Seguridad informática del Internet de las cosas (IoT) con AWS

Adopción segura de la nube

Abril de 2019

Avisos

Este documento se suministra únicamente con fines informativos. Representa las ofertas y prácticas actuales de AWS a partir de la fecha de publicación de este documento, y pueden modificarse sin previo aviso. Los clientes son responsables de realizar sus propias evaluaciones independientes de la información contenida en este documento y de cualquier uso de los productos o servicios de AWS, cada uno de los cuales se ofrece “tal cual”, sin garantía de ningún tipo, ya sea expresa o implícita. Mediante este documento no se genera ninguna garantía, declaración, compromisos contractuales, condición ni certeza por parte de AWS, sus filiales, proveedores o licenciantes. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

Contenido

Finalidad

Este documento técnico ofrece una descripción detallada de los servicios del Internet de las cosas (IoT) que proporcionan funciones de seguridad informática. Los clientes pueden sacar partido de estos servicios en la nube de AWS. Está dirigido a propietarios de programas de nivel sénior, responsables de toma de decisiones y profesionales de la seguridad informática que se estén planteando la adopción segura de soluciones del IoT por parte de la empresa.

Introducción

La tecnología IoT permite que las compañías optimicen procesos, mejoren las ofertas de productos y transformen la experiencia de los clientes de distintos modos. Aunque los líderes empresariales están entusiasmados con la forma en que sus negocios pueden beneficiarse de esta tecnología, siguen existiendo inquietudes sobre la seguridad informática, los riesgos y la privacidad. Esto se debe, en parte, al conflicto con ofertas de seguridad informática dispares, incompatibles y a veces aún poco desarrolladas que no logran proteger adecuadamente las implementaciones, lo que genera un mayor riesgo para los datos del cliente o del propietario de la empresa.

Las compañías anhelan prestar servicios inteligentes que puedan mejorar drásticamente la calidad de vida de las poblaciones, las operaciones y la inteligencia empresarial, la calidad de la atención a los proveedores de servicios, la resiliencia de las ciudades inteligentes, la sostenibilidad medioambiental y una serie de escenarios aún por imaginar. Más recientemente, AWS ha visto un aumento en la adopción del IoT por parte del sector sanitario y de los ayuntamientos, y se espera que otras industrias se sumen en corto plazo. Muchos ayuntamientos han sido pioneros y están tomando la iniciativa cuando se trata de integrar tecnologías modernas, como el IoT. Por ejemplo:

- **Kansas City, Misuri:** Kansas City ha creado una plataforma unificada para su ciudad inteligente con el fin de administrar los nuevos sistemas que operan los corredores del tranvía de la ciudad. Los sensores de vídeo, los detectores de tráfico, el alumbrado público conectado, una red wifi pública y la gestión del estacionamiento y el tráfico han ayudado a lograr una reducción del 40% en costes energéticos, un nuevo plan de desarrollo de la zona céntrica de 1700 millones de USD y 3247 nuevas unidades residenciales.
- **Ciudad de Chicago, Illinois:** Chicago está instalando sensores y cámaras en intersecciones para medir los niveles de polen y controlar la calidad del aire.
- **Ciudad de Catania, Italia:** Catania ha desarrollado una aplicación que indica a quienes acuden al trabajo dónde está la plaza de estacionamiento libre más cercana de camino a su destino.
- **Ciudad de Recife, Brasil:** Recife ha colocado dispositivos de seguimiento en todos los camiones de recogida de residuos y carros de limpieza. Esto ha permitido a la ciudad ahorrar 250 000 USD al mes en costes de limpieza y, a la vez, ha mejorado la fiabilidad del servicio y la eficiencia operativa.
- **Ciudad de Newport en Gales, Reino Unido:** Newport ha implementado soluciones IoT para convertirse en una ciudad inteligente y mejorar la calidad del aire, el control de inundaciones y la gestión de residuos en unos pocos meses.

- **Yakarta, Indonesia:** Yakarta, una ciudad de 28 millones de residentes que a menudo sufre inundaciones, aprovecha el IoT para medir los niveles de agua en canales y tierras bajas, y utiliza las redes sociales para conocer la opinión de los ciudadanos. También puede avisar anticipadamente a los barrios en peligro para que las autoridades y los equipos de servicio de respuesta rápida sepan qué áreas necesitan más ayuda, y así puedan coordinar el proceso de evacuación.

Según Machina Research, el mercado global del IoT alcanzará los 4,3 billones de dólares en 2024[1]. Según el informe del Departamento de Innovación y Aptitudes Empresariales del Reino Unido, el mercado global de soluciones de ciudades inteligentes y los servicios adicionales necesarios para implementarlas se estima que será de 408 mil millones de dólares para 2020[2]. Además, Forbes[3] estima que "el mantenimiento predictivo, la producción auto-optimizadora y la gestión automatizada de inventarios son los tres casos de uso principales que impulsarán el crecimiento del mercado del IoT hasta 2020". Forbes afirma que a las empresas les interesa beneficiarse de la existencia de proveedores de TI establecidos y experimentados, con una infraestructura fiable, para crear o implementar soluciones del IoT debido a la gran repercusión que tienen en los clientes.

Aunque los clientes anhelan aprovechar las oportunidades de negocio disponibles gracias al IoT, históricamente no ha quedado claro si es posible adoptar de forma segura el IoT. Las características y servicios que permiten estas soluciones no siempre han sido seguros por defecto, lo que ha dejado posibles brechas de seguridad informática en las bases arquitectónicas. Además, las actualizaciones y el mantenimiento no se han automatizado en prácticas esenciales como es el caso de las comunicaciones cifradas y las actualizaciones inalámbricas (por su sigla inglesa "OTA"). Por último, pocos proveedores han ofrecido la posibilidad de aplicar parches a los dispositivos y gateways de forma remota tras la implementación, lo que deja a estos dispositivos vulnerables frente a nuevos riesgos de seguridad informática.

En cambio, AWS se toma muy en serio la seguridad informática y ofrece varias opciones de requisitos de privacidad y confidencialidad de datos a millones de clientes activos pertenecientes a una amplia gama de industrias y geografías. AWS invierte una gran cantidad de recursos para garantizar que se incluya la seguridad informática en cada capa de sus servicios, extendiéndola a dispositivos con IoT. Ayudar a proteger la confidencialidad, la integridad y la disponibilidad de los sistemas y datos de los clientes y, a la vez, proporcionar una plataforma segura, escalable y fiable para las soluciones del IoT representa una prioridad para AWS.

