Espirales revista multidisciplinaria de investigación

ISSN: 2550-6862

Metodología de gestión de seguridades informáticas para internet de las cosas [1]

Methodology of computer security management for the internet of things

Ivette Mateo Washbrum, I[2]

ACEPTADO – JULIO 2018 REVISADO – NOVIEMBRE 2018 PUBLICADO ENERO 2019

[1] Artículo original derivado del proyecto de titulación " Desarrollo de Metodología de Gestión de Riesgos de Seguridad para redes de dispositivos de internet de las cosas IoT", fecha de realización febrero de 2018.

[2] Ingeniera en Electrónica y Telecomunicaciones, Master en Ingeniería de Software y Sistemas Informáticos, Docente de la Carrera de Redes, ITSVR, imateo@itsvr.edu.ec, imateo33@gmail.com, orcid.org/0000-0002-7523-7219

Resumen

Introducción. La red de internet de las cosas, objetos y dispositivos conectados al internet está creciendo exponencialmente, debido a que el despliegue y diseño de equipos se ha realizado de forma muy diversificada, ya que no se dispone de un estándar de internet de las cosas IoT, por lo que se ha hecho engorroso el control y gestión de seguridades informáticas en las redes de conexión de dispositivos al internet de las cosas. **Objetivo.** Plantear el desarrollo de un protocolo estándar para internet de las cosas, considerando las especificaciones de los dispositivos existentes y las tecnologías de comunicación vigentes, como las que se encuentran en etapa de despliegue basadas en 5G.

Basado en el protocolo estándar de internet de las cosas, se propone una metodología de gestión de riesgos y seguridades informáticas para dispositivos IoT. **Materiales y métodos.** Se propone una metodología generalizada, que combine buenas praxis para gestionar los riesgos en un sistema de conexión de objetos inteligentes al internet de las cosas, revisando los principales factores de la seguridad del sistema de conexión IoT.

Palabras clave

Metodología, Seguridad, Conexión, Dispositivos IoT.

Abstract

Introduction. The internet network of things, objects and devices connected to the internet is growing exponentially, due to the fact that the deployment and design of equipment has been carried out in a very diversified way, since there is no Internet standard for IoT things, so it has become cumbersome control and management of computer security in the networks connecting devices to the Internet of things. **Objective.** To propose the development of a standard protocol for the internet of things, considering the specifications of the existing devices and the current communication technologies, such as those that are in the deployment stage based on 5G.

Based on the standard internet protocol of things, a methodology of risk management and IT security for IoT devices is proposed. **Materials and methods.** A generalized methodology is proposed, which combines good praxis to manage the risks in a system of connection of intelligent objects to the internet of things, reviewing the main factors of the security of the IoT connection system.

key words

Methodology, Security, Connection, IoT Devices.

1. Introducción

Las propiedades autónomas de algunos objetos tales como: smartphones, tablets, relojes, pulseras, equipos de control para telemedicina, televisores, equipos de control domótica, autos, etc; requieren permanecer conectados siempre a la red de internet para actualizaciones o envío de información, como consecuencia de los estándares de vida actuales de los usuarios, quienes por comodidad realizan sus actividades cotidianas con la

ayuda y dependencia de estos dispositivos, agravando la inseguridad ya que por desconocimiento no son cuidadosos de la información que sus equipos inteligentes envían a través de la red de internet y por ende no toman las precauciones de modificar las configuraciones de seguridad por defecto que poseen estos objetos IoT.

