, en cualquier lugar del mundo.

Caso Jungle Disk

Jungle cuenta con un sistema de almacenamiento en línea simple, siendo confiable y asequible para el servicio de la realización de copias de seguridad usando Amazon Simple Storage Service.

5.5 MARCO LEGAL

Según Borenstein and J.Blake ⁴⁶ Explica que los modelos para esta nueva tecnología deben manejar un estándar prescriptivo y uno evaluativos. Los estándares representan la calidad de los sistemas de Cloud Computing, siendo los encargados de evaluar los procedimientos en general, según la norma ISO 9000 y para procedimientos específicos, siendo la norma ISO 27000 especifica la seguridad de la información, siendo uno de los mecanismos que busca al proveedor de estos servicios que puedan medir las características como el tiempo de actividad, la disponibilidad, el cumplimiento y servicio al cliente.⁴⁷

⁴⁵ AMAZON WEB SERVICES, LLC. (S.F.). *AMAZON ELASTIC COMPUTE CLOUD (AMAZON EC2)*. (EN LINEA). 20 DE OCTUBRE DE 2014, DE [HTTP://AWS.AMAZON.COM/EC2/](http://aws.amazon.com/ec2/)

⁴⁶ ORIOL FITO Y JORDI GUITART. (2015). *INTRODUCING RISK MANAGEMENT INTO CLOUD COMPUTING* (EN LINEA).

⁴⁷ AZEEM KHALIL KHREISHAH. (2014). *CLOUD COMPUTING SECURITY: A SURVEY COMPUTERS* (EN LINEA).

La normatividad de Colombia se opera en un contexto de servicios para su infraestructura de computación en la nube, existiendo leyes, normas y otros recursos. Contribuyendo al progreso de esta tendencia tecnológica.

El Gobierno Nacional de Colombia han preparado para que cumplan con los estándares de los proveedores de los servicios⁴⁸:

- La ley 1273 de 2009, “La protección de la información y de los datos, en busca de preservar la integridad de los sistemas que utilicen las tecnologías de la información. La finalidad de esta ley es proteger los sistemas de información de violaciones en la confidencialidad, integridad y disponibilidad de información”.⁴⁹
- Ley 1221 de 2008, Esta ley define sus diferentes formas y constituye políticas públicas para promover actividades, ofreciendo garantías laborales, seguridad al personal para el desarrollo de actividades.⁵⁰
- El plan Nacional de TIC fue tomado como la estrategia del Gobierno Nacional, están orientados a contribuir y fortalecer las políticas de la inclusión para acciones y proyectos descritos ⁵¹.
- Ley 1341 de 2009, Se define conceptos sobre la información y las organizaciones de la información y comunicaciones (TIC), su principio es proteger los derechos de los usuarios, calidad de servicios y derecho de la comunicación.⁵²
- ISO 27018, Es de buenas prácticas, “siendo controles de protección de datos en los servicios de computación en la nube”⁵³. Esta norma se complementa de la iso 27001 e iso 27002 para el ámbito de la seguridad de la información, especificados a los proveedores de los servicios de la nube⁵⁴.

⁴⁸ GARFINKEL ROSENBLUM. (2013). VIRTUAL MACHINE INTROSPECTION BASED ARCHITECTURE FOR INTRUSION DETECTION.(EN LINEA).

⁴⁹ BUITRAGO, Y., & SILVA, D. (2009). HACIA UNA ONTOLOGÍA UNIFICADA DE LA COMPUTACIÓN EN LA NUBE.(EN LINEA).

⁵⁰ MELL GRANCE. (2011). THE NIST DEFINITION OF CLOUD COMPUTING RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.(EN LINEA).

⁵¹ JENSEN SCHWENK, GRUSCHKA IACONO. (2010). ON TECHNICAL SECURITY ISSUES IN CLOUD COMPUTING (EN LINEA).

⁵² ALCALDIA MAYOR DE BOGOTÁ. (2009). LEY 1341 DE 2009 (EN LINEA).

⁵³ NORMA ISO 27001(SEGURIDAD DE LA INFORMACIÓN),ISO 31000(RIESGO),9001(CALIDAD),ISO 27018(PROTECCIÓN INFORMACIÓN PERSONAL NUBE)(EN LINEA). (s.f.).

⁵⁴ (NORMA ISO 27001(SEGURIDAD DE LA INFORMACIÓN),ISO 31000(RIESGO),9001(RIESGOS),ISO 27018(PROTECCIÓN INFORMACIÓN PERSONAL NUBE))

6 DESARROLLO DE LOS OBJETIVOS

6.1 AMENAZAS CIBERNÉTICAS QUE ENFRENTAN LOS SERVICIOS DE ALMACENAMIENTO DE NUBES PÚBLICAS.

De acuerdo con la revisión documental se puede evidenciar que las principales amenazas según UpGuard⁵⁵ son las siguientes:

- **Malware**

Malware (software malicioso) se refiere a cualquier software intrusivo desarrollado por ciberdelincuentes para robar datos y dañar o destruir computadoras y sistemas informáticos. Ejemplos de malware común incluyen virus, gusanos, virus troyanos, spyware, adware y ransomware.

El malware puede revelarse con muchos comportamientos en el sistema, entre ellos encontramos tenemos lo siguientes:

- El rendimiento de la computadora se ralentiza.
- La pantalla está desbordada de anuncios aleatorios
- Es notable la perdida de espacio en el disco
- Se altera la actividad del internet en el sistema
- Las configuraciones del navegador cambian
- El antivirus deja de funcionar
- Se pierde el acceso a los archivos o toda la computadora

- **Spyware**

Es un software malicioso o malware programado para exhibir o robar información confidencial o dañar dispositivos informáticos. Se considera Spyware a cualquier software descargado en el dispositivo de un usuario sin su respectiva autorización.

La forma en la que funciona un Spyware es ejecutándose en un segundo plano, ocasionando actividades de CPU no deseadas, aceleración del disco duro, conexiones de internet alteradas, bloqueo de aplicaciones y fallas en todo el sistema, usualmente los usuarios asumen los problemas de rendimiento del dispositivo como software defectuoso (virus) o desactualizado, sin darse cuenta de que realmente se trata de un

⁵⁵ UpGuard. (s.f.). *The new standard in third-party risk and attack surface management [En línea]*.
Obtenido de Disponible en: <https://www.upguard.com/>

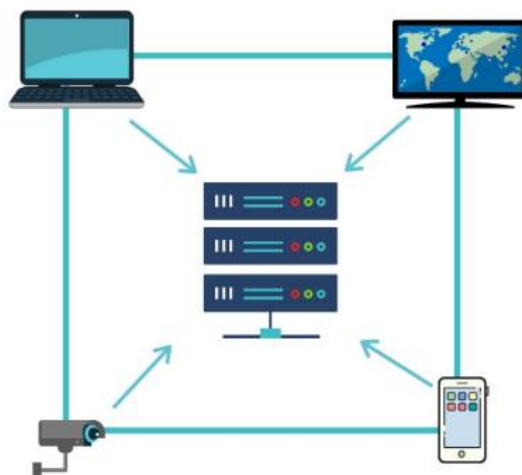
software espía. La forma más agresiva de este software malicioso es capaz de restablecer páginas de inicio del navegador, redirigir búsquedas web, abrir anuncios emergentes y afectar la seguridad del navegador.

- **Distributed Denial of Service (DDoS) Attacks**

El ataque de denegación de servicio distribuido (ataque DDoS) es el proceso en la cual los ciber atacantes envían solicitudes de datos a un servidor web de forma masiva, con el propósito de impedir su rendimiento. Esta alteración podría provocar que el servidor web se ralentizara o en el peor de los casos que colapsara por completo.

El ataque DDoS es coordinado entre varios dispositivos (IoT) y computadoras. Estos dispositivos son infectados con malware por los ciberdelincuentes con anterioridad y así tener el control y poder realizar el ataque, entre más unidades infectadas (bots) reclute un atacante, más peligroso será el ataque y si estos bots tienen una vinculación entre sí, la red se conoce como botnet.

Ilustración 2 Ataque DDoS



Fuente: <https://www.upguard.com/blog/is-ddosing-illegal>

En un ataque DDoS, cada bot envía de forma constante peticiones a la dirección IP del host, esto obliga que el servidor web denegué la entrada o el servicio a los usuarios que visitan el sitio web.

- **Ransomware**

Es un tipo de software malicioso o malware diseñado para robar y cifrar archivos, datos confidenciales o información de identificación personal (PII) para evitar que las víctimas accedan a esos archivos hasta que se pague una tarifa o rescate. Los atacantes de ransomware utilizan tácticas de extorsión para obligar a las víctimas a realizar pagos de rescate y, por lo general, se dirigen a personas con prácticas de seguridad deficientes o vulnerabilidades sin parches. Una vez que los piratas informáticos obtienen acceso a una red, pueden inyectar software malicioso que contiene la carga útil del ransomware en la computadora o el dispositivo móvil de la víctima.

Sin una clave de descifrado, es casi imposible recuperar archivos que se han cifrado con ransomware. Las infecciones de ransomware pueden ser especialmente devastadoras para las empresas que dependen de datos cifrados para mantener sus operaciones diarias. Si el rescate no se paga en un tiempo específico, los archivos pueden perderse permanentemente o incluso exponerse al público.