Retos de seguridad informática

Los riesgos y fallos de seguridad informática pueden comprometer la seguridad y privacidad de la información de los clientes en una aplicación de IoT. Junto con el creciente número de dispositivos y de datos generados, el potencial de daño plantea dudas sobre cómo abordar los riesgos de seguridad informática que suponen los dispositivos IoT y su comunicación con la nube.

[1] Por https://machinaresearch.com/news/the-global-iot-market-opportunity-will-reach-usd43-trillion-by-2024

[2] Véase https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/249423/bis-13-1217 - smart-city-market-opportunties-uk.pdf

[3] Véase https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by - 2020 / #74c8f8c7609b

Las inquietudes comunes de los clientes con respecto a los riesgos se centran en la seguridad y el cifrado de datos durante el tránsito entre el dispositivo y la nube o el tránsito entre los servicios perimetrales y el dispositivo, junto con la aplicación de parches, la autenticación de dispositivos y usuarios y el control de acceso. La seguridad informática en los dispositivos IoT es esencial, no solo para mantener la integridad de la información, sino también para proteger contra ataques que pueden afectar a la fiabilidad de los dispositivos. Dado que los dispositivos pueden enviar grandes cantidades de datos confidenciales a través de Internet y que los usuarios finales pueden controlar directamente el dispositivo, la seguridad de las "cosas" debe extenderse a todas las capas de la solución.

Las noticias sobre filtración de datos llevan a la seguridad informática del IoT a un escrutinio adicional por parte de los clientes, pero nos ofrecen la oportunidad de aprender de estas lecciones y fomentar mejores prácticas. La base de una solución del IoT debe comenzar y terminar con la seguridad informática, junto con el uso de servicios capaces de comprobar continuamente las configuraciones de IoT[4] para garantizar que no dejen de seguir las prácticas recomendadas de seguridad informática. Una vez que se detecta una desviación, deben generarse alertas para que se puedan implementar las medidas correctivas apropiadas, idealmente, de forma automática.

Para mantenerse al día con la aparición de dispositivos en el mercado, así como con las futuras amenazas en línea, lo mejor es implementar servicios que aborden cada parte del ecosistema del IoT y se superpongan para asegurar, proteger, controlar, reparar y administrar implementaciones de flotas de dispositivos IoT (con o sin conexión a la nube).

¿Cómo están abordando los Gobiernos la seguridad informática del IoT?

Mientras que las organizaciones del sector privado están implementando activamente el IoT en casos de uso como la sanidad, la construcción industrial y los bienes de consumo de baja potencia, los gobiernos a nivel nacional y local están empezando a abordar la adopción y la seguridad informática del IoT (véase el Apéndice 2). Además de evaluar el futuro panorama de políticas sobre IoT, AWS continúa añadiendo servicios a varios marcos de conformidad para ayudar a que los clientes cumplan con sus obligaciones (véase el Apéndice 3).

Servicios y capacidades de la seguridad informática del IoT de AWS

AWS ofrece un conjunto de servicios de IoT para ayudar a los clientes a proteger sus dispositivos, conectividad y datos. Estos servicios permiten a los clientes aprovechar la seguridad de extremo a extremo, desde la protección del dispositivo hasta los datos en tránsito y en reposo. También proporcionan características de seguridad informática que permiten la aplicación y ejecución de las políticas de seguridad necesarias para cumplir con la marca de agua de seguridad.

[4] Una configuración es un conjunto de controles técnicos que los clientes establecen para ayudar a mantener la información a salvo cuando los dispositivos se comunican entre ellos y con la nube.

AWS IoT proporciona una funcionalidad amplia y profunda; los clientes pueden crear soluciones del IoT para prácticamente cualquier caso de uso en una amplia gama de dispositivos. AWS IoT se integra con los servicios de inteligencia artificial (AI) para que los clientes puedan hacer que los dispositivos sean más inteligentes, incluso sin conexión a Internet. Desarrollado en la nube de AWS y utilizado por millones de clientes en 190 países, AWS IoT puede adaptarse fácilmente a medida que las flotas de dispositivos de los clientes crecen y los requisitos de sus negocios evolucionan. AWS IoT también ofrece funciones de seguridad integrales para que los clientes puedan crear políticas de seguridad preventivas y responder de forma inmediata a posibles problemas de seguridad informática.

AWS IoT proporciona servicios en la nube y software perimetral, lo que permite a los clientes conectar dispositivos de forma segura, recopilar datos y realizar acciones inteligentes localmente, incluso cuando no tienen conexión a Internet. Los servicios en la nube permiten a los clientes integrar y conectar de forma rápida y segura flotas grandes y diversas; mantener la flota segura y en buen estado; y detectar y responder ante eventos en sensores y aplicaciones de IoT. Para acelerar el desarrollo de aplicaciones de IoT, los clientes pueden conectar dispositivos y servicios web con facilidad mediante una interfaz de arrastrar y colocar. AWS IoT también se puede utilizar para analizar datos y crear modelos sofisticados de aprendizaje automático (ML). Estos modelos se pueden implementar en la nube o en dispositivos del cliente para hacerlos más inteligentes.

Si bien los servicios actuales de AWS IoT[5] abarcan mucho para permitir soluciones de IoT innovadoras y completas, este documento técnico se centra en los cinco servicios siguientes, que son esenciales para la seguridad informática del IoT. La descripción de los servicios y las características de seguridad informática se analizan con más detalle a continuación.

- **Amazon FreeRTOS** es un sistema operativo de código abierto para microcontroladores que facilita la programación, implementación, seguridad, conexión y gestión de dispositivos perimetrales pequeños de baja potencia.
- **AWS IoT Greengrass** es un software que permite a los clientes ejecutar capacidades locales de computación, mensajería, almacenamiento en caché de datos, sincronización e inferencia de ML en dispositivos conectados.
- **AWS IoT Core** es un servicio administrado en la nube que permite a los dispositivos conectados interactuar de forma fácil y segura con aplicaciones en la nube y otros dispositivos.
- **AWS IoT Device Management** es un servicio de administración de dispositivos basado en la nube que facilita la integración, organización, supervisión y administración remota de dispositivos IoT de forma segura a escala.
- **AWS IoT Device Defender** es un servicio de seguridad de IoT que supervisa y controla continuamente las configuraciones de IoT de los clientes para garantizar que no dejen de cumplir con las prácticas recomendadas de seguridad informática.