Dado el crecimiento de las conexiones de dispositivos inteligentes al internet, la evolución del IoT, y la masificación de servicios de nube pública, se presentan más vulnerabilidades y riesgos para el tráfico de información que se transmite a través de internet, pudiendo ser interceptado por terceros y corromper los datos originales. (IBM.COM, 2017)

1.1. Fabricantes

Para los fabricantes el inconveniente se presenta porque los objetos IoT se diseñan para un propósito específico, y por ende no se contemplan todos los aspectos que involucran las seguridades generales de los equipos IoT y no se ha considerado una metodología estándar para el desarrollo de las aplicaciones IoT, cuyas validaciones de seguridad hayan sido satisfactorias para cualquier plataforma. (MICROSOFT.COM, 2017)

Se propone de manera estandarizada desarrollar la metodología de seguridad informática que gestione los riesgos de las conexiones de los dispositivos de IoT.
Verificando las políticas de seguridad aplicadas a las conexiones de dispositivos IoT, planteando un sistema general de conexiones de dispositivos inteligentes que combina los escenarios de modelos de comunicación de IoT actuales. Estableciendo los procesos de verificación de revisión de vulnerabilidades en los programas y aplicaciones para equipos inteligentes, desde el desarrollo y codificación de software seguro, con la generación de certificado y firma de seguridad previa a la salida a producción de los mismos en IoT.

2. Metodología

Se propone una metodología generalizada, que combine buenas praxis para gestionar los riesgos en un sistema de conexión de objetos inteligentes al internet de las cosas, revisando los principales factores de la seguridad del sistema de conexión IoT.

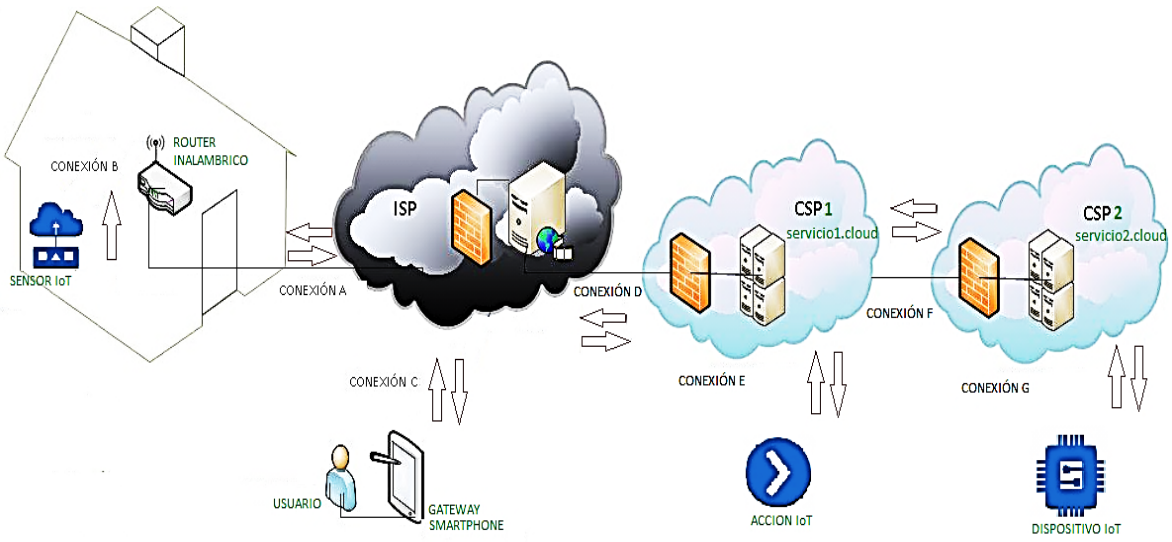

Fig.1 Sistema de Conexión de IoT. (Elaboración Ivette Mateo)

2.1. Descripción de la Metodología

Consiste en las siguientes actividades:

1.- Definir procesos de verificación de vulnerabilidades para mitigar riesgos en el hardware y software de los dispositivos inteligentes.

2.- Proponer una guía de revisión de huecos de seguridad en las comunicaciones que se establecen en cada conexión de los dispositivos IoT a través de internet con los usuarios o plataformas Cloud. (ENISA, 2017)

3.- Establecer procesos de verificación de vulnerabilidades en las Plataformas y aplicaciones Cloud.