Hoy en día, muchos ciberdelincuentes exigirán criptomonedas como Bitcoin como pago de rescate, un sistema de pago descentralizado conocido por su capacidad para ocultar actividades financieras. Aunque rastrear los pagos de rescate en la cadena de bloques de criptomonedas es difícil, ciertamente no es imposible.

para denegar el acceso a un sistema informático o datos hasta que se pague el rescate el ransomware se propaga a través de correos electrónicos de phishing, publicidad maliciosa, visitando sitios web infectados o explotando vulnerabilidades.

- **Zero-Day-Exploits**

Un día cero (día 0) es una vulnerabilidad de seguridad sin parches que es desconocida para el desarrollador de software, hardware o firmware, y los atacantes aprovechan la vulnerabilidad para aprovechar el agujero de seguridad.

En general, el día cero se refiere a dos cosas:

Vulnerabilidades de día cero: un agujero de seguridad, como uno en un sistema operativo, que es desconocido para su desarrollador y software antivirus.

Exploits de día cero: un ataque cibernético que aprovecha una vulnerabilidad de día cero. Los exploits de día cero se pueden usar para instalar diferentes tipos de malware, robar datos confidenciales o números de tarjetas de crédito y provocar filtraciones de datos.

El día cero recibe su nombre del número de días que ha existido un parche para la falla: cero.

Las amenazas de día cero representan un riesgo significativo para la seguridad cibernética porque son desconocidas para la parte responsable de reparar la falla y es posible que ya estén siendo explotadas.

Por ejemplo, BlueKeep (CVE-2019-0708) es una falla de ejecución remota de código que afecta aproximadamente a un millón de sistemas (al 29 de mayo de 2019) que ejecutan versiones anteriores de los sistemas operativos de Microsoft.

Esta vulnerabilidad de día cero apareció en los titulares durante el martes de parches de mayo de 2019 de Microsoft debido a su capacidad de gusano.

- **Advanced Persistent Threats**

Una amenaza persistente avanzada (APT) es una campaña de ciberataque en la que un actor de amenazas establece una presencia a largo plazo dentro de una red violada para robar continuamente datos confidenciales.

Para evadir la detección durante todo el ciclo de vida del ataque APT (que podría durar muchos años), estas amenazas cibernéticas siempre deben superar la sofisticación en evolución de los controles de seguridad comunes.

Los métodos de ataque avanzados de los grupos APT hacen que esta amenaza cibernética sea significativamente más difícil de interceptar.

Las amenazas persistentes avanzadas son sofisticadas porque están bien financiadas y generalmente coordinadas por algunos de los piratas informáticos más avanzados en el ámbito digital: los ciberdelincuentes del estado-nación.

Para garantizar un retorno sustancial de las inversiones superiores en recursos y experiencia requeridas para lanzar ataques APT, los grupos APT no perderán el tiempo enfocándose en víctimas de bajo valor. Su punto de mira se fija en las entidades que alojan la información confidencial más valiosa o los objetivos que causarán el mayor perjuicio a un adversario cuando se vean comprometidos.

Éstos incluyen:

- Infraestructuras críticas
- Entidades financieras
- Bufetes de abogados
- Grandes organizaciones

Los grupos APT están a la caza de los siguientes tipos de datos:

- Información interna confidencial (credenciales de empleados, información de identificación personal del cliente)
- Propiedad Intelectual (Planes comerciales, patentes, planes de marketing, desarrollo de productos).
- Credenciales privilegiadas

La preferencia de las grandes empresas no significa que las organizaciones más pequeñas no corran el riesgo de sufrir un ataque APT.

- **Trojans**

Es un tipo de malware que generalmente se oculta como un archivo adjunto en un correo electrónico o un archivo de descarga gratuita y luego se transfiere al dispositivo del usuario. Una vez descargado, el código malicioso ejecutará la tarea para la que el atacante lo diseñó, como obtener acceso de puerta trasera a los sistemas corporativos, espiar la actividad en línea de los usuarios o robar datos confidenciales.

A diferencia de los virus informáticos, un caballo de Troya no puede manifestarse por sí mismo, por lo que necesita que el usuario descargue la aplicación del lado del servidor para que funcione. Esto significa que se debe implementar el archivo ejecutable (.exe) y el programa instalado para que el troyano ataque el sistema de un dispositivo.

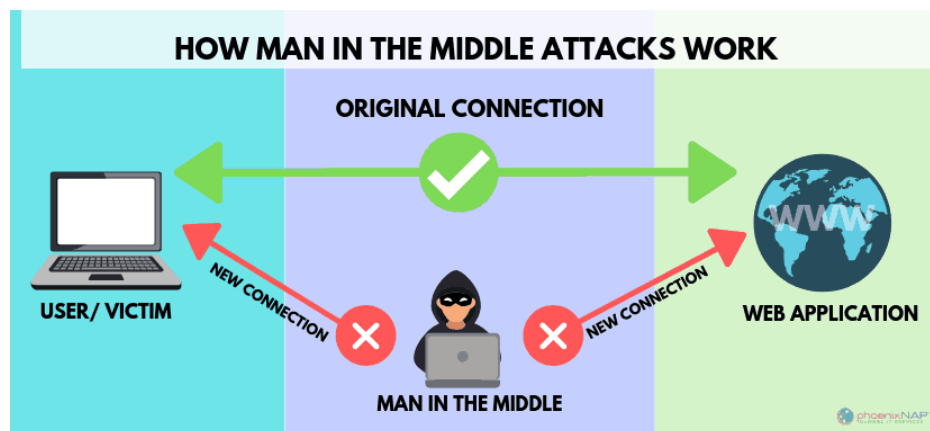
Un virus troyano se propaga a través de correos electrónicos que parecen legítimos y archivos adjuntos a correos electrónicos, que se envían como spam para llegar a las bandejas de entrada de tantas personas como sea posible. Cuando se abre el correo electrónico y se descarga el archivo adjunto malicioso, el servidor troyano se instalará y se ejecutará automáticamente cada vez que se encienda el dispositivo infectado. Los dispositivos también pueden ser infectados por un troyano a través de tácticas de ingeniería social, que los ciberdelincuentes utilizan para obligar a los usuarios a descargar una aplicación maliciosa. El archivo malicioso podría estar oculto en anuncios publicitarios, anuncios emergentes o enlaces en sitios web.

- **Man-in-the-Middle Attack (MITM Attack)**

Un ataque man-in-the-middle (ataque MITM) es un ataque cibernético en el que un atacante transmite y puede interrumpir la comunicación entre dos partes que creen que se están comunicando directamente. Esto permite que un atacante transmita comunicaciones, escuche a escondidas e incluso modifique lo que dice cada parte.

Los ataques Man-in-the-middle permiten la escucha entre personas, clientes y servidores. Esto puede incluir conexiones HTTPS a sitios web, otras conexiones SSL/TLS, conexiones de redes Wi-Fi y más.

Ilustración 3 Ataque Man in the Middle



Fuente: <https://wallstreetinv.com/cyber-security/man-in-the-middle-attack-mitm/>

6.1.1 AMENAZAS Y RIESGOS CONTRA LOS SERVICIOS EN LA NUBE

Las organizaciones que tienen pensado usar los servicios en la nube no están completamente informadas de los riesgos involucrados que se exponen al implementar estos servicios, tales como riesgos comerciales, financieros, técnicos, legales y de cumplimiento. Sin embargo, se deben considerar los siguientes 5 riesgos de seguridad primordiales:

- Visibilidad limitada de las operaciones y almacenamiento de los datos en la red
- Exposición a ataques cibernéticos como el malware
- Pocos controles de acceso a los usuarios de la organización para el ingreso a la nube
- Pérdida de datos a manos de terceros fuera de la organización debido al poco monitoreo de la nube.

- Mala diligencia al momento de pasar los servicios a la nube

Por otra parte, encontramos las diferentes amenazas o riesgos que pueden obtener los servicios de nube pública, en las cuales encontramos SaaS, Las y PaaS. Teniendo en cuenta que las posibles amenazas que pueden obtener estos servicios comienzan desde su propia configuración inicial. Por tal razón, las empresas que ofrecen este tipo de servicios tienen una gran responsabilidad al momento de configurar adecuadamente cada servicio, dependiendo los requerimientos del cliente.

Dentro del servicio de nube publica PaaS encontramos las posibles amenazas:

- Configuraciones de aplicaciones predeterminadas:

Al momento de ejecutar una aplicación en una infraestructura en la nube, las probabilidades de que la configuración con respecto a la seguridad sea segura son muy pocas, ya que se debe configurar la aplicación a medida que la aplicación la vaya requiriendo y no realizar una instalación por defecto. Entre las configuraciones a tener en cuenta se encuentra el entorno de Windows (Internet Information Services IIS) configuración LAMP si se trata de un entorno basado en Linux, Apache o MySQL, configuración en el protocolo ligero de acceso a directorios (LDAP), protocolo siempre de administración de redes (SNMP) y nombre de usuarios y contraseñas predeterminadas para la gestión de aplicaciones.⁵⁶

- Defectos de implementación y protocolo SSL:

Es una de las amenazas más probables en cuanto a navegar por internet se refiere y si es por medio de un servicio PaaS, se debe tener mayor cuidado, pero esta protección lo debe garantizar el proveedor del servicio, dado que existen varias técnicas para falsificar un certificado SSL y un ataque conocido como man-in-the-middle (MITM).