[5] Los servicios de AWS IoT incluyen Amazon FreeRTOS, AWS IoT Greengrass, AWS IoT Core, AWS IoT Device Management, AWS IoT Device Defender, AWS IoT Things Graph, AWS IoT Analytics, AWS IoT SiteWise y AWS IoT Events. Para obtener más información, visite https://aws.amazon.com/IoT

Amazon FreeRTOS: software para dispositivos

Descripción general del servicio: Amazon FreeRTOS (a:FreeRTOS) es un sistema operativo de código abierto para microcontroladores[6] que facilita la programación, implementación, seguridad, conexión y gestión de dispositivos perimetrales pequeños de baja potencia. Amazon FreeRTOS se basa en el kernel FreeRTOS, un popular sistema operativo de código abierto para microcontroladores, y lo amplía con bibliotecas de software que facilitan la conexión segura de dispositivos pequeños y de baja potencia de los clientes directamente a los servicios en la nube de AWS, como AWS IoT Core, o a dispositivos perimetrales más potentes que estén ejecutando AWS IoT Greengrass.

Funciones de seguridad informática: Amazon FreeRTOS incluye bibliotecas para ayudar a proteger los datos y las conexiones de los dispositivos, así como compatibilidad con el cifrado de datos y la gestión de claves. Amazon FreeRTOS incluye compatibilidad con Transport Layer Security (TLS v1.2) para ayudar a los dispositivos a conectarse de forma segura a la nube. Amazon FreeRTOS también tiene una función de firma de código para garantizar que el código del dispositivo del cliente no se vea vulnerado durante la implementación, así como capacidades para que las actualizaciones de OTA puedan actualizar dispositivos de forma remota con mejoras de características o parches de seguridad.

AWS IoT Greengrass: software para computación perimetral

Descripción general del servicio: AWS IoT Greengrass es un software que permite a los clientes ejecutar capacidades locales de computación, mensajería, almacenamiento en caché de datos, sincronización e inferencia de ML en dispositivos conectados[7], lo que permite que funcionen incluso con conectividad intermitente a la nube. Una vez que el dispositivo se vuelve a conectar, AWS IoT Greengrass sincroniza los datos del dispositivo con AWS IoT Core, proporcionando así una funcionalidad constante sin depender de la conectividad. AWS IoT Greengrass amplía sin dificultades AWS a los dispositivos para que puedan actuar de forma local sobre los datos que generan y, al mismo tiempo, utilizar la nube para gestión, análisis y almacenamiento duradero.

Funciones de seguridad informática: AWS IoT Greengrass autentica y cifra los datos de los dispositivos tanto para comunicaciones locales como en la nube, y nunca se intercambian datos entre los dispositivos y la nube sin comprobar primero la identidad. El servicio utiliza una administración de seguridad y acceso informáticos similares a los que los clientes ya conocen por AWS IoT Core, con autenticación y autorización mutua de dispositivos y conexión segura a la nube.

---

[6] Un microcontrolador es un solo chip que contiene un sencillo procesador que se puede encontrar en muchos dispositivos, como electrodomésticos, monitores de actividad, sensores industriales de automatización y automóviles. Muchos de estos pequeños dispositivos podrían tener la ventaja de conectarse a la nube o localmente a otros dispositivos. Por ejemplo, los contadores de electricidad inteligentes necesitan conectarse a la nube para informar sobre el consumo y los sistemas de seguridad de los edificios necesitan comunicarse localmente para que las puertas se abran cuando alguien utilice su tarjeta identificativa.

[7] Para empezar a utilizar AWS IoT Greengrass, los clientes necesitarán un dispositivo capaz de ejecutar el núcleo de AWS IoT Greengrass. Existe una lista completa de dependencias técnicas y dispositivos cualificados aquí. Haga clic aquí para obtener una guía práctica de introducción. Los clientes pueden encontrar la referencia detallada del desarrollador aquí.

Más específicamente, AWS IoT Greengrass utiliza certificados X.509[8], suscripciones administradas, políticas de AWS IoT y políticas y roles de AWS Identity and Access Management (IAM) para garantizar que las aplicaciones Greengrass de AWS IoT sean seguras. Los dispositivos de AWS IoT requieren una cosa de AWS IoT, un certificado de dispositivo y una política de AWS IoT para conectarse al servicio AWS IoT Greengrass. Esto permite que los dispositivos principales de AWS IoT Greengrass se conecten de forma segura al servicio en la nube de AWS IoT. También permite al servicio en la nube de AWS IoT Greengrass implementar información de configuración, funciones de AWS Lambda y suscripciones administradas en los dispositivos principales de AWS IoT Greengrass. Además, AWS IoT Greengrass proporciona almacenamiento de claves privadas en hardware de confianza para dispositivos perimetrales.

Otras capacidades de seguridad importantes de AWS IoT Greengrass son la supervisión y el inicio de sesión. Por ejemplo, el software principal del servicio puede escribir registros en Amazon CloudWatch[9] (que también funciona para AWS IoT Core) y en el sistema de archivos local de los dispositivos principales de los clientes.

El registro se configura en el nivel de grupo y todas las entradas de registro de AWS IoT Greengrass incluyen una marca de tiempo, nivel de registro e información sobre el evento. AWS IoT Greengrass está integrado con AWS CloudTrail[10], un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en AWS IoT Greengrass y, si el cliente lo activa, captura como eventos todas las llamadas de la interfaz de programación de aplicaciones (API) para AWS IoT Greengrass. Esto incluye llamadas desde la consola de AWS IoT Greengrass y llamadas de código a las operaciones de la API de AWS IoT Greengrass. Por ejemplo, los clientes tienen la posibilidad de crear un registro, mientras que las llamadas pueden continuar con la transmisión de eventos de AWS CloudTrail a un bucket de Amazon Simple Storage Service (Amazon S3), incluidos eventos para AWS IoT Greengrass. Si los clientes no desean crear un registro, pueden ver los eventos más recientes en el historial de eventos de la consola de AWS CloudTrail (si la opción está habilitada). Esta información se puede utilizar con varios fines, como determinar cuándo se realizó una solicitud a AWS IoT Greengrass y la dirección IP desde la que se efectuó.