Se identifican los requisitos, descripción, para el desarrollo, aplicación y evaluación de la metodología de gestión de seguridad informática del sistema de dispositivos inteligentes conectados al internet de las cosas.

La identificación de requisitos de desarrollo de la metodología para gestión de seguridades informáticas del sistema de conexiones de dispositivos de internet de las cosas, requiere la colaboración de los proveedores de servicios Cloud y de los fabricantes de dispositivos inteligentes.

---

3. Resultados

De la investigación realizada se ha evidenciado que no existen protocolos genéricos de IoT, lo que complica establecer una metodología generalizada de gestión de seguridades en IoT.

Se requiere tomar de base las especificaciones de los protocolos genéricos de IoT, para el diseño de los dispositivos inteligentes, en el que se debe incluir las consideraciones de seguridad, ya que dichos equipos conforman las redes de internet de las cosas IoT y la metodología propuesta se aplicaría de manera generalizada a las redes de conexiones IoT.

Se establece las especificaciones del protocolo general IoT:

- Compatibilidad con protocolos existentes: IP, TCP, UDP, TLS, DTLS, 802.11, 802.15, ZigBee, Zwave, CoAP, LTE, WirelessHart; LoRaWAN, MQTT, Json, Oauth; etc.
- Arquitectura de seguridad de canales seguros, para garantizar la integridad del sistema.
- La red ad hoc a la que puede acceder cualquier dispositivo externo y entorno de trabajo.
- Firewall entre las entidades de la capa de aplicación.
- Políticas de acceso, en el modelo de confianza abierta para permitir credenciales

compartidas reduciendo el costo.

- Credenciales de 128 bits.
- Los servicios provistos a través de este protocolo deberán utilizar variaciones de la clave de enlace en un solo sentido para evitar riesgos de seguridad.
- La distribución de claves por capas es para garantizar seguridad de la red.
- Se designará un dispositivo que hará las veces de centro de confianza que es el que distribuirá las claves.
- El dispositivo centro de confianza dispondrá clave default de inicio y la dirección IP matriz.
- Los dispositivos aceptaran únicamente conexiones generadas con una clave transmitida por el centro de confianza, con la excepción de la clave principal de inicio.
- Como excepción se facilitará el acceso a las credenciales de red, a los dispositivos que se registran por primera vez a la red.
- El emparejamiento para registro de los equipos y objetos inteligentes, se realizará través de códigos o Pin único para cada dispositivo, estas seguridades permiten cumplir estándares de encriptación para transmisiones entre nodos.
- La seguridad de los datos es responsabilidad de la capa que envía la trama.
- Las tramas de datos estarán cifradas, para prevenir el tráfico no autorizado de equipos de usuarios maliciosos. (ISO.ORG, 2017)

Basado en lo anterior se especifica la arquitectura de red de IoT.

- Interfaces compatibles con protocolo IoT entre las redes de sensores y otras redes para aplicaciones de sistemas de redes inteligentes.
- Arquitectura de red de sensores basada en protocolo IoT para soportar sistemas inteligentes.
- Interface IoT entre redes de sensores con sistemas de red inteligente.
- Aplicaciones y servicios emergentes basados en redes de sensores IoT para soportar sistemas de redes inteligentes. (CASTELLANOS, 2017)

3.1. Metodología de gestión de seguridad de IoT.

Se describe la metodología a aplicarse en el sistema IoT, basado en el modelo PHVA, Planificar, Hacer, Verificar y Actuar. (PALMES, 2010)

Definir	Se identifican los roles en esta metodología.
	Se identifica la información de usuario y equipos de red, como objetivo de protección y gestión de seguridad del sistema de redes IoT.
	Se define la estructura de autenticación de los dispositivos y servidores en la nube.
	Se utiliza una matriz de autenticación para definir los casos de uso.
	Se identifica los componentes de la red IoT, cuya seguridad se está tratando de gestionar.
	Se define la secuencia de llamadas para cada caso de uso.