- Permisos inseguros sobre datos en la nube:

Los usuarios que adquieran este servicio deben verificar los permisos adecuados para el almacenamiento de datos en la nube, ya que puede existir fugas de información debido a que los permisos subyacentes de los datos no se establecieron o configuraron correctamente.

⁵⁶ Cox, P. (s.f.). *Krypton SOLID*. Obtenido de Principales amenazas en un servicio en la nube PaaS y cómo evitarlas [En línea]: Disponible en: <https://kryptonsolid.com/principales-amenazas-en-un-servicio-en-la-nube-paas-y-como-evitarlas/#:~:text=Seg%C3%BAAn%20mi%20experiencia%2C%20estas%20son%20las%20amenazas%20m%C3%A1s,3%20Permisos%20inseguros%20sobre%20datos%20en%20la%20nube>

Posibles amenazas encontradas en la nube pública SaaS:

Los riesgos que invaden el servicio SaaS son difíciles de detener e identificar, ya que es imperceptible a nivel de usuario, dado a que los archivos y datos se sincronizan automáticamente en todos los dispositivos vinculados, lo que conlleva a tener un canal viable por el cual el malware se puede propagar. Dentro de las amenazas más comunes encontramos las siguientes:⁵⁷

- Phishing
- Robo de credenciales
- Malware oculto y amenazas zero-day
- Amenazas internas

El último servicio de nube pública es IaaS, el cual está siendo demandado por las compañías debido a su escalabilidad, flexibilidad y su rápida adaptación de crecimiento en los servicios ofrecidos por el proveedor. No obstante IaaS contiene diferentes amenazas cibernéticas, en las cuales encontramos:⁵⁸

- Denegación de servicios (DoS)
- Fuga de datos / pérdida de datos (DLL)
- Abuso de servicios de cloud (Ab CS)
- Insider / errores humanos (Insid)
- Suplantación
- Aplicaciones inseguras (APIS)

⁵⁷ CSO COMPUTERWORLD. (29 de Enero de 2020). *Los riesgos más trascendentes de los entornos SaaS [En línea]*. Obtenido de Disponible en: <https://cso.computerworld.es/tendencias/los-riesgos-mas-trascendentes-de-los-entornos-saas>

⁵⁸ OWASP. (Marzo de 2013). *Cloud Security en IaaS Una visión de Seguridad desde el Data Center [En línea]*. Obtenido de Disponible en: https://owasp.org/www-pdf-archive/3-Cloud_Security_IaaS.pdf

6.1.2 AMENAZAS Y RIESGOS PARA LOS SERVIDORES

Las amenazas y riesgos de seguridad usuales van desde amenazas internas hasta amenazas constantes mejoradas, las cuales pueden poner en una posición difícil a una organización, a menos que su módulo de seguridad interno esté al tanto de ellas y esté preparado para responder. La seguridad del servidor depende de muchos factores, incluido el sistema operativo y el propósito, entre ellas están:⁵⁹

- Administración del servidor a una persona no muy capacitada
- Poca seguridad física en el lugar del servidor
- Dejar que cualquier empleado tenga acceso al servidor
- Tener desactualizado el software del servidor y de la aplicación
- Activar funciones que no son necesarias en el servidor

6.1.3 AMENAZAS Y RIESGOS CONTRA LOS USUARIOS

- **Phishing**

Es un ataque informático que colecciona información privada como contraseñas, número de tarjetas de crédito, número de cuenta bancaria, a través de una página ilegítima o correo, haciéndose pasar por sitios oficiales y confiables, en algunos casos hacerles creer que obtendrá algún beneficio si otorga esa información.

Las estafas de phishing engañan a las víctimas mediante el uso de la ingeniería social para crear una sensación de urgencia. Una vez que la víctima abre un correo electrónico o mensaje de texto de phishing y hace clic en el enlace malicioso, se le lleva a un sitio web falso que coincide con el sitio legítimo.

A pesar de ser uno de los delitos cibernéticos más antiguos, el phishing sigue siendo una gran amenaza cibernética para muchas organizaciones. Esto se debe a su uso generalizado y a las sofisticadas campañas de phishing. Los phishers recopilan cada

⁵⁹ stratix system. (s.f.). *Five Server Security Concerns You Need to Know [En línea]*. Obtenido de Disponible en: <https://stratixsystems.com/five-server-security-concerns-need-know-3/>

vez más información sobre sus objetivos para mejorar la eficacia de sus mensajes de phishing.

- **Ingeniería social**

Es una de las estrategias más comunes usadas por los delincuentes debido a que su principal objetivo es obtener información del usuario por medio del engaño, ya sea por un mensaje, correo electrónico o una llamada del soporte técnico de alguna empresa de servicios, haciéndoles creer que está ingresando en un sitio seguro o que debe responder de manera urgente esa llamada o mensaje, de lo contrario traerá consecuencias.

Los ataques de ingeniería social son populares porque ayudan a los ciberdelincuentes a evitar el arduo esfuerzo de localizar y explotar vulnerabilidades de seguridad para acceder a una red. En cambio, los empleados manipulados esencialmente entregan a los actores de amenazas las llaves de la red. De igual forma El objetivo es influir, manipular o engañar a las víctimas para que entreguen información personal para que pueda usarse para acceder a una red objetivo.

6.2 TÉCNICAS Y TÁCTICAS UTILIZADAS POR LOS CIBERCRIMINALES.

La base de datos ATT&CK de MITRE se puso en marcha en 2013 con el objetivo de documentar las tácticas, técnicas y procedimientos utilizados habitualmente por los cibercriminales, con el objetivo de poder conocer en profundidad cómo operan y así implementar medidas oportunas para limitar la posibilidad de verse afectado por sus ataques. Con las técnicas se puede demostrar las habilidades que tiene un ciberdelincuente para llevar a cabo diferentes acciones y cómo logra un objetivo táctico para realizar dicha acción, por otra parte, las tácticas es la utilización inteligente de la habilidad, dependiendo de la ocasión el ciberdelincuente aplica la mejor táctica para que el resultado final del ataque sea exitoso, cada táctica varía en función de la situación.

ATT&CK es una lista estructurada de comportamientos que usualmente aplican los ciberdelincuentes antes de realizar un ataque, por tal razón existe tácticas y técnicas que se expresan en forma de matriz.

En la figura 4 MITRE nos presenta de forma principal la matriz en la cual encontramos todas las técnicas y técnicas más utilizadas.

Ilustración 4 Matriz ATT&CK

ATT&CK Matrix for Enterprise

layout: side

show sub-techniques

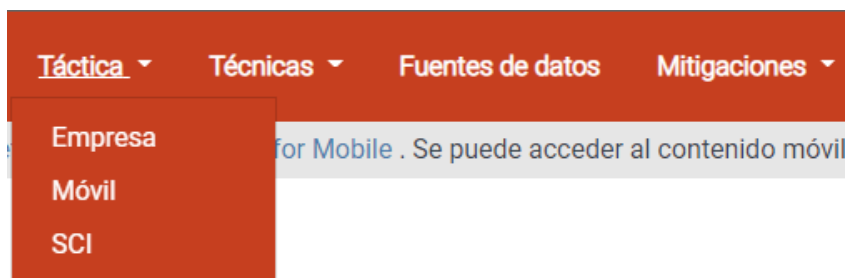
hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	42 techniques	16 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Gather Victim Org Information (4) Phishing for Information (2) Search Closed Sources (2) Search Open Technical Databases (2) Search Open Websites/Domains (2) Search Victim-Owned Websites	Acquire Infrastructure (3) Compromise Accounts (2) Compromise Infrastructure (6) Develop Capabilities (4) Establish Accounts (2) Obtain Capabilities (4) Stage Capabilities (2) Supply Chain Compromise (2) Trusted Relationship Valid Accounts (4)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (2) Replication Through Removable Media Scheduled Task/Job (2) Supply Chain Compromise (2) Trusted Relationship User Accounts (2) Windows Management Instrumentation	Command and Scripting Interface (2) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (2) Native API Scheduled Task/Job (2) Shared Modules Software Deployment Tools System Services (2) User Execution (2)	Account Manipulation (2) BITS Jobs Boot or Logon Autostart Execution (4) Boot or Logon Initialization Scripts (2) Boot or Logon Initialization Scripts (2) Browser Extensions Compromise Client Software Process (4) Create Account (2) Create or Modify System Process (4) Event Triggered Execution (2) Event Triggered Execution (2) External Remote Services Hijack Execution Flow (2) Process Injection (2) Scheduled Task/Job (2) Modify Authentication Process (2) Office Application Startup (2)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (2) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Domain Policy Modification (2) Escape to Host Event Triggered Execution (2) File and Directory Permissions Modification (2) Hide Artifacts (2) Hijack Execution Flow (2) Process Injection (2) Indicator Removal on Host (2) Valid Account (2)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (2) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Force Authentication Forge Web Credentials (2) Input Capture (2) Modify Authentication Process (2) Domain Trust Discovery Multi-Factor Authentication Interception Multi-Factor Authentication Request Generation Network Sniffing Network Share Discovery Network Sniffing Steal Application Access Token Steal or Forge Tickets (2) Permission Groups	Adversary-in-the-Middle (2) Brute Force (2) Credentials from Passwords (2) Credentials from Passwords (2) Exploitation for Credential Access Force Authentication Forge Web Credentials (2) Input Capture (2) Modify Authentication Process (2) Domain Trust Discovery Multi-Factor Authentication Interception Multi-Factor Authentication Request Generation Network Sniffing Network Share Discovery Network Sniffing Peripheral Device Discovery Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (2)	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Service Session Hijacking (2) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (2)	Adversary-in-the-Middle (2) Archive Collected Data (2) Audio Capture Automated Collection Browser Session Hijacking (2) Clipboard Data Data from Cloud Storage Object Data from Configuration Repository (2) Data from Information Repositories (2) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2) Email Collection (2) Input Capture (2)	Application Layer Protocol (2) Communication Through Removable Media Data Encoding (2) Data Obfuscation (2) Dynamic Resolution (2) Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (2) Remote Access Software Traffic Signaling (2) Web Service (2)	Automated Exfiltration (2) Data Transfer Size Limits Data Destruction for Impact Data Manipulation (2) Defacement (2) Disk Wipe (2) Endpoint Denial of Service (2) Firmware Corruption Exfiltration Over Physical Channel Resource Hijacking Scheduled Transfer Service Stop System Shutdown/Reboot		

Fuente: <https://attack.mitre.org/>

De igual forma podemos realizar la clasificación por tácticas, técnicas y mitigaciones, en donde en las 3 elecciones encontramos la opción de elegir empresa, móvil o SCI como se evidencia en la figura 5.