Existen prácticas recomendadas para proteger los datos de los clientes en el dispositivo y deben utilizarse siempre que sea posible. Para AWS IoT Greengrass, todos los dispositivos IoT deben permitir el cifrado de disco completo y seguir las prácticas recomendadas de administración de claves. Los clientes pueden utilizar el cifrado de disco completo mediante el uso de claves AES de 256 bits basadas en algoritmos FIPS 140-2 validados por el NIST[11] y seguir las prácticas recomendadas de administración de claves. Para dispositivos de baja potencia como los que

[8] Los certificados X.509 son certificados digitales que utilizan el estándar de infraestructura de clave pública X.509 para asociar una clave pública con una identidad contenida en un certificado. Los certificados X.509 son emitidos por una entidad de confianza denominada entidad emisora de certificados (CA). La CA administra uno o más certificados especiales llamados certificados de CA, que utiliza para generar certificados X.509. Solo la autoridad de certificación tiene acceso a los certificados de CA. Consulte https://docs.aws.amazon.com/iot/latest/developerguide/x509-certs.html para más información.

[9] Véase https://aws.amazon.com/cloudwatch.

[10] Véase https://aws.amazon.com/cloudtrail.

[11] NIST FIPS 140-2 Approved Cryptographic Algorithms: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402annexa.pdf.

utilizan Amazon FreeRTOS, los clientes pueden seguir las recomendaciones de criptografía[12] ligera 8114 del NIST.

Las secciones anteriores abarcaban microcontroladores y casos de uso de dispositivos perimetrales. A continuación, el documento se centrará en los servicios del IoT que operan en la nube.

AWS IoT Core: gateway del IoT basado en la nube

Descripción general del servicio: AWS IoT Core es un servicio administrado en la nube que permite a los dispositivos conectados interactuar de forma fácil y segura con aplicaciones en la nube y otros dispositivos. AWS IoT Core proporciona comunicación segura y procesamiento de datos en diferentes tipos de dispositivos y ubicaciones conectados para que los clientes puedan desarrollar fácilmente aplicaciones IoT. Entre los ejemplos de caso de uso de clientes están las soluciones industriales y domésticas conectadas, con capacidad para miles de millones de dispositivos y miles de millones de mensajes que se pueden procesar y redirigir a puntos de enlace de AWS y a otros dispositivos de forma fiable y segura.

Capacidades de seguridad informática: AWS IoT Core ofrece una serie de soluciones a los clientes que ayudan a habilitar y mantener la seguridad informática. Los mecanismos de seguridad de la nube de AWS protegen los datos a medida que se transmiten entre AWS IoT y otros dispositivos o servicios de AWS. Los dispositivos pueden conectarse utilizando una variedad de opciones de identidad (certificados X.509, usuarios y grupos de IAM, identidades de Amazon Cognito o tokens de autenticación personalizados) a través de una conexión segura. Los clientes realizan las validaciones del lado del cliente (es decir, validación de cadena de confianza, verificación del nombre de host, almacenamiento seguro y distribución de sus claves privadas), mientras que AWS IoT Core proporciona canales seguros de transmisión mediante TLS. El motor de reglas de AWS IoT también reenvía datos de dispositivos a otros dispositivos y servicios de AWS de acuerdo con las reglas definidas por el cliente. Los sistemas de administración de acceso de AWS se utilizan para transferir datos de forma segura a su destino final. Otra característica de autorización de AWS IoT que vale la pena destacar son las variables de políticas de AWS IoT, que ayudan a evitar el aprovisionamiento de credenciales con privilegios excesivos en un dispositivo. Estas características, que se utilizan junto con las prácticas recomendadas generales de ciberseguridad, sirven para proteger los datos de los clientes.

AWS IoT Device Management: servicio de administración de dispositivos IoT basado en la nube

Descripción general del servicio: AWS IoT Device Management ayuda a los clientes a integrar, organizar, supervisar y administrar de forma remota dispositivos IoT a escala. AWS IoT Device Management se integra con AWS IoT Core para conectar fácilmente dispositivos a la nube y a otros dispositivos, de modo que los clientes puedan gestionar de forma remota sus flotas de dispositivos. AWS IoT Device Management ayuda a los clientes a integrar nuevos dispositivos mediante el uso de AWS IoT en la consola de administración de AWS o en una API, para cargar plantillas que rellenan con información como el fabricante del dispositivo y el número de serie,

[12] NIST 8114 – Lightweight Cryptography: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf.

certificados de identidad X.509 o políticas de seguridad informática. Con esta información, los clientes pueden configurar toda la flota de dispositivos con unos pocos clics en AWS IoT dentro de la consola de administración de AWS.

Capacidades de seguridad informática: con AWS IoT Device Management, los clientes pueden agrupar su flota de dispositivos en una estructura jerárquica basada en funciones, requisitos de seguridad informática o categorías similares. Pueden agrupar un solo dispositivo en una habitación, varios dispositivos en el mismo piso o todos los dispositivos que operan dentro de un edificio. Estos grupos se pueden utilizar para administrar políticas de acceso, ver métricas operativas o realizar acciones que afecten a todo el grupo. Además, una función conocida como "Dynamic Things" puede agregar automáticamente dispositivos que cumplan los criterios definidos por el cliente y eliminar aquellos que ya no cumplan los requisitos. Esto optimiza el proceso de forma segura y al mismo tiempo mantiene la integridad operativa. Dynamic Things también facilita la búsqueda de registros de dispositivos basados en cualquier combinación de atributos de dispositivo y permite a los clientes realizar actualizaciones por lote.

Con AWS IoT Device Management, los clientes también pueden instalar software y firmware en los dispositivos en el terreno para corregir vulnerabilidades de seguridad informática y mejorar la funcionalidad del dispositivo; ejecutar actualizaciones por lote; controlar la velocidad de implementación; establecer umbrales de errores; y definir trabajos continuos para actualizar el software del dispositivo automáticamente, de modo que siempre estén ejecutando la versión más reciente del software. Los clientes pueden enviar acciones de forma remota, como reinicios de dispositivos o reinicios de fábrica, para solucionar errores de software y restablecer los parámetros originales del dispositivo. También pueden firmar digitalmente archivos que se envían a sus dispositivos, lo que ayuda a garantizar que estos no se vean comprometidos.

La capacidad de enviar actualizaciones de software no se limita a los servicios en la nube. De hecho, los trabajos de actualización de OTA en Amazon FreeRTOS permiten a los clientes utilizar AWS IoT Device Management para programar actualizaciones de software. Del mismo modo, los clientes también pueden crear un trabajo de actualización básica de AWS IoT Greengrass para uno o más dispositivos de núcleo de AWS IoT Greengrass mediante AWS IoT Device Management, con el fin de implementar actualizaciones de seguridad informática, correcciones de errores y nuevas características de AWS IoT Greengrass para los dispositivos conectados.