Modelar	Se genera el listado de amenazas de acuerdo a las recomendaciones de Alianza de Seguridad en la Nube CSA y el Concejo de Cyber Defensa CDC. (ALLIANCE CYBER SECURITY, 2016)
	Se define las contramedidas para cada amenaza con la información presente en la librería de ataques. (OWASP.ORG, 2018)
	Se identifica como tratar los riesgos de cada amenaza. (VIOLINO, 2018)
Cuantificar	Se determina el impacto del riesgo asociado con cada amenaza, utilizando la herramienta Threat Analysis and Modeling Tool 2016 de la compañía Microsoft
	Determinar la probabilidad de riesgo asociado con cada amenaza.
Validar	Se valida el modelado. Se realiza las optimizaciones y mejoras oportunas.

Se esquematiza la revisión de seguridad en el sistema de conexiones IoT en el anexo A.

4. Discusión o Conclusiones

La conexión de equipos inteligentes hacia Internet genera nuevos escenarios de casos de uso. Algunos utilizan Internet Protocol Suite que les ofrece mayor capacidad de procesar y obtener información de datos que recoge la red de sensores, que poseen estos dispositivos, la combinación de información que se puede obtener de estos equipos y sus redes sensoriales y neuronales, ocasionan más vulnerabilidades y riesgos a los que se exponen los dispositivos y usuarios del IoT. (TEJERO, 2017)

El desarrollo de sistemas de redes IoT, que involucran redes de sensores, neuronales, la interacción con equipos y protocolos de comunicación inalámbricos, conlleva a los diseñadores de hardware y software para IoT a considerar los siguientes aspectos:

- ✓ Tiempo de operación del dispositivo, consideraciones de energización.
- ✓ Interacción a través de sensores u otro tipo de red.
- ✓ Tipos de conexión soportados hacia la red.
- ✓ Tipos de mantenimiento y actualización del dispositivo.
- ✓ Modelo de seguridad aplicable al dispositivo. (TINAJERO, 2017)

Por lo que se requiere información de tecnologías y protocolos de IoT utilizadas para el diseño de objetos y sistemas de interconexión de internet de las cosas.

Es justamente en la etapa de diseño de hardware y software que se debe tomar las consideraciones necesarias para evitar que las vulnerabilidades de seguridad de los equipos y aplicaciones sean aprovechadas por terceros inescrupulosos quienes pueden corromper la

información. (INTERNET A.B., 2017)

Los protocolos de IoT deben ser aplicados a los entornos en los que se conectan los dispositivos, y considerarse en el diseño de hardware y software, la posibilidad de reconfiguración adaptándose a la necesidad y requerimiento del usuario. (ELIZALDE, 2016)

La infraestructura de la red de Internet, los dispositivos, y aplicaciones IoT evolucionan en el transcurso del tiempo, por lo que las consideraciones de diseño y seguridad en Hardware y software deben evolucionar conjuntamente.

4.1. Conclusiones

De la investigación se concluye que en la actualidad no se dispone de una plataforma IoT que provea todas las facilidades requeridas para verificación y pruebas propuestas en la metodología de gestión de seguridades IoT.

- Se recomienda trabajar en la estandarización de equipamiento hardware y software para internet de las cosas.
- Se requiere el desarrollo de plataformas integrales de internet de las cosas que suministren herramientas para revisión automática de mecanismos de los dispositivos, así como la verificación por defecto de la codificación del software de las aplicaciones de dispositivos inteligentes y de aplicaciones en la nube.
- Las plataformas actuales fueron desarrolladas prioritariamente para trabajar con sistemas diseñados para trabajar en sus plataformas tal es el caso de AWS y Azure, por lo que la adaptabilidad de dispositivos que operen con protocolos propietarios de otros proveedores, requiere el desarrollo de interfaces que les permitan integrar estos equipos a las plataformas existentes.