Ilustración 5 Clasificación de tácticas, técnicas y mitigaciones



Fuente: <https://attack.mitre.org/>

No obstante, se cuenta con una matriz denominada PRE-ATT&CK la cual permite a las organizaciones a percibir donde podría concentrar mas recursos de seguridad dependiendo del sistema establecido, de igual forma la presente matriz se enfoca en las fases de preparación, lo que permite a las organizaciones predecir y prepararse ante un posible ataque y así poder mitigarlo a tiempo o detenerlo.

Ilustración 6 Matriz PRE-ATT&CK

Matriz PRE

A continuación se encuentran las tácticas y técnicas que representan MITRE ATT&CK® Matrix for Enterprise que cubren las técnicas preparatorias. La Matriz contiene información para la plataforma PRE.

Ver en el navegador ATT&CK®

Versión Enlace permanente

diseño: lado
mostrar subtécnicas
ocultar subtécnicas
ayuda

Reconocimiento 10 técnicas	Desarrollo de recursos 7 técnicas
Escaneo activo (3)	Adquirir Infraestructura (6)
Recopilar información sobre el anfitrión de la víctima (4)	Cuentas de Compromiso (2)
Recopilar información de identidad de la víctima (3)	Infraestructura comprometida (6)
Recopilar información de la red de víctimas (6)	Desarrollar capacidades (4)
Recopilar información de la organización de la víctima (4)	Establecer Cuentas (2)
Phishing para Información (3)	Obtener capacidades (6)
Buscar fuentes cerradas (2)	Capacidades de escenario (5)
Buscar bases de datos técnicas abiertas (5)	
Buscar sitios web/dominios abiertos (2)	
Buscar sitios web propiedad de las víctimas	

Fuente: <https://attack.mitre.org/matrices/enterprise/pre/>

Teniendo en cuenta lo anterior, se propone un cuadro comparativo donde se estable algunas de las técnicas y tácticas de ejecución su estado Enterprise (empresas), tenidas en cuenta por los ciber atacantes (ATT&CK) y de igual forma, las técnicas y tácticas de prevención establecidas por las organizaciones (PRE- ATT&CK).

	Técnicas	Tácticas
PRE-ATT&ACK	Escaneo activo	Definición de prioridad
	Información sobre el anfitrión de la víctima	Selección de destino
	Información de la identidad de la víctima	Recopilación de información
	Recopilación información de la red de las víctimas	Identificación de debilidades
	Establecer cuentas	Capacidades de prueba
	Capacidades de escenario	Capacidades de montaje
ATT&CK	Aprovechar la aplicación orientada al publico	Acceso inicial
	Interpretación de comandos y secuencias de comandos	Ejecución
	Scripts de inicialización de arranque o inicio de sesión	Escala de privilegios

	Exfiltración a través del servicio web	Exfiltración
	Protocolo de capa de aplicación	Comando y control

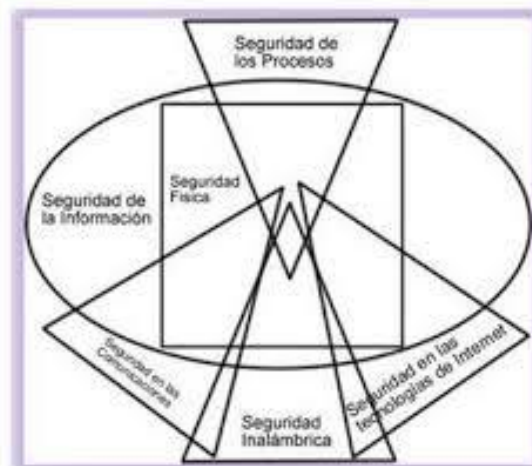
6.2.1 METODOLOGIAS UTILIZADAS POR LOS CIBERDELINCUENTES

Las siguientes metodologías están enfocadas a la auditoria de seguridad de la información, en las cuales establecen una serie de pasos para efectuar pruebas que utilizan los expertos en la materia o hacker éticos para analizar las posibles brechas de seguridad o mitigar alguna vulnerabilidad existente, sin embargo, también son tomadas por los ciberdelinquentes que usan estos métodos para penetrar la seguridad de los sistemas con el mayor sigilo posible. Conocer estas metodologías nos permite tener claridad de lo que puede suceder en un ataque y como se podría mitigar.

- **OSSTMM (Open-Source Security Testing Methodology Manual)**

El Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM) Se ha desarrollado principalmente como una metodología de auditoría de seguridad que evalúa los requisitos reglamentarios y de la industria, es revisado periódicamente por pares y mantenido por el Instituto de Seguridad y Metodologías Abiertas (ISECOM) donde su principal objetivo es proporcionar un proceso científico para la caracterización precisa de la seguridad de las operaciones que se puede utilizar para pruebas de penetración, piratería ética y otras pruebas de seguridad.

Ilustración 7 Modelo OSSTMM



Fuente: <https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcS4p-5PwkqOtvoogzfZupBwHiPWp7uv01-2kg&usqp=CAU>

OSSTMM brinda orientación sobre las pruebas de seguridad operativa de cinco canales para que las organizaciones puedan comprender el alcance completo de su seguridad y determinar qué tan bien funcionan realmente sus procesos de seguridad. Se trata de lo que realmente hacen tus actividades, no solo de lo que se supone que deben hacer.⁶⁰

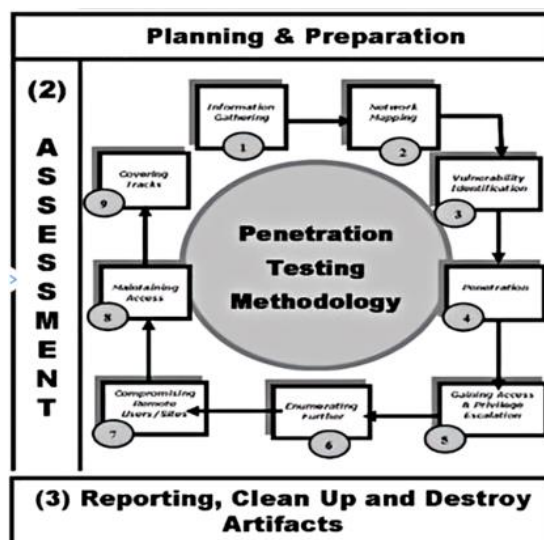
- **ISSAF (Information Systems Security Assessment Framework)**

El marco de evaluación de seguridad de los sistemas de información (ISSAF) es una metodología en la cual consiste en que el verificador de penetración copia los pasos de piratería más comunes con algunas fases complementarias. Su objetivo principal es

⁶⁰ KirkpatrickPrice. (3 de Octubre de 2019). *What You Need to Know About OSSTMM*. Obtenido de What is the Open Source Security Testing Methodology Manual (OSSTMM)? [En línea]: Disponible en: <https://kirkpatrickprice.com/blog/what-you-need-to-know-about-osstmm/>

suministrar una guía completa para efectuar un pentest, siendo una base fundamental para crear su propia metodología personalizada.

Ilustración 8 Modelo ISSAF



Fuente: <https://www.researchgate.net/profile/Redho-Maland/publication/348648583/figure/fig3/AS:982287277621249@1611206945302/ISSAF-Penetration-Testing-Methodology.ppm>

Esta metodología cuenta con el soporte del Grupo de Seguridad de los Sistemas de Información Abiertos (OISSG). Aunque últimamente no está siendo muy usada, por lo tanto, está un poco desactualizado, uno de sus puntos significativos es que relaciona los pasos de pentest individuales con las herramientas de pentest, la cual pasa por las siguientes fases:

- ✓ Recopilación de información
- ✓ Mapeo de red
- ✓ Identificación de vulnerabilidades
- ✓ Penetración
- ✓ Obtención de acceso y escalada de privilegios
- ✓ Enumerando más
- ✓ Comprometer usuarios/sitios remotos
- ✓ Mantenimiento del acceso
- ✓ Cubriendo las pistas

ISSAF también analiza la aplicación de las capas (actividades) en diferentes tipos de objetivos. Para cada uno de estos, la metodología proporciona información básica sobre los objetivos, sus configuraciones típicas, qué herramientas de ataque usar y los resultados de la evaluación que se pueden

esperar. Los pasos/ejemplos específicos de esta sección están desactualizados, por lo que deberán adaptarse a las últimas versiones de los sistemas (SO, aplicaciones, etc.).⁶¹

- **OWASP (Open Web Application Security Project)**

La Metodología de calificación de riesgos de OWASP fue creada como un medio para evaluar de manera fácil y precisa la probabilidad y el impacto de una vulnerabilidad de aplicación web, explotando de manera segura y ayudando a abordar estas vulnerabilidades para que cualquier debilidad descubierta pueda abordarse rápidamente.