AWS IoT Device Defender: servicio de seguridad informática de dispositivos IoT basado en la nube

Descripción general del servicio: AWS IoT Device Defender es un servicio totalmente administrado que ayuda a los clientes a auditar las características de seguridad establecidas para su flota de dispositivos IoT. El servicio controla continuamente las configuraciones de IoT para garantizar que no se desvíen de las prácticas recomendadas de seguridad informática y asegurarse de que se mantienen. Algunas de estas prácticas consisten en garantizar la identidad de los dispositivos, autenticar y autorizar dispositivos, y cifrar los datos que

contienen. El servicio puede enviar una alerta si hay brechas en la configuración de IoT de un cliente que pueda crear un riesgo para la seguridad informática, como certificados de identidad compartidos por varios dispositivos o un dispositivo con un certificado de identidad revocado que intente conectarse a AWS IoT Core.

Capacidades de seguridad informática: además de las capacidades de supervisión y control del servicio, los clientes pueden configurar alertas que tomen medidas para corregir cualquier desviación que se encuentre en los dispositivos. Por ejemplo, los picos en el tráfico saliente pueden indicar que un dispositivo está participando en un ataque de denegación de servicio distribuido (DDoS). AWS IoT Greengrass y Amazon FreeRTOS también se integran automáticamente con AWS IoT Device Defender para proporcionar métricas de seguridad informática de los dispositivos para su evaluación.

AWS IoT Device Defender puede enviar alertas a AWS IoT, Amazon CloudWatch y Amazon Simple Notification Service (Amazon SNS), con publicación de alertas en métricas de Amazon CloudWatch. Si un cliente decide abordar una alerta, puede utilizarse AWS IoT Device Management para llevar a cabo medidas de atenuación, como la ejecución de reparaciones de seguridad informática.

AWS IoT Device Defender controla las configuraciones de IoT asociadas con los dispositivos del cliente en función de un conjunto de prácticas recomendadas de seguridad informática de IoT definidas para que los clientes puedan ver dónde existen brechas de seguridad y ejecutar auditorías de forma continua o ad hoc. Asimismo, existen prácticas de seguridad informática en AWS IoT Device Defender que se pueden seleccionar y ejecutar como parte de la auditoría. Este servicio también se integra con otros servicios de AWS, como Amazon CloudWatch y Amazon SNS: para enviar alertas de seguridad a AWS IoT cuando se produzca un error en una comprobación o cuando se detecten anomalías de comportamiento para que los clientes puedan investigar y determinar la causa principal. Por ejemplo, AWS IoT Device Defender puede alertar a los clientes cuando las identidades de los dispositivos acceden a API sensibles. AWS IoT Device Defender también puede recomendar acciones que minimicen el impacto de problemas de seguridad informática, como revocar permisos, reiniciar un dispositivo, restablecer los valores predeterminados de fábrica o transmitir correcciones de seguridad a cualquiera de los dispositivos conectados de los clientes.

Los clientes también pueden estar preocupados por agentes malintencionados ya que los errores humanos o sistémicos y los usuarios autorizados con malas intenciones pueden iniciar configuraciones que tengan un impacto negativo en la seguridad informática. AWS IoT Core proporciona los componentes básicos de seguridad informática para que los clientes puedan conectar dispositivos de forma segura a la nube y a otros dispositivos. Los componentes básicos permiten aplicar controles de seguridad informática como autenticación, autorización, registros de auditoría y cifrado de extremo a extremo. A continuación, AWS IoT Device Defender entra en juego y ayuda a auditar de forma constante las configuraciones de seguridad informática, de modo que se garantice el cumplimiento de las prácticas recomendadas de seguridad informática y las políticas de seguridad de la organización de los clientes.

Explotación de la seguridad demostrable para mejorar el IoT: un diferenciador del sector

AWS está creando nuevos servicios y tecnologías de seguridad informática para ayudar a las empresas a proteger sus IoT y dispositivos perimetrales. En concreto, hace poco AWS puso en marcha comprobaciones en AWS IoT Device Defender gracias a la tecnología de inteligencia artificial conocida como razonamiento automatizado, que aprovecha pruebas matemáticas para verificar que el software esté escrito correctamente y determinar si existe acceso no deseado a los dispositivos. AWS IoT Device Defender es un ejemplo de cómo los clientes pueden utilizar el razonamiento automatizado para proteger sus propios dispositivos. De forma interna, AWS ha utilizado el razonamiento automatizado para verificar la integridad de la memoria del código que se ejecuta en Amazon FreeRTOS y para protegerse contra malware. La inversión en razonamiento automatizado para ofrecer garantías ampliables de software seguro (denominado "seguridad demostrable") permite que los clientes gestionen cargas de trabajo confidenciales en AWS.

AWS Zelkova[13] utiliza el razonamiento automatizado para demostrar que los controles de acceso a los datos de los clientes funcionan según lo previsto. Las comprobaciones de control de acceso en AWS IoT Device Defender cuentan con tecnología Zelkova, que permite a los clientes comprobar que sus datos están protegidos de forma adecuada. Una política de AWS IoT es demasiado permisiva si concede acceso a recursos fuera de la configuración de seguridad informática prevista por el cliente. Los controles con tecnología Zelkova que se encuentran en AWS IoT Device Defender comprueban que las políticas no permitan acciones restringidas por la configuración de seguridad informática del cliente y que los recursos previstos tengan permisos para realizar determinadas acciones.

Otras herramientas automatizadas basadas en el razonamiento han ayudado a proteger las bases de la infraestructura de AWS IoT. Se ha utilizado una herramienta de código abierto llamada CBMC para demostrar la exactitud de Amazon FreeRTOS, lo que proporciona mayor confianza al cliente para ejecutar cargas de trabajo en dispositivos de Amazon IoT. Esto garantiza que ningún atacante pueda obtener o aprovecharse de un acceso no autorizado a Amazon FreeRTOS. Los mecanismos automatizados de control de razonamiento en Amazon FreeRTOS se han integrado continuamente como comprobaciones de actualizaciones realizadas en el sistema operativo. Esto garantiza que cada vez que se realice un cambio de código, se adopten medidas para que los desarrolladores de AWS puedan verificar automáticamente que la memoria del software Amazon FreeRTOS esté a salvo.