La estandarización demanda que se establezcan políticas de seguridad para compartición de servicios e infraestructura de los proveedores de Cloud, actualmente no se dispone de este tipo de políticas según lo indicado por la Alianza de Seguridad en la Nube CSA y el Concejo de Ciber Defensa CDC.

Referencias bibliográficas

ALLIANCE CYBER SECURITY. (DICIEMBRE de 2016). *https://downloads.cloudsecurityalliance.org/.* Obtenido de https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

CASTELLANOS, J. (OCTUBRE de 2017). *https://www.exploit-db.com/.* Obtenido de https://www.exploit-db.com/docs/spanish/43160-reversing-and-exploiting-iot-devices.pdf

ELIZALDE, D. (DICIEMBRE de 2016). *https://techproductmanagement.com/.* Obtenido de https://techproductmanagement.com/iot-decision-framework/

ENISA. (20 de NOVIEMBRE de 2017). *https://www.enisa.europa.eu.* Obtenido de https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

IBM.COM. (MAYO de 2017). *https://www.ibm.com/.* Obtenido de https://www.ibm.com/developerworks/library/iot-trs-secure-iot-solutions1/index.html

INTERNET A.B. (OCTUBRE de 2017). *https://tools.ietf.org/.* Obtenido de https://tools.ietf.org/html/rfc6347

ISO.ORG. (NOVIEMBRE de 2017). *https://www.iso.org.* Obtenido de https://www.iso.org/standard/

MICROSOFT.COM. (DICIEMBRE de 2017). *https://azure.microsoft.com/.* Obtenido de https://azure.microsoft.com/en-us/updates/microsoft-azure-iot-reference-architecture-available/

OWASP.ORG. (ENERO de 2018). *https://www.owasp.org.* Obtenido de https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

PALMES. (2010). *PDCA: PLANIFICAR, HACER, VERIFICAR, ACTUAR. MADRID: AENOR. ASOCIACION ESPAÑOLA DE NORMALIZACION Y CERTIFICACION.* MADRID.

TEJERO, A. (FEBRERO de 2017). *https://www.researchgate.net/.* Obtenido de https://www.researchgate.net/publication/313400021_Metodologia_de_analisis_de_riesgos_para_la_mejora_de_la_seguridad_del_Internet_de_las_Cosas_Caso_Smartwatch?enrichId=rgreq-3bbb99f0acf96b6624d901d73697e9c2-XXX&enrichSource=Y292ZXJQYWdlOzMxMzQwMDAyMTtBUzo

TINAJERO, A. (FEBRERO de 2017). *https://www.researchgate.net.* Obtenido de https://www.researchgate.net/profile/Alberto_Tejero/publication/313400021_Metodologia_de_analisis_de_riesgos_para_la_mejora_de_la_seguridad_del_Internet_de_las_Cosas_Caso_Smartwatch/links/589976e34585158bf6f795db/Metodologia-de-analisis-de-riesgos-para-la

VIOLINO, C. (ENERO de 2018). *https://www.csoonline.com/.* Obtenido de https://www.csoonline.com/article/3043030/security/12-top-cloud-security-threats-for-2018.html