Ilustración 9 Evaluación de una vulnerabilidad por OWASP

Gravedad general del riesgo				
Impacto	ALTO	Medio	Alto	Crítico
	MEDIO	Bajo	Medio	Alto
	BAJO	Nota	Bajo	Medio
		BAJO	MEDIO	ALTO
	Probabilidad			

Fuente: <https://www.simplerisk.com/sites/default/files/2021-02/owasp-risk-rating-methodology.png>

Esta metodología es un juego centrado en la aplicación en la Calificación de Riesgo Clásica descrita anteriormente, donde la Probabilidad se evalúa en función de los factores de Agente de Amenaza y Vulnerabilidad y el Impacto se evalúa en función de factores Técnicos y Comerciales. Se centra únicamente en las fases de prueba principales de las pruebas de seguridad de las aplicaciones web.

Un pentest de seguridad de OWASP puede ayudar a identificar vulnerabilidades clave como las enumeradas en OWASP Top Ten:

⁶¹ Future Learn . (s.f.). *Information System Security Assessment Framework (ISSAF)* [En línea]. Obtenido de Disponible en: <https://www.futurelearn.com/info/courses/ethical-hacking-an-introduction/0/steps/71521>

- ✓ Defectos de inyección
- ✓ Autenticación rota
- ✓ Exposición de datos confidenciales
- ✓ Entidades externas XML (XXE)
- ✓ Controles de acceso rotos
- ✓ Configuración incorrecta de seguridad
- ✓ Script entre sitios (XSS)
- ✓ Deserialización insegura
- ✓ Uso de componentes con vulnerabilidades conocidas
- ✓ Registro y monitoreo insuficientes

La metodología proporciona una discusión detallada sobre la evaluación de la seguridad de las aplicaciones web, así como su pila de implementación, incluida la configuración del servidor web. Sigue un enfoque de pentesting de caja negra y comprende "qué" y "cuándo". También hay algunas guías sobre 'cómo', principalmente en forma de lista de herramientas que se pueden usar en cada paso o tarea.⁶²

- **CEH (Certified Ethical Hacker)**

CEH "Hacker ético certificado", es una certificación ofrecida a través de EC-Council (Consejo internacional de consultores de comercio electrónico) que indica la capacidad de un individuo para usar técnicas de piratería para identificar y solucionar tanto debilidades como vulnerabilidades en las redes de seguridad existentes. Los piratas informáticos éticos utilizan algunas de las mismas técnicas que los piratas informáticos ilegales, pero de una manera legal y legítima para evaluar la postura de seguridad de un objetivo del sistema, pero el objetivo es ayudar a fortalecer los sistemas de seguridad, no derribarlos.

Varios vectores de ataque y contramedidas preventivas. Todos los temas cubiertos por la certificación dan una idea de cómo piensan y actúan los piratas informáticos. Los profesionales están mejor posicionados para configurar una infraestructura de seguridad y defenderse de los ataques. Esta prueba evalúa a los candidatos en su conocimiento en 9 fases de piratería:

- ✓ Descripción general de seguridad de la información y piratería ética
- ✓ Técnicas de reconocimiento
- ✓ Fases de Hackeo del Sistema y Técnicas de Ataque
- ✓ Hackeo de red y perímetro
- ✓ Hackeo de aplicaciones web

⁶² REDSACAN. (16 de Noviembre de 2020). *What is OWASP penetration testing?* [En línea]. Obtenido de Disponible en: <https://www.redscan.com/news/what-is-owasp-penetration-testing/>

- ✓ Hackeo de redes inalámbricas
- ✓ Hacking de plataforma móvil, IoT y OT
- ✓ Computación en la nube
- ✓ Criptografía

Como afirma el Consejo de la CE, "para atrapar a un pirata informático, debe pensar como tal"; entonces, la credencial CEH está diseñada para brindar a los profesionales la capacidad de aplicar los mismos conocimientos y metodologías que los piratas informáticos malintencionados, pero de manera legal y legítima. En esencia, "CEH se creó para incorporar un entorno práctico y un proceso sistemático en todos los dominios y metodologías de piratería ética, lo que le permite trabajar para demostrar el conocimiento y las habilidades necesarios para realizar el trabajo de un hacker ético".⁶³

• OFFENSIVE SECURITY

La metodología de seguridad ofensiva es un tipo de ciberseguridad que se basa en implementar medidas de seguridad, a través de estrategias de hacking que identifican riesgos potenciales antes de un ataque real. En otras palabras, la seguridad ofensiva utiliza las herramientas, mecanismos y tecnologías que usaría un ciberdelincuente para identificar amenazas ante posibles intentos de ataque y tener un plan sobre cómo responder de inmediato y mantener la situación bajo control.

⁶³ INFOSEC. (26 de ABRIL de 2022). *Certified Ethical Hacker (CEH) certification – Overview of domains*. Obtenido de Disponible en: <https://resources.infosecinstitute.com/certification/certified-ethical-hacker-ceh-certification-overview-of-domains/>

Ilustración 10 Identificación de amenazas Offensive Security



Fuente: <https://auditech.es/wp-content/uploads/2020/10/Infographic-Auditech-Offensive-Security-.png>

La metodología de seguridad ofensiva tiene como objetivo estar un paso más allá de los ciberdelincuentes al implementar métodos ofensivos de manera defensiva. Los métodos constan de tres componentes principales: molestia, atribución y ataque.

- ✓ El componente molesto: consiste en frustrar deliberadamente el intento de un atacante de entrar en un sistema atrayéndolo a directorios, servicios y puertos falsos.
- ✓ El componente de atribución: identifica con precisión al atacante, generalmente colocando una baliza web en documentos confidenciales.
- ✓ El componente de ataque: se refiere a las medidas de prueba de penetración convencionales utilizadas para identificar las vulnerabilidades del sistema antes de que lo hagan los atacantes.⁶⁴

Esta trata de probar las posturas de seguridad desde el punto de vista de un adversario o competidor. Por ejemplo, supongamos que un producto tiene la mejor seguridad jamás construida para proteger las contraseñas de los usuarios. Sin embargo, un competidor quiere aplicar ingeniería inversa al código fuente del producto para hacer una copia. Si el producto no cuenta con protecciones para evitar que un competidor

⁶⁴ CYBRARY. (7 de Enero de 2022). *What Is Offensive Security?* Obtenido de Disponible en: <https://www.cybrary.it/blog/what-is-offensive-security/>

robe su producto, entonces la seguridad general del producto es inadecuada, independientemente de qué tan bien cumpla su propósito previsto.⁶⁵

6.2.2 HERRAMIENTAS UTILIZADAS POR LOS CIBERDELINCUENTES

Independientemente de lo que piense el ciberdelincuente, sus objetivos iniciales son encontrar la debilidad de seguridad común, los softwares sin parches o los sistemas mal configurados. La mayoría de las herramientas de fácil uso, son fáciles de encontrar en internet y se propagan mediante correos electrónicos no deseados y redes públicas o con poca seguridad. Las siguientes 4 herramientas son las más utilizadas:⁶⁶

- **Trojanos de acceso remoto (RAT):** son un programa de malware utilizado por los ciberdelinquentes para tomar el control total de la computadora para realizar actividades maliciosas. Las RAT se adjuntan con programas de uso común y también en juegos. Hay muchas RAT disponibles, pero JBi Frost ha estado en el mundo digital debido a su gran demanda por parte de los ciberdelinquentes, según lo dicho por los expertos en **ciberforense** del Instituto Internacional de Seguridad Cibernética (IICS).
- **WEBSHELL EL HELICÓPTERO DE CHINA:** Esta herramienta bien escrita se puede utilizar para apuntar al servidor web. los webshells se cargan después de comprometer el objetivo y obtienen capacidad administrativa remota. crea una terminal virtual en dispositivos comprometidos. Esta herramienta tiene un tamaño muy pequeño, por lo que es fácil para el atacante cargar y explotar el objetivo.
- **LADRÓN DE CREDENCIALES: MIMIKATZ:** La herramienta fue desarrollada para apuntar a los usuarios de Windows, su principal objetivo es robar las credenciales de otros usuarios. Acceso Mimikatz en el servicio de subsistema de autoridad de seguridad local de Windows (LSASS). Esta herramienta también se implementa en metasploit. Mimikatz ha sido utilizado recientemente por ciberdelinquentes para atacar a los usuarios de Windows y las redes del directorio activo.
- **MARCO DE MOVIMIENTO LATERAL: POWERSHELL EMPIRE:** Esta herramienta está diseñada para permitir que un atacante obtenga acceso a la red, es difícil de detectarla en una red que utiliza herramientas antivirus

⁶⁵ BCSECURITY. (16 de Abril de 2020). *AN INTRODUCTION TO OFFENSIVE SECURITY [En línea]*. Obtenido de Disponible en: <https://www.bc-security.org/post/an-introduction-to-offensive-security/>

⁶⁶ Guru99. (30 de Abril de 2022). *What is Cybercrime? Types, Tools, Examples*. Obtenido de Disponible en: <https://www.guru99.com/cybercrime-types-tools-examples.html>

tradicionales ya que usa módulos como recolección de credenciales, enumeración de hosts, registro de claves. También es implementada para hacer ejecutables que puedan acceder a las redes de ingeniería social.