Se sigue implementando razonamiento automatizado en una variedad de servicios y características de AWS, lo que proporciona mayores niveles de garantía de seguridad informática para los componentes críticos de la nube de AWS. AWS continúa implementando razonamientos automatizados para desarrollar herramientas para los clientes, así como tecnología de verificación de infraestructura interna para la pila de IoT de AWS.

[13] Para obtener más información sobre Zelkova, visite https://aws.amazon.com/blogs/security/protect-sensitive-data-in-the-cloud-with-automated- reasoning-zelkova

¿Cuáles son las principales prácticas recomendadas para la seguridad informática del IoT?

A pesar del número de prácticas recomendables disponibles, no existe un enfoque único para mitigar los riesgos que se refieren a las soluciones del IoT. En función del dispositivo, sistema, servicio y entorno en el que se implementen los dispositivos, existen diferentes amenazas, vulnerabilidades y tolerancias de riesgo que los clientes deben tener en cuenta. A continuación, se indican las prácticas recomendadas para incorporar seguridad de extremo a extremo en datos, dispositivos y servicios en la nube:

1. **Incorporar seguridad informática en la fase de diseño**
   La base de una solución de IoT comienza y termina con la seguridad informática. Como los dispositivos pueden enviar grandes cantidades de datos confidenciales, y los usuarios finales de las aplicaciones de IoT también pueden controlar directamente un dispositivo, la seguridad informática de las "cosas" es un requisito de diseño generalizado. La seguridad informática no es una fórmula estática; las aplicaciones de IoT deben poder modelar, supervisar e iterar continuamente las prácticas recomendadas de seguridad informática.
   Entre los desafíos para la seguridad informática del IoT existen el ciclo de vida de un dispositivo físico y las limitaciones del hardware de sensores, microcontroladores, actuadores y bibliotecas integradas. Estos factores pueden limitar las capacidades de seguridad informática que cada dispositivo puede realizar.
   Con estas dinámicas adicionales, las soluciones del IoT deben adaptar continuamente su arquitectura, firmware y software para mantenerse a la vanguardia del cambiante panorama de la seguridad informática. Aunque los factores de los dispositivos pueden presentar mayores riesgos, obstáculos y posibles compensaciones entre la seguridad informática y el coste, la creación de una solución del IoT segura debe ser el objetivo principal de cualquier organización.

2. **Aprovechar las estructuras reconocidas de seguridad informática y ciberseguridad**
   AWS fomenta un enfoque abierto, cuyos estándares promueven la implementación segura del IoT. La interoperabilidad es vital a la hora de analizar los miles de millones de dispositivos y puntos de conexión necesarios para apoyar un ecosistema del IoT robusto destinado al uso por parte de los consumidores, la industria y el sector público. Por lo tanto, los servicios de AWS IoT se adhieren a los protocolos estándar del sector y a las prácticas recomendadas. Además, AWS IoT Core admite otros protocolos estándar y personalizados del sector, lo que permite que los dispositivos se comuniquen entre sí, incluso si utilizan protocolos diferentes. AWS defiende firmemente la interoperabilidad para que los desarrolladores puedan aprovechar las plataformas existentes con el fin de satisfacer las necesidades cambiantes de los clientes. AWS también es compatible con un próspero ecosistema de socios, el que permite ampliar el

menú de opciones y superar las limitaciones que los clientes enfrentan. La aplicación de prácticas recomendadas y reconocidas a nivel mundial conlleva una serie de beneficios para todas las partes interesadas del IoT, entre las que se incluyen:

- Repetición y reutilizo, en lugar de reinicio y restablecimiento
- Consistencia y consenso para promover la compatibilidad de la tecnología y la interoperabilidad a través de las fronteras geográficas
- Maximización de eficiencias para acelerar la modernización y la transformación de la TI

3. **Centrarse en el impacto para jerarquizar las medidas de seguridad informática**
   La naturaleza de los ataques o de las anormalidades no es siempre la misma y es posible que el impacto en personas, operaciones empresariales y datos no sea el mismo. La comprensión de los ecosistemas del IoT de los clientes y de dónde operarán los dispositivos dentro de éste permite identificar dónde se encuentran los mayores riesgos: dentro del dispositivo, como parte de la red, o como componente físico o de seguridad informática. Centrarse en la evaluación del impacto del riesgo y las consecuencias es fundamental para determinar dónde se deben dirigir los esfuerzos de seguridad informática y quién es responsable de los mismos en el ecosistema del IoT.

Conclusión

Junto con un crecimiento exponencial en dispositivos conectados, cada "cosa" en el IoT comunica paquetes de datos que requieren conectividad, almacenamiento y seguridad informática fiables. Con el IoT, una empresa enfrenta el desafío de administrar, supervisar y asegurar una inmensa cantidad de volúmenes de datos y conexiones desde dispositivos dispersos. Pero este desafío no tiene por qué suponer un obstáculo en un entorno basado en la nube. Además de escalar y ampliar una solución en una sola ubicación, la computación en la nube permite que las soluciones del IoT se expandan globalmente y en diferentes ubicaciones físicas, reduciendo a la vez la latencia de la comunicación y permitiendo una mejor capacidad de respuesta desde dispositivos en el campo. AWS ofrece un conjunto de servicios de IoT con seguridad informática de extremo a extremo, incluidos servicios para operar y proteger puntos de enlace, gateways, plataformas y aplicaciones, así como el tráfico que atraviesa estas capas. Esta integración simplifica la utilización y gestión segura de dispositivos y datos que interactúan continuamente entre ellos, lo que permite a las empresas beneficiarse de la innovación y las eficiencias que puede ofrecer el IoT a la vez que se mantiene la seguridad informática como prioridad.

Apéndice 1: Integración de servicios de AWS IoT

AWS IoT se integra directamente con los siguientes servicios de AWS:

- **Amazon Simple Storage Service (Amazon S3)** proporciona almacenamiento escalable en la nube de AWS. Para obtener más información, consulte Amazon S3.
- **Amazon DynamoDB** proporciona bases de datos NoSQL administradas. Para obtener más información, consulte Amazon DynamoDB.
- **Amazon Kinesis** permite el procesamiento en tiempo real de transmisión de datos a gran escala. Para obtener más información, consulte Amazon Kinesis.
- **AWS Lambda** ejecuta el código de los clientes en servidores virtuales de Amazon Elastic Compute Cloud (Amazon EC2) en respuesta a eventos. Para obtener más información, consulte AWS Lambda.
- **Amazon Simple Notification Service (Amazon SNS)** envía o recibe notificaciones. Para obtener más información, consulte Amazon SNS.
- **Amazon Simple Queue Service (Amazon SQS)** almacena datos en una cola para que las aplicaciones los recuperen. Para obtener más información, consulte Amazon SQS.