ISSN: 2550-6862

ANEXO A

ANALISIS DE SEGURIDAD DEL SISTEMA DE CONEXIONES IoT

ITEM	ETAPA	RIESGO	OBJETIVOS DE CONTROL	CONTROLES DE SEGURIDAD	PRUEBAS DE SEGURIDAD
1	HARDWARE DEL DISPOSITIVO	a) Manipulación del dispositivo. b) Reemplazo del dispositivo.	a) Implementar controles para prevenir manipulación física de los dispositivos. b) Implementar controles para evitar reemplazo de los objetos inteligentes.	a) Comprobar la aplicación de mecanismos a prueba de manipulaciones o reemplazo de los equipos.	a) Verificar que el dispositivo posea sensores con funcionalidad de detección de manipulación, mediante la observación de cambios en los datos del sensor. b) Verificar los seriales de los sensores y dispositivo para comprobar si no han sido cambiados.
2	SOFTWARE DEL DISPOSITIVO	a) Suplantación de identidad al acceder al dispositivo. b) Manipulación de sistema operativo y aplicaciones del dispositivo. c) Lectura de datos desde el almacén del dispositivo y manipulación de los mismos. d) Manipulación de datos de control de comandos en la memoria del dispositivo. e) Manipulación de paquetes de actualización del dispositivo, durante el almacenamiento local, provocando que los componentes del mismo estén en riesgo. f) Divulgación de información del objeto inteligente, una vez que ha sido vulnerado el software. g) Elevación de privilegios, modificando las funciones del software del dispositivo para que realice una función distinta de la establecida.	a) Asignación de identidad y credenciales para autenticación del dispositivo, y así evitar la suplantación de identidad. b) Implementar controles de acceso para evitar la manipulación de sistema y aplicaciones del equipo. c) Implementar controles de acceso para prevenir la lectura de datos del almacén del dispositivo y alteración de los mismos. d) Implementar controles de acceso para contrarrestar la manipulación de datos de control de comandos del objeto inteligente. e) Implementar técnicas de control de acceso para evitar la manipulación de paquetes de actualización del dispositivo, y mitigar el riesgo de los	a) Verificar autenticación del dispositivo utilizando seguridad de capa de transporte (TLS) o IPSec. para prevenir la suplantación de identidad. b) Comprobar el uso de clave encriptado en los dispositivos que no pueden controlar la criptografía asimétrica para evitar la manipulación del sistema y aplicaciones del equipo. c) Verificar el cifrado de la memoria del dispositivo, para prevenir la lectura y alteración de la información del mismo. d-e) Verificar el esquema de autorización del dispositivo	a) Pruebas de autenticación del dispositivo para verificar Autorización y Auditoría (AAA): hash, firma digital. b) Pruebas de descifrado de clave del dispositivo, para verificar si el encriptamiento es vulnerable. c) Pruebas de acceso a la memoria del dispositivo para verificar encriptación de la memoria del mismo. d-e) Pruebas de vulneración de la aplicación del dispositivo, para validación de entradas y listas de control de acceso al software del equipo. f-g) Revision de código de aplicaciones, para verificar código cifrado y firmado.

		h) Vulnerabilidades Meltdown y Spectre, ataques a la operación de los procesadores.	componentes del mismo. f) Implementar técnicas de control de acceso para prevenir la divulgación de información del equipo inteligente. g) Implementar controles para mitigar la elevación de privilegios en el acceso a los dispositivos. h) Implementar medidas para contrarrestar ataques Meltdown y Spectre.	para contrarrestar la manipulación de datos de control de comandos y los paquetes de actualización del dispositivo para mitigar el riesgo de los componentes del mismo. f-g) Verificar aplicación de técnicas de codificación de cifrado y firmas en el software para prevenir la divulgación de información y elevación de privilegios en los equipos inteligentes. h) Verificar la implementación de parches de seguridad para contrarrestar ataques Meltdown y Spectre.	h) Pruebas de penetración ataques Meltdown y Spectre, para verificar si el procesador ha sido parchado contra estos tipos de riesgos de seguridad.
3	ENLACES DE COMUNICACIÓN	a) Desvío de tráfico en las rutas de trasmisión entre el dispositivo y la plataforma de servicios en la nube, mediante ataques de Hombre en el medio de la comunicación, invalida parcialmente la difusión, suplantando al dispositivo o usuario que origina el envío de información. b) Alteración de la información, una vez que el atacante ha interceptado la comunicación, puede modificar parte del contenido de la misma. c) Divulgación de la información, ya con la comunicación interceptada, el ciberdelincuente, puede acceder a la información sin estar autorizado ni autenticado. d) Ataques de denegación de servicios con	a) Implementar medidas de control, a fin de proteger la puerta de enlace para prevenir vulneraciones y desvío de información. b) Implementar técnicas de control de acceso para prevenir ataques y la alteración de la información. c) Implementar medidas de control de acceso para evitar la divulgación de la información. d) Implementar técnicas de control para mitigar ataques de denegación de servicios.	a) Verificar aplicación de seguridades del protocolo MQTT Transporte de telemetría de cola del mensaje. El mismo que verifica que está conectado el cliente autorizado, autenticando el certificado de cliente con el protocolo SSL o autenticando la identidad del cliente con una contraseña, para prevenir ataques y desvíos de información. b) Verificar aplicación de un algoritmo de clave público / privado completo como RSA (River, Shamir, Adleman), para prevenir ataques y la	a) Pruebas de checksum en envío de mensajes MQTT Transporte de telemetría de cola del mensaje. Para verificar certificados SSL. b) Pruebas de códigos de autenticación MAC. c) Pruebas de interceptación de la comunicación para verificar cifrado de tráfico. d) Pruebas de emparejamiento de dispositivos con LE NFC para verificar si es vulnerable a ataques de denegación de servicios.