Un ciberdelincuente experimentado que tiene bastante experiencia en programación, programación inversa, hacking y vulnerabilidad de sistemas, usa herramientas más avanzadas, las cuales aumenta la efectividad del ataque, otorgándole fácilmente la información del objetivo sin inconvenientes y sin ser detectado, las herramientas más usadas por los expertos son:

- **KaliLinux:** es un software de código abierto mantenido y financiado por Offensive Security. Es un programa especialmente diseñado para análisis forense digital y pruebas de penetración.
- **Ophcrack:** Esta herramienta se utiliza principalmente para descifrar los hashes, que son generados por los mismos archivos de Windows. Ofrece un sistema GUI seguro y le permite ejecutarse en múltiples plataformas.
- **Estuche:** Este software permite a un investigador obtener imágenes y examinar datos de discos duros y discos extraíbles.
- **SafeBack:** se utiliza principalmente para crear imágenes de los discos duros de los sistemas informáticos basados en Intel y restaurar estas imágenes en otros discos duros.
- **Volcador de datos:** Esta es una herramienta forense informática de línea de comandos. Está disponible gratuitamente para el sistema operativo UNIX, que puede hacer copias exactas de discos adecuados para el análisis forense digital.
- **Md5sum:** Una herramienta para verificar lo ayuda a verificar que los datos se copien a otro almacenamiento con éxito o no.⁶⁷

6.3 RECOMENDACIONES Y BUENAS PRACTICAS ENFOCADAS A LOS USUARIOS.

En el sector tecnológico nadie está exento de recibir un ataque generado por ciberdelincuentes, sin embargo, existen varios métodos que los usuarios deben tener en cuenta al momento de navegar por internet. Inicialmente se recomienda hacer uso de un VPN (red privada virtual), el cual es un software diseñado para proteger la privacidad mientras se navega por la web, entre sus beneficios se encuentra tener el tráfico de navegación y la ubicación en anonimato, permitiendo que los ciberdelincuentes se les dificulte rastrear a su víctima.

⁶⁷ INFORMATION SECURITY NEWSPAPER. (s.f.). *TOP 5 TOOLS USED BY CYBER CRIMINALS RECENTLY* [En línea]. Obtenido de Disponible en: <https://www.securitynewspaper.com/2019/05/03/top-5-tools-used-by-cyber-criminals-recently/>

Una recomendación muy importante para los usuarios es saber las buenas prácticas de la ingeniería social y cómo por medio de esta técnica todos los usuarios están expuestos a un ataque de tipo phishing, suplantación de identidad, introducir una memoria USB a la computadora con una procedencia desconocida, dejar el dispositivo móvil o el computador de la empresa desbloqueado, dejando expuesto su identidad o su rol dentro de la organización para robar información. Por ello es importante fortalecer este ámbito porque es el más deficiente en seguridad y por donde más se efectúan los ataques actualmente. También es importante mantener los softwares actualizados para aumentar el nivel de seguridad y cerrar las posibles brechas de seguridad en donde se pueden filtrar información, de igual forma no descargar e instalar archivos procedentes de sitios web o correos sospechosos ya que pueden contener algún tipo de virus. No obstante, realizar copias de seguridad de los datos que se consideren delicados o de vital importancia, así se evitan desastres en caso de resultar el software defectuoso, vulnerado, con fallas en el hardware, corrupción de datos o posibles hackeos.

De igual forma es importante conocer los sitios web seguros, son aquellos que inician con HTTPS en la barra de navegación, esto demuestra que es un sitio web seguro y que cumplen con el protocolo de seguridad confiable para el usuario, como por ejemplo la página de la Universidad UNAD (<https://www.unad.edu.co/>), de igual forma, identificar enlaces y direcciones de correo electrónico fraudulentas.

Una recomendación de seguridad vital es la autenticación multifactorial (MFA), en la cual consiste en realizar una autenticación doble del usuario al momento de ingresar a cualquier sistema, por ejemplo, digitar un PIN como contraseña es un método muy débil de proteger nuestra identidad, sin embargo, si combinamos nuestro PIN con reconocimiento facial, es una forma mas seguridad de validar al usuario real y dar acceso al sistema predeterminado. Las tecnologías MFA más comunes para los usuarios son:⁶⁸

- **Autenticación biométrica:** Es uno de los métodos mas seguros y precisos de autenticar a los usuarios como también lo sería el reconocimiento facial. Este consiste en escanear las huellas dactilares y realizar el registro de este y cada vez que vaya a ingresar al sistema, esté ya sepa que es una persona valida.
- **Autenticación móvil:** Es un proceso de verificación fundamental para los usuarios ya que a través de su dispositivo móvil puede iniciar sesión en lugares seguros y acceder a los recursos necesarios desde cualquier lugar con mayor seguridad, teniendo como base la autenticación multifactorial.

⁶⁸ OneSpan . (s.f.). *¿Qué es la autenticación multifactorial (MFA)? [En línea]*. Obtenido de Disponible en: <https://www.onespan.com/es/topics/autenticacion-multifactorial>

De igual forma se recomienda diversos puntos enfocados específicamente a los usuarios, la cual se debe tener presente al momento de acceder a cualquier sistema informático.

1. En el ámbito de las contraseñas seguras, se recomienda:
 - 1.1 Usar contraseñas alfanuméricas entre 12 y 15 caracteres
 - 1.2 Evitar usar palabras y datos comunes, tales como el nombre personal o de algún familiar, fechas de nacimiento, nombre de mascotas etc.
 - 1.3 Evitar el uso de la misma contraseña en diferentes sitios web
2. No instalar Software pirata o de fuentes no confiables ya que puede resultar que estos programas pueden estar alterados por ciberdelincuentes y así crear posibles puertas de entrada en nuestro computador, de igual forma pueden contener programa maligno oculto o algún tipo de ransomware.
3. Realizar copias de seguridad de toda la información importante; hoy en día tenemos muchas alternativas de servicios de almacenamiento en la nube, son servicios de vital importancia si no deseamos guardar la información en un disco duro físico.
4. Evitar las redes inalámbricas WiFi publicas debido a que los ciber atacantes pueden realizar este tipo de redes como anzuelo para atraer a usuarios y robarles información a través del tráfico de navegación, por ende, se recomienda el uso de una VPN.

7 CONCLUSIONES

Realizando un análisis detallado de las diferentes amenazas cibernéticas que enfrentan los servicios de almacenamiento las cuales son: Malware, Spyware, Distributed Denial of Service (DDoS) Attacks, Ransomware, Zero-Day-Exploits, Advanced Persistent Threats, Trojans y Man-in-the-Middle Attack (MITM Attack), es una gran ventaja poder conocer en que consiste cada una de ellas y sobre entender la importancia de crear seguridad cibernética para evitar estos diferentes tipos de amenazas, pues hoy en día vemos con total claridad el uso progresivo de las tecnologías en todos los ámbitos como la economía, la educación, la religión, entre otros, que se han visto afectados en alguna ocasión por complejos ataques cibernéticos, es así que conociendo los posibles ataques los diferentes usuarios puedan crear barreras oportunas e identificar y conocer el procedimiento que se debe tener en caso de caer en una amenaza cibernética.

Los cibercriminales cada vez están siendo más astutos a la hora de emplear diferentes técnicas y tácticas para cometer sus delitos, afectando directamente y con más frecuencia a los usuarios de grandes empresas y además de eso a las diferentes plataformas abiertas al público, que son de fácil acceso y de poca seguridad, ellos buscan poder fortalecer e identificar que técnica puede aplicar y funcionar para ir más adelante que la seguridad cibernética, algunas técnicas y tácticas más reconocidas gracias a la ATT&CK de MITRE son: OSSTMM (Open-Source Security Testing Methodology Manual), ISSAF (Information Systems Security Assessment Framework), CEH (Certified Ethical Hacker) y OFFENSIVE SECURITY, estas técnicas y tácticas dejan a la vista como actual los cibercriminales y alertan a los usuarios para evitar este tipo de amenazas y hackers.

El avance de las TI ha llevado a que los usuarios de todo el mundo estén en su mayoría en tendencia frente a las TI, es así que se deben controlar el uso inadecuado de las mismas, tener en cuenta las diferentes recomendaciones para evitar las amenazas cibernéticas, con prácticas muy sencillas y que día a día las grandes empresas y diferentes usuarios a partir de sus vivencias recomiendan, tener en cuenta los diferentes procesos que impiden que se puedan presentar amenazas cibernéticas, es de vital importancia no dejar expuesta información personal, el bloqueo de los aparatos tecnológicos previenen actos de amenazas, el no exponer contraseñas y claves en las diferentes aplicaciones, además de ser cautelosos con la información que se obtiene, de donde proviene y las diferentes recomendaciones de diferentes empresas para evitar cualquier tipo de fraude en lo financiero.