Apéndice 2: Gobiernos que abordan el IoT

Estados Unidos de América

Instituto Nacional de Estándares y Tecnología (NIST): Departamento de Comercio

El Departamento de Comercio de los Estados Unidos lidera múltiples esfuerzos para abordar la seguridad informática del IoT. El Instituto Nacional de Estándares y Tecnología (NIST) publicó un documento técnico[14] que pone de manifiesto temas que tanto los clientes como las agencias gubernamentales contemplan a la hora de evaluar la seguridad informática de los datos y los dispositivos. En dicho documento técnico, se invita a los lectores a evaluar estas inquietudes y se proporcionan recomendaciones sobre cómo mitigar los problemas. El NIST también publicó el informe interno de NIST 8228 (en inglés, NIST Internal Report),[15] que identifica los riesgos que pueden afectar a la adopción del IoT. El documento también ofrece recomendaciones para mitigar o reducir los efectos de estas inquietudes. Entre otras iniciativas, el NIST está convocando asociaciones públicas y privadas, solicitando comentarios y organizando talleres relacionados con las ciudades inteligentes y la estandarización internacional del IoT[16]. Aunque los indicadores iniciales señalan que los riesgos potenciales de ciberseguridad y privacidad son retos importantes para los beneficios que los Gobiernos y los consumidores pueden conseguir a través del IoT.

Departamento de Defensa

Otro ejemplo en el ámbito del gobierno se encuentra en el sector de defensa. En 2016, el director de sistemas de información del Departamento de Defensa de los Estados Unidos (por su sigla en inglés “DoD”) emitió recomendaciones de políticas para abordar las vulnerabilidades y riesgos que supone el IoT[17]. De acuerdo con la recomendación de la política, el Departamento de Defensa ya suministra millones de dispositivos y sensores de IoT en todas las instalaciones, vehículos y dispositivos médicos del Departamento de Defensa, y está considerando la posibilidad de incorporarlos a los sistemas de armas e inteligencia. La complejidad de la seguridad en el IoT se debe a la limitación de la potencia de procesamiento de los dispositivos para ejecutar firewalls y antimalware, así como al gran número de dispositivos, lo que aumenta la exposición a vulnerabilidades con respecto a los dispositivos móviles tradicionales.

Entre los enfoques y las acciones que el Departamento de Defensa recomienda para abordar los riesgos de seguridad del IoT se incluyen los siguientes: 1) un análisis de riesgos de seguridad informática y privacidad que apoye cada implementación de IoT y sus flujos de datos asociados, 2) el cifrado de todos los puntos y que los costes sean proporcionales al riesgo y al valor, y 3) una supervisión de las redes IoT para identificar tráfico anómalo y amenazas emergentes.

---

[14] Jeffrey Voas (NIST), Richard Kuhn (NIST), Phillip Laplante (Penn State University) y Sophia Applebaum (MITRE), "Internet of Things (IoT) Trust Concerns" (16 de octubre de 2018, https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iot-trust-concerns/draft)

[15] NISTIR 8228, “Considerations for Managing IoT Cybersecurity and Privacy Risks Out for Public Comment” (español no garantizado; 26 de septiembre de 2018, https://www.nist.gov/news-events/news/2018/09/draft-nistir-8228-considerations-managing-iot-cybersecurity-and-privacy)

[16] Véase https://www.nist.gov/itl/applied-cybersecurity/nist-initiatives-iot

[17] Véase https://dodcio.defense.gov/Portals/0/Documents/Announcement/DoD%20Policy%20Recommendations%20for%20Internet% 20of% 20Things% 20-% 20White% 20Paper.pdf? ver = 2017-01-26-152811-440

Comisión Federal de Comercio (por su sigla en inglés "FTC")

La FTC ha sido un participante importante en las conversaciones sobre la seguridad del IoT, llevando a cabo acciones contra los fabricantes de dispositivos que han tergiversado o demostrado negligencia en sus compromisos de seguridad informática. La FTC ha elevado el listón hasta "seguridad razonable de los datos". La FTC ha detectado de forma repetida las siguientes deficiencias de seguridad informática en los fabricantes de dispositivos:

- Seguridad informática no integrada en los dispositivos
- Los desarrolladores no están formando a sus empleados en buenas prácticas de seguridad informática
- No garantizar la seguridad informática y el cumplimiento de normas en las fases posteriores (a través de contratos)
- Falta de defensa en estrategias minuciosas
- Falta de controles razonables de acceso (los clientes pueden eludir o deducir contraseñas predeterminadas)
- Falta de un programa de seguridad informática de datos

Estado de California

California es uno de los primeros estados de Estados Unidos en aprobar legislación sobre el IoT. Los proyectos de ley vigentes contemplan problemas como la seguridad del diseño de dispositivos y la protección de datos, pero no plantean requisitos específicos para los fabricantes de IoT. En cambio, los legisladores se han centrado en la seguridad en la fase de diseño, estableciendo que la protección de los datos debe ser "apropiada a la naturaleza y función del dispositivo" y "adecuada a la información que puede recopilar, contener o transmitir".

Reino Unido

El Departamento de Cultura, Medios de Comunicación y Deporte del Reino Unido (por su sigla inglesa "DCMS") publicó la versión final de su Code of Practice for Consumer IoT Security (Código de práctica en material de seguridad informática del IoT para los consumidores) en octubre de 2018[18]. Este Código de práctica fue redactado conjuntamente con el Centro Nacional de Ciberseguridad británico e incluyó aportaciones de asociaciones de consumidores, la industria y el mundo académico.

El documento proporciona 13 directrices sobre cómo lograr un enfoque "seguro por diseño" para todas las organizaciones involucradas en el desarrollo, fabricación y venta al por menor de productos de consumo de IoT.

[18] Véase https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security

El Código de práctica hace hincapié en tres prácticas principales para permitir a los usuarios obtener los mayores y más inmediatos beneficios en materia de seguridad informática, e insta a las partes interesadas del IoT a implementarlas según sus prioridades: 1) Sin contraseñas predeterminadas: muchos usuarios no cambian la contraseña predeterminada y eso ha sido la fuente de muchos problemas de seguridad informática del IoT. 2) Implementar una política de divulgación de vulnerabilidades: los desarrolladores de dispositivos, servicios y aplicaciones del IoT deben tener una política de divulgación de vulnerabilidades y un punto de contacto público para permitir informar sobre vulnerabilidades y sus correcciones de manera oportuna. 3) Mantener el software actualizado: las actualizaciones de software deben ser oportunas, fáciles de implementar y no disruptivas para el funcionamiento del dispositivo.