		ello el atacante evita el envío de información a su plataforma de destino.		alteración de la información. c) Verificar cifrado de tráfico en el transporte de datagrama de capa segura, DTLS, para la interceptación de la comunicación para la divulgación de la información. d) Verificar la aplicación de técnicas de emparejamiento seguro de la entidad externa con el dispositivo LE NFC o Bluetooth, para control del panel operativo del dispositivo, a través de una puerta de enlace de campo o en la nube, actuando solo como clientes hacia la red IoT, para mitigar ataques de denegación de servicios.	
4	PLATAFORMAS EN LA NUBE	a) Administración de identidad y credenciales insuficientes para el control de acceso a las plataformas en la nube. b) Interfaces de usuario y de programación de aplicaciones inseguras y estas se utilizan para interactuar con los servicios en la nube. c) Vulnerabilidades de los componentes del sistema operativo en la plataforma en la nube, ponen en riesgo la seguridad de la información y servicios Cloud. d) Amenazas internas en la red Cloud, usuarios administradores inescrupulosos, pueden hacer mal uso de la información confidencial a la que tienen acceso. e) Amenazas persistentes avanzadas, ataque cibernético que establece un punto de interceptación en la red Cloud, una vez	a) Implementar controles de acceso para administración de identidad y credenciales para el acceso autorizado a las plataformas en la nube. b) Implementar controles de acceso a las interfaces de usuario y de programación de aplicaciones de los servicios en la nube, para mitigar los riesgos de seguridad. c) Implementar técnicas de control para evitar vulnerabilidades de los componentes del sistema operativo en las plataformas Cloud. d) Tomar acciones por parte de los proveedores de servicios Cloud, para mitigar las amenazas internas en las redes y plataformas en la nube.	a-b) Verificar autenticación de la puerta de enlace de campo en la puerta de enlace en la nube con certificado PSK basado en notificación utilizando TLS RSA/PSK, IPSec, en la administración de identidad y credenciales para el acceso autorizado a las plataformas Cloud y las interfaces de programación de aplicaciones y de usuarios de los servicios en la nube, para mitigar los riesgos de seguridad. c) Verificar que se haya implementado una partición de	a-b) Pruebas de autenticación en la puerta de enlace en la nube para verificar certificados PSK basado en notificación TLS RSA/PSK, IPSec, en el acceso a plataformas Cloud y las interfaces de programación de aplicaciones Cloud. c) Pruebas de verificación de particiones de sistema operativo, una solo de lectura, pruebas de penetración para verificar cifrado y firma de imagen del sistema operativo la plataforma en la nube. d-g) Verificar políticas de seguridad de los proveedores de