8 RECOMENDACIONES

Es importante el estudio que se le realice para determinar las necesidades de la empresa u organización para el uso del servicio de TI. Para la identificación de los diferentes análisis con sus enfoques, capacidades y sus características. Para la implementación del modelo eficiente.

Si es rentable para la empresa u organización los costos que tienen el consumo de esos servicios siendo un factor importante para analizar y estudiar sobre la nube publica para la implementación de los servicios TI que ofrece. Pagando por el servicio sin contar con una infraestructura propia.

Es necesario determinar el nivel de seguridad sobre los servicios TI que requieren, ya que se debe tener su nivel estratégico para el manejo de su almacenamiento y seguridad de sus datos. Siendo la Cloud Computing Pública líder e innovadora para el futuro cumpliendo las necesidades de las empresas u organizaciones.

9 DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este; con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema del análisis de las amenazas cibernéticas más representativas que enfrentan los servicios de nube pública, puedan acceder al documento.

10 ANEXO

A continuación, se adjunta el enlace del video de la sustentación:

https://drive.google.com/file/d/1mVl3tWlJwBSUtlbdxiTKhA3m7_QWQba-/view?usp=sharing

BIBLIOGRAFÍA

ALCALDIA MAYOR DE BOGOTÁ. (s.f.). LEY 1341 DE 2009 (EN LINEA) {18 febrero de 2022}.

AMAZON WEB SERVICES. (20 de OCTUBRE de 2013). *AMAZON ELASTIC COMPUTE CLOUD (AMAZON EC2)*(EN LINEA). Obtenido de <http://aws.amazon.com/ec2/>

AMAZON WEB SERVICES. (2019). *AMAZON SIMPLE QUEUE SERVICE (AMAZON SQS)* (EN LINEA). Obtenido de [HTTP://AWS.AMAZON.COM/SQS/](http://AWS.AMAZON.COM/SQS/)
ambit Bulding Solutions together. (11 de Febrero de 2020). *Importancia de los SLAs en los Servicios IT {En línea}*. Obtenido de Disponible en: <https://www.ambit-bst.com/blog/importancia-de-los-slas-en-los-servicios-it>

AREOS, I. (2015). *ARTEFACTOS FORENSES* (EN LINEA). Obtenido de <http://insecuredata.blogspot.com/2015/03/artefactos-forenses-i.html>

AZEEM KHALIL KHREISHAH. (2014). CLOUD COMPUTING SECURITY: A SURVEY COMPUTERS (EN LINEA).

BCSECURITY. (16 de Abril de 2020). *AN INTRODUCTION TO OFFENSIVE SECURITY [En línea]*. Obtenido de Disponible en: <https://www.bc-security.org/post/an-introduction-to-offensive-security/>

BOXBYTE. (01 de 01 de 2012). *FAYERWAYER*(EN LINEA). Obtenido de <https://www.fayerwayer.com/2012/01/el-origen-de-el-computo-en-la-nube/>

BROW ANDERSON. (2018). SECURITY RISKS AND COUNTERMEASURES (EN LINEA). *ATHABASCA UNIVERSITY*.

BUITRAGO, Y., & SILVA, D. (2009). HACIA UNA ONTOLOGÍA UNIFICADA DE LA COMPUTACIÓN EN LA NUBE.(EN LINEA).

BURNS, A., HERRING, C., & PETERSON, K. (2007). PROVABLE DATA POSSESSION AT UNTRUSTED STORES. (EN LINEA).

BUYYA, B., & GOSCINSKI, A. (2014). PRINCIPIOS Y PARADIGMAS DE LA NUBE COMPUTACIONAL.(EN LINEA).

CAMPS, C., & ORIOL, A. (2012). LA NUBE: OPORTUNIDADES Y RETOS PARA LOS INTEGRANTES DE LA CADENA DE VALOR.(EN LINEA). *MANAGEMENT SOLUTIONS*.

CARTER, W., & ZHENG, D. (2015). THE EVOLUTION OF CYBERSECURITY REQUIREMENTS FOR THE U.S.(EN LINEA). *FINANCIAL INDUSTRY*.

CCN. (2014). CENTRO CRIPTOLOGICO NACIONAL (EN LINEA). *GUÍA DE SERGURDAD DE LAS TIC*.

CERVIGON DAVID. (2012). *IAAS, PAAS, SAAS, NUBER PRIVADAS Y PÚBLICAS E ITAAS (EN LINEA)*.

CHAKI, B., & CHAKI, S. (2014). A SURVEY ON SECURITY ISSUES IN CLOUD COMPUTING.(EN LINEA). *UNIVERSITY POLITEHANICA TIMISOARA*.

CHANG, F., GHEMAWAT, S., & HSIEH, W. (2006). *BIGTABLE: A DISTRIBUTED*

STORAGE SYSTEM FOR STRUCTURED DATA.(EN LINEA). SEVENTH SYMPOSIUM ON OPERATING SYSTEM DESIGN AND IMPLEMENTATIO.

CHOW GOLLE, J., & MOLINA, M. (2009). *CONTROLLING DATA IN THE CLOUD: OUTSOURCING COMPUTATION WITHOUT OUTSOURCING CONTROL ACM.(EN LINEA)*.

CONTRACTOR PATEL. (2012). TRUT MANAGEMENT FRAMEWORK FOR ATTENUATION OF APPLICATION LAYER DOS ATTACK INCLOUD COMPUTING.(EN LINEA).

Cox, P. (s.f.). *Krypton SOLID*. Obtenido de Principales amenazas en un servicio en la nube PaaS y cómo evitarlas [En línea]: Disponible en: <https://kryptonsolid.com/principales-amenazas-en-un-servicio-en-la-nube-paas-y-como-evitarlas/#:~:text=Seg%C3%BAAn%20mi%20experiencia%2C%20estas%20son%20las%20amenazas%20m%C3%A1s,3%20Permisos%20inseguros%20sobre%20datos%20en%20la%20nube>

CSA. (2011). CLOUD SECURITY ALLIANCE (EN LINEA). *GUÍAS DE SEGURIDAD DE ÁREAS CRITICAS EN CLOUD COMPUTING V3.0*.

CSO COMPUTERWORLD. (29 de Enero de 2020). *Los riesgos más trascendentes de los entornos SaaS [En línea]*. Obtenido de Disponible en: <https://cso.computerworld.es/tendencias/los-riesgos-mas-trascendentes-de-los-entornos-saas>

CYBRARY. (7 de Enero de 2022). *What Is Offensive Security?* Obtenido de Disponible en: <https://www.cybrary.it/blog/what-is-offensive-security/>

DANIEL, D. B. (4 de SEPTIEMBRE de 2018). *GLOBB SECURITY [En Línea]*. Obtenido de <https://globbsecurity.com/servicios-cloud-las-12-amenazas-de-seguridad-en-la-nube-que-no-se-deben-olvidar-43654/>

EINATEC. (2012). *EINATEC (EN LINEA)*. Obtenido de <https://einatec.com/historia-cloud-computing/>

FABREGA , A. (2012). UN CONCEPTO TECNOLÓGICO REVOLUCIONARIO Y DE GRAN IMPACTO ECONÓMICO.(EN LINEA). *INNOVACION*.

Future Learn. (s.f.). *Information System Security Assessment Framework (ISSAF) [En línea]* {6 febrero de 2022}. Obtenido de Disponible en: <https://www.futurelearn.com/info/courses/ethical-hacking-an-introduction/0/steps/71521>

GARCIA ZABALLOS, A., IGLESIAS RODRÍGUEZ, E., PUIG GABARRÓ, P., & CAMPERO, T. (2020). *IDB [En línea]*. Obtenido de CONTRATACIÓN PÚBLICA DE SERVICIOS DE COMPUTACIÓN EN LA NUBE: Disponible en: <https://publications.iadb.org/publications/spanish/document/Contratacion-publica-de-servicios-de-computacion-en-la-nube-Mejores-pr%C3%A1cticas-para-su-implementacion-en-America-Latina-y-el-Caribe.pdf>

GARFINKEL ROSENBLUM. (2013). VIRTUAL MACHINE INTROSPECTION BASED ARCHITECTURE FOR INTRUSION DETECTION.(EN LINEA).

GARFINKEL, R. (2013). SECURITY CHALLENGES IN VIRTUAL MACHINE BASED COMPUTING ENVIRONMENTS(EN LINEA). *STANFORD UNIVERSITY DEPARTMENT OF COMPUTER*.

GARTHER INC. (20 de OCTUBRE de 2009). *GARTNER SAYS CLOUD COMPUTING WILL BE AS INFLUENTIAL AS E-BUSINESS*. Obtenido de <http://www.gartner.com/it/page.jsp?id=707508>

GOOGLE. (209). *GOOGLE APP ENGINE (EN LINEA)*. Obtenido de <HTTP://CODE.GOOGLE.COM/>

GROBAUER, W. (2012). UNDERSTANDING CLOUD COMPUTING VULNERABILITIES.(EN LINEA). *IEEE COMPUTER SOCIETY*.

HARAUZ KAUFMAN. (2010). POTTER DATA SECURITY IN THE WORL OF CLOUD COMPUTING (EN LINEA). *IEEE COMPUTER AND RELIABILITY SOCIETIES*.