En función de las inquietudes y los enfoques expuestos tanto por los Estados Unidos como por el Reino Unido, la seguridad informática del IoT seguirá siendo lo más importante para los Gobiernos. Los órganos nacionales e internacionales de normalización también están realizando esfuerzos para desarrollar estándares, directrices y prácticas recomendadas para garantizar la seguridad informática del IoT[19], incluida la Arquitectura de Referencia de IoT de la Organización Internacional de Normalización (ISO) y el grupo de estudio de la Unión Internacional de Telecomunicaciones (UIT) sobre IoT y ciudades inteligentes[20].

En el contexto del IoT, los clientes deben tener la flexibilidad de usar prácticas existentes probadas en uso en lo que se considera una "ciberseguridad de red tradicional". Por ejemplo, al intentar identificar vulnerabilidades, detectar irregularidades, responder a posibles incidentes y recuperarse de daños o interrupciones en los dispositivos IoT, los clientes pueden usar los controles de ciberseguridad asignados en el marco de la ciberseguridad del NIST (CSF)[21]. Este conjunto fundamental de disciplinas de ciberseguridad está reconocido a nivel mundial y ha sido apoyado por Gobiernos e industrias como una base de referencia recomendada para su uso por cualquier organización, independientemente de su sector o tamaño. La ventaja de utilizar el CSF del NIST no solo radica en su reputación, sino también en la flexibilidad que permite aplicar la ciberseguridad sin perder de vista su efecto sobre las dimensiones físicas, cibernéticas y de las personas. Junto con el aspecto humano, el marco se aplica a las organizaciones que dependen de la tecnología, ya se trate principalmente de tecnología de la información, sistemas de control industrial, sistemas ciberfísicos o IoT.

[19] Para obtener un compendio de estándares e iniciativas actuales sobre seguridad informática del IoT, consulte el catálogo del Departamento de Comercio, Administración Nacional de Telecomunicaciones e Información (por su sigla inglesa "NTIA") de los Estados Unidos: https://www.ntia.doc.gov/files/ntia/publications/ iotsecuritystandardscatalog_draft_17.pdf

[20] Véase https://www.itu.int/en/ITU-T/about/groups/Pages/sg20.aspx

[21] Para obtener más detalles sobre cómo ajustarse al CSF del NIST mediante los servicios de AWS, consulte este documento técnico y libro de trabajo de clientes: https://d0.awsstatic.com/whitepapers/compliance/NIST_Cybersecurity_Framework_CSF.pdf

Apéndice 3: Servicios y cumplimiento normativo de AWS IoT

Como proveedor global de servicios en la nube a gran escala, AWS adopta un enfoque riguroso y basado en el riesgo para la seguridad informática de sus servicios del IoT y la protección de los datos de los clientes. AWS impone procesos de seguridad informática interna en todos sus servicios en la nube con el fin de evaluar la eficacia de los controles administrativos, técnicos y operativos necesarios para protegerse frente a amenazas de seguridad actuales y emergentes que afectan a la seguridad y la resiliencia. Este proceso obligatorio de garantía de seguridad no solo conlleva la certificación de diversos marcos de cumplimiento, sino que refuerza el compromiso de AWS de integrar la seguridad informática en todas las fases de desarrollo y en los procesos operativos del ciclo de vida de sus servicios. AWS ofrece servicios en la nube comercial a gran escala que cuentan con la acreditación de estándares internacionalmente reconocidos como ISO 27001[22], Payment Card Industry Data Security Standard (PCI)[23], y Service Organization Control Reports (SOC)[24], entre otras acreditaciones internacionales, nacionales y sectoriales. AWS también cumple con los rigurosos requisitos de seguridad informática en lo que respecta a la compatibilidad con los entornos clasificados de determinadas agencias de inteligencia. En conjunto, los clientes de cualquier sector y de cualquier tamaño que utilicen los servicios en la nube de AWS obtienen estos y otros beneficios de seguridad informática porque AWS pone el sello de excelencia en todos sus servicios.

AWS es sensible al hecho de que los clientes pueden tener requisitos de cumplimiento específicos que deben comprobarse y respetarse. Con este objetivo, AWS añade continuamente, y a petición de los clientes, servicios ajustados a sus programas de cumplimiento. Los servicios de IoT incluidos en el ámbito de aplicación se enumeran por programa de cumplimiento en el sitio web de AWS[25].

[22] ISO 27001/27002 es un estándar de seguridad global ampliamente adoptado. Establece requisitos y prácticas recomendadas para lograr un enfoque sistemático de la gestión de la información de la empresa y del cliente, basado en evaluaciones de riesgo periódicas y apropiadas a un escenario de amenazas en constante cambio. ISO 27018 es un código de práctica que se centra en la protección de datos personales en la nube. Se basa en la norma ISO 27002 de seguridad de la información y proporciona orientación de implementación sobre los controles ISO 27002 aplicables a la información de identificación personal (PII) en nubes públicas. También proporciona un conjunto de controles adicionales y orientación destinados a abordar los requisitos de protección de PII en la nube pública que no se incluyen en el conjunto de controles ISO 27002 existente.

[23] El Estándar de Seguridad de los Datos de la Industria de las Tarjetas de Pago (PCI DSS) es un estándar exclusivo de seguridad de la información administrado por el Consejo de Estándares de Seguridad de PCI, (https://www.pcisecuritystandards.org), fundado por American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa Inc. PCI DSS se aplica a todas las entidades que almacenan, procesan o transmiten datos de titulares de tarjetas (CHD) o datos de autenticación confidenciales (SAD), incluidos comerciantes, procesadores, adquisidores, emisores y proveedores de servicios.

[24] Los informes de Service Organization Controls (SOC 1, 2, 3) están diseñados para cumplir una amplia gama de requisitos de auditoría financiera para los organismos de auditoría estadounidenses e internacionales. La auditoría de este informe se lleva a cabo de conformidad con las Normas Internacionales de Contratación de Aseguramiento n.º 3402 (ISAE 3402) y el Instituto Americano de Contables Públicos Certificados (por su sigla inglesa "AICPA"): AT 801 (anteriormente SSAE 16).

[25] Véase https://aws.amazon.com/compliance/services-in-scope