		instaladas se mezclan con el tráfico normal para el robo de información. f) Perdida de datos en los servicios de hosting en la nube, por fenómenos naturales o errores internos del proveedor de servicios en la nube. g) Vulnerabilidades de tecnología compartida, se da por la compartición de infraestructura y plataformas en la nube por parte de los proveedores de servicios cloud, que pueden ser explotadas por terceros que acceden a esta infraestructura.	e) Implementar medidas de control para mitigar amenazas persistentes avanzadas, para evitar el robo de información. f) Tomar acciones para mitigar la perdida de información de los servicios de hosting en la nube, por fenómenos naturales. g) Tomar acciones por parte de los proveedores de servicio para reducir las vulnerabilidades en tecnología e infraestructura Cloud compartida.	sistema operativo de solo lectura, imagen de sistema operativo firmada, y cifrada, para evitar alteración de los componentes del sistema operativo de la plataforma de servicios en la nube. d-g) Impulsar el establecimiento de políticas de seguridad para la interconexión de infraestructura Cloud de los proveedores de estos servicios, para mitigar las amenazas internas en las redes, infraestructura y plataformas en la nube compartidas. e) Verificar la ejecución de listas blancas de aplicaciones para mitigar amenazas persistentes avanzadas, para evitar software malicioso y programas no autorizados que facilitan el robo de información en las plataformas de Cloud. f) Verificar si se dispone de sitios alternos de los Data Centers de los proveedores de servicios Cloud, para mitigar la perdida de información de los servicios de hosting en la nube causados por fenómenos naturales.	servicios Cloud para la interconexión y compartición de infraestructura Cloud. e) Pruebas de penetración de seguridad informática en la nube, según recomendaciones de la Alianza de Seguridad en la Nube CSA y el Concejo de Cyber Defensa CDC, para verificar cifrado de tráfico, considerando inclusive los nuevos ataques. f) Constatar sitios alternos de los Data Centers de los proveedores de servicios Cloud, en caso de requerir contingencia de servicios principales.

5	APLICACIONES EN LA NUBE	a) Administración de identidad y credenciales insuficientes para el control de acceso a las aplicaciones en la nube. b) Violación de datos de las aplicaciones c) Interfaces de aplicaciones de usuario inseguras. d) Secuestro de sesiones de aplicaciones de usuarios. e) Ataques de denegación a las aplicaciones en la nube, forzando a los servicios Cloud a consumir exceso de recursos: procesamiento, memoria, almacenamiento, ralentizando el sistema, dejando a los usuarios del sistema sin acceso a los servicios.	a) Implementar controles de acceso de identidad y credenciales de acceso autorizado a las aplicaciones en la nube. b) Implementar técnicas de control para mitigar la violación de datos de las aplicaciones. c) Implementar controles de acceso en las interfaces de aplicación de usuario. d) Implementar controles de acceso para evitar vulneraciones y secuestro de sesiones en las aplicaciones de usuarios. e) Tomar acciones para mitigar ataques de denegación a las aplicaciones en la nube.	a-c-d) Verificar la autenticación con TLS (PSK/RSA) para cifrar el tráfico y acceso autorizado a las interfaces de usuario en las aplicaciones en la nube, para evitar vulneración y secuestro de sesiones. b) Verificar la aplicación de cifrado de almacenamiento, firma de los registros de datos, para mitigar la violación de datos de las aplicaciones. e) Verificar gestión de seguridad en el nivel de protocolo (MQTT/AMQP/HTTP/CoAP), con control de acceso seguro a través de listas de control de acceso (ACL) a los recursos o permisos, para mitigar ataques de denegación a las aplicaciones en la nube.	a-c-d) Pruebas de autenticación de las aplicaciones de usuario para verificar cifrado TLS (PSK/RSA) emisión de certificados y firmas credenciales de acceso. b) Pruebas de penetración de seguridad de aplicaciones en la nube, según recomendaciones de la Alianza de Seguridad en la Nube CSA y el Concejo de Ciber Defensa CDC, para verificar cifrado de tráfico, considerando inclusive los nuevos ataques. e) Revisión de código de aplicaciones en la nube, para verificar código cifrado y firmado.