INFORMATION SECURITY NEWSPAPER. (s.f.). *TOP 5 TOOLS USED BY CYBER CRIMINALS RECENTLY [En línea]*. Obtenido de Disponible en: <https://www.securitynewspaper.com/2019/05/03/top-5-tools-used-by-cyber-criminals-recently/>

INFOSEC. (26 de aBRIL de 2022). *Certified Ethical Hacker (CEH) certification – Overview of domains*. Obtenido de Disponible en: <https://resources.infosecinstitute.com/certification/certified-ethical-hacker-ceh-certification-overview-of-domains/>

JENSEN SCHWENK, GRUSCHKA IACONO. (2010). ON TECHNICAL SECURITY ISSUES IN CLOUD COMPUTING (EN LINEA).

JOYANES AGUILAR, L. (2010). COMPUTACIÓN EN LA NUBE NOTAS PARA UNA ESTRATEGIA ESPAÑOLA EN CLOUD COMPUTING.(EN LINEA). *UNIVERSIDAD PONIFICIA COMILLAS*.

J

OYANES, L. (2012). COMPUTACIÓN EN LA NUBE: ESTRATEGIAS DE CLOUD COMPUTING EN LA EMPRESAS.(EN LINEA). *EDICIONES ALFAOMEGA*.

KAPLAN. (s.f.). *WHAT IS THE CEH CERTIFICATION?* [En línea]. Obtenido de Disponible en: WHAT IS THE CEH CERTIFICATION?

Kezherashvili, B. (s.f.). *Computación en la Nube* [En línea]. Obtenido de Disponible en: http://www.adminso.es/recursos/Proyectos/PFM/2011_12/PFM_cloud_beka.pdf

KirkpatrickPrice. (3 de Octubre de 2019). *What You Need to Know About OSSTMM*. Obtenido de What is the Open Source Security Testing Methodology Manual (OSSTMM)? [En línea]: Disponible en: <https://kirkpatrickprice.com/blog/what-you-need-to-know-about-osstmm/>

LLEIXA, A. (2015). *LA EVIDENCIA DIGITAL ANTE RIESGOS Y AMENAZAS EN EL CLOUD COMPUTING. ASPECTOS PROFESIONALES: PROTECCIÓN DE DATOS, CLOUD COMPUTING Y SISTEMAS DE GESTIÓN*.(EN LINEA). Obtenido de <http://www.aspectosprofesionales.info/2015/06/la-evidencia-digital-ante-riesgos-y.html>

MELL GRANCE. (2011). *THE NIST DEFINITION OF CLOUD COMPUTING RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*.(EN LINEA).

MELL, P., & GRANCE, T. (s.f.). *DEFINITION OF CLOUD COMPUTING*.(EN LINEA). *NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*.

MICROSOFT. (209). *MICROSFT SQL AZURE DATABASE* (EN LINEA). Obtenido de <HTTP://WWW.MICROSOFT.COM/WINDOWSAZURE/SQLAZURE/>

MITRE | ATT&CK. (s.f.). *ATT&CK Matrix for Enterprise* [En línea]. Obtenido de Disponible en: <https://attack.mitre.org/>

NORMA ISO 27001(SEGURIDAD DE LA INFORMACIÓN),ISO 31000(RIESGO),9001(CALIDAD),ISO 27018(PROTECCIÓN INFORMACIÓN PERSONAL NUBE)(EN LINEA). (s.f.).

OneSpan . (s.f.). *¿Qué es la autenticación multifactorial (MFA)?* [En línea]. Obtenido de Disponible en: <https://www.onespan.com/es/topics/autenticacion-multifactorial>

ORIOL FITO Y JORDI GUITART. (2015). *INTRODUCING RISK MANAGEMENT INTO CLOUD COMPUTING* (EN LINEA).

Orozco, I., & Jacobs, O. (2017). *LA NUEVA ERA DE LOS NEGOCIOS: COMPUTACIÓN EN LA NUBE*.(EN LINEA). *REVISTA ELECTRÓNICA DE ESTUDIOS TELEMÁTICOS*, 21.

Ortiz Chimbo, K. M., Luna Aveiga, H., Yanez, R. M., & Parra, M. A. (2016). *LA IMPORTANCIA DEL USO DE LAS CLOUD COMPUTING EN LAS EMPRESAS PUBLICAS Y PRIVADAS*.(EN LINEA). *CONTRIBUCIONES A LA ECONOMÍA*.

OSCAR AVILA. (2012). DIRECCIÓN GENERAL DE POLÍTICAS INTERIORES (EN LINEA). *COMPUTACIÓN EN LA NUBE*.

OWASP.ORG. (s.f.). *Cloud Security en IaaS Una visión de Seguridad desde el Data Center* {En línea} {20 de marzo de 2022}. Obtenido de Disponible en: https://owasp.org/www-pdf-archive/3-Cloud_Security_IaaS.pdf

PASTRANA PERALTA, F. S., MUÑOS RAMOS, J. S., & RUIZ RUIZ, R. A. (2016). IMPLEMENTACIÓN DE UNA NUBE PRIVADA PARA LOS SERVICIOS INTERNOS DE LA DIRECCIÓN DE PROMOCIÓN A LA INNOVACIÓN Y CREATIVIDAD DEL

MINISTERIO DE LA JUVENTUD DE MANAGUA.(EN LINEA). *UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA*.

Pastrana Peralta, F., Muñoz Ramos, J., & Ruiz Ruiz, R. (2016). *Servicios en la Nube* [En línea]. Obtenido de Implementación de una nube privada para los servicios internos de la Dirección de Promoción a la Innovación y Creatividad del Ministerio de la Juventud de Managua, en el segundo semestre de 2016 [En línea].

PEREZ BOTERO, SZEFER LEE. (2013). CHARACTERIZING HYPERVISOR VULNERAILITIES IN CLOUD COMPUTING SERVERS (EN LINEA).

PRIMORAC, C. R., & LA RED, D. L. (2014). *COMPUTACIÓN EN LA NUBE (MONOGRAFIA DE ADSCRIPCIÓN DE LICENCIATURA EN COMPUTACIÓN)*.(EN LINEA).

Primorac, C., & La Red, D. L. (2014). *COMPUTACIÓN EN LA NUBE*.(EN LINEA). *UNIVERSIDAD NACIONAL NORDESTE*.

REDÍGOLO, M. G., & NASLUD, S. C. (2012). *A QUANTITATIVE ANALYSIS OF CURRENT SECURITY CONCERNS AND SOLUTIONS FOR CLOUD COMPUTING*.(EN LINEA). *SPRINGER JOURNAL OF CLOUD COMPUTING: ADVANCES, SYSTEMS AND APPLICATIONS*.

REDSACAN. (16 de Noviembre de 2020). *What is OWASP penetration testing?* [En línea]. Obtenido de Disponible en: <https://www.redscan.com/news/what-is-owasp-penetration-testing/>

RIVERO, M. (s.f.). *¿QUE SON LOS MALWARES?* (EN LINEA). Obtenido de <<https://www.infospyware.com/articulos/que-son-los-malwares/>>.

SAPIÉN AGUILAR, A. L., PIÑON HOWLET, L. C., & GUITIERREZ DIEZ, M. (2013). ANALISIS DEL SERVICIO DE LA NUBE COMPUTACIONAL. CASO DE ESTUDIO:

EMPRESAS DE LA CUIDAD DE CHIHUAHUA.(EN LINEA). *CONGRESO INTERNACIONA EN CIENCIAS ADMINISTRATIVAS*.

SARIPALLI WALTERS. (2010). *A QUANTITATIVE IMPACT AND RISK ASSESSMENT FRAMEWORK FOR CLOUD SECURITY*.(EN LINEA).

SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V4.0 (EN LINEA). (2017).

SK GARG, B., & GREEN, H. (2012). GREEN CLOUD COMPUTING AND ENVIRONMENTAL SUSTAINABILITY.(EN LINEA).

stratix system. (s.f.). *Five Server Security Concerns You Need to Know [En línea] { 2 octubre de 2022}*. Obtenido de Disponible en: <https://stratixsystems.com/five-server-security-concerns-need-know-3/>

SULLIVAN F. (04 de 10 de 2011). *GUEST EDITOR´S INTRODUCTION: CLOUD COMPUTING FOR THE SCIENCES.* (EN LINEA). Obtenido de COMPUTING IN SCIENCE AND ENGINEERING: <http://www.savvis.net/en-US/Pages/Home.aspx>

SURYATEJA. (2018). THREATS AND VULNERABILITIES OF CLOUD COMPUTING.(EN LINEA).

SWATHI, S., & RAM, G. (2016). A SURVEY ON INTRUSION DETECTION TECHNIQUES FOR CLOUD.(EN LINEA). *INSTITUTE OF TECHNOLOGY, VIJAYAWADA AND INDIRA GANDHI NATIONAL OPEN UNIVERSITY.*

UpGuard. (s.f.). *The new standard in third-party risk and attack surface management [En línea]*. Obtenido de Disponible en: <https://www.upguard.com/>

Wall Street Consultancy. (29 de Mayo de 2021). *Company News.* Obtenido de A Complete Guide to Man in The Middle Attack (MitM) [En línea]: Disponible en: <https://wallstreetinv.com/cyber-security/man-in-the-middle-attack-mitm/>

Williams,, L. (s.f.). *What is Cybercrime? Types, Tools, Examples {2 junio de 2022}*. Obtenido de Disponible en: <https://www.guru99.com/cybercrime-types-tools-examples.html>