Trabajo final. El Internet de las Cosas

Integrantes
Acosta Porcayo Alan Omar 320206102
Medina Villa Samuel 320249538
Mendez Barcena Marlene 320328116

Definición y concepto

La expresión IoT, que corresponde a Internet de las cosas, hace referencia a la interconexión de dispositivos y a la tecnología que posibilita la comunicación entre dichos dispositivos y la nube, así como entre ellos mismos.

Los dispositivos en objetos físicos dentro de la Internet de las cosas generalmente se dividen en dos categorías: aquellos que actúan como interruptores, enviando instrucciones a un objeto, y aquellos que funcionan como sensores, recopilando datos y transmitiéndolos a otro destino.

Breve historia y evolución

En 1982, se iniciaron las primeras discusiones sobre la creación de una red de dispositivos inteligentes, marcadas por la transformación de una máquina de Coca-Cola en el primer electrodoméstico conectado a Internet. A lo largo de la década de los 90, se publicaron diversos artículos académicos, consolidándose el término “Internet de las cosas” en 1999.

A partir de ese punto, el desarrollo del concepto de Internet de las cosas estuvo vinculado a la integración de sensores y conexiones en cualquier dispositivo capaz de admitirlos. Esencialmente, se buscaba infundir “inteligencia” en varios objetos electrónicos que tuvieran la capacidad de soportar dicha incorporación.

Tecnologías fundamentales

Protocolos de comunicación

Dentro del ámbito del Internet de las Cosas (IoT), se emplean diversos protocolos de comunicación con el propósito de facilitar la transferencia de datos entre los dispositivos conectados. Estos protocolos se pueden categorizar en varias capas del modelo OSI (Open Systems Interconnection) y desempeñan funciones específicas en el intercambio de información. Algunos de los protocolos más habituales en IoT incluyen:

1. **MQTT (Message Queuing Telemetry Transport):** Un protocolo de mensajería eficiente diseñado para entornos donde la red puede ser inestable, ampliamente utilizado en IoT para la transmisión de mensajes entre dispositivos y servidores.
2. **CoAP (Constrained Application Protocol):** Un protocolo diseñado para redes de dispositivos con recursos limitados, como sensores y actuadores, operando de manera eficiente sobre el protocolo de transporte UDP (User Datagram Protocol).
3. **HTTP/HTTPS (Hypertext Transfer Protocol/Secure):** Aunque comúnmente asociado con la web, se emplea en IoT para la comunicación entre dispositivos y servidores. HTTPS agrega seguridad mediante SSL/TLS (Secure Sockets Layer/Transport Layer Security).
4. **AMQP (Advanced Message Queuing Protocol):** Un protocolo de mensajería orientado a la empresa que facilita la comunicación eficiente y confiable entre sistemas y dispositivos.
5. **DDS (Data Distribution Service):** Un estándar de la Object Management Group (OMG) para la comunicación de datos en sistemas distribuidos, utilizado en aplicaciones que requieren baja latencia y el intercambio de datos en tiempo real.
6. **Bluetooth y Bluetooth Low Energy (BLE):** Utilizados para la comunicación inalámbrica de corto alcance entre dispositivos IoT, especialmente en aplicaciones de hogares inteligentes o dispositivos portátiles.
7. **Zigbee y Z-Wave:** Protocolos de comunicación inalámbrica de bajo consumo de energía, empleados en redes de área personal para IoT, especialmente en aplicaciones de hogares inteligentes.

Sensores y actuadores

Sensores y actuadores desempeñan roles fundamentales al percibir información del entorno y participar en interacciones con él. Los sensores se encargan de recopilar datos, mientras que los actuadores habilitan al sistema para llevar a cabo acciones específicas.

Existen dos categorías de sensores: aquellos de uso general y los especializados en tareas específicas.

Los sensores de uso general aprovechan dispositivos convencionales, como cámaras y micrófonos, para la recopilación de datos. En esta instancia, los datos, como imágenes o grabaciones de sonido, son analizados mediante aplicaciones informáticas y algoritmos.

Por otro lado, los sensores destinados a tareas específicas están diseñados para medir valores particulares y destacan por su bajo costo, robustez o eficiencia energética. Estos sensores, como termómetros, medidores de humedad, detectores de movimiento, monitores de frecuencia cardíaca y electrocardiogramas, así como los sensores de básculas, por lo general, requieren soluciones de software más simples en comparación con los sensores de uso general.

Algunos tipos habituales incluyen:

1. **Motores:** Eléctricos para ejecutar movimientos mecánicos, como abrir puertas, y motores paso a paso para lograr posicionamiento preciso.
2. **Válvulas:** Encargadas de regular el flujo de líquidos o gases en sistemas de fontanería o climatización.
3. **Servomecanismos:** Los servomotores brindan un control preciso de la posición angular, utilizados en aplicaciones como la dirección de vehículos a control remoto.
4. **Piezoeléctricos:** Generan movimiento en respuesta a cambios en el voltaje, empleados en aplicaciones que requieren movimientos precisos a pequeña escala.
5. **Neumáticos e Hidráulicos:** Cilindros neumáticos para control mediante aire comprimido y cilindros hidráulicos que utilizan líquidos.
6. **Magnéticos:** Electroimanes que regulan el movimiento de objetos metálicos a distancia.
7. **De Forma Variable:** Materiales con memoria de forma que alteran su estructura en respuesta a estímulos como temperatura o corriente eléctrica.
8. **Retroalimentación Háptica:** Actuadores de vibración para proporcionar retroalimentación táctil en dispositivos como mandos a distancia o dispositivos de juego.

Redes inalámbricas

En informática y telecomunicaciones, se conoce como red inalámbrica a un tipo de conexión entre sistemas informáticos (o sea, entre computadoras) que se lleva a cabo mediante diversas ondas del espectro electromagnético.

Es decir, es una conexión de nodos que no requiere de ningún tipo de cableado o dispositivo alámbrico, ya que la transmisión y recepción de la información se produce mediante puertos especializados. Este tipo de tecnología representa un enorme salto adelante respecto de los métodos tradicionales.

Se originó en 1971, cuando un grupo de investigadores dirigidos por el ingeniero informático estadounidense Norman Abramson (1932), crearon en la Universidad de Hawái ALOHA, el primer sistema de conmutación de paquetes a través una red de comunicaciones por ondas de radio.

Según su área de alcance. Se clasifican de modo similar a las redes alámbricas:

1. **WPAN.** Siglas de Wireless Personal Area Network (Red Inalámbrica de Área Personal), tiene un rango máximo de 10 metros, por lo que sirve para uno o dos usuarios máximo, que se encuentren juntos. Este tipo de tecnologías incluye el Bluetooth, ZigBee, etc.

2. **WLAN.** Siglas de Wireless Local Area Network (Red Inalámbrica de Área Local), es el estándar de comunicaciones en el que se basan las tecnologías WiFi, capaces de alcanzar una distancia mucho mayor en base a repetidoras, interconectando diversos tipos de aparatos mediante ondas de radio.
3. **WMAN.** Siglas de Wireless Metropolitan Area Network (Red Inalámbrica de Área Metropolitana), redes de mucho mayor alcance, capaces de cubrir hasta 20 kilómetros.
4. **WWAN.** Siglas de Wireless Wide Area Network (Red Inalámbrica de Área Amplia), emplea tecnologías de telefonía celular y microondas para transferir datos a lo largo de enormes distancias. Algunos de sus tipos de tecnología son GPRS, EDGE, GSM, 3G, 4G o 5G.

Según su rango de frecuencias. Dependiendo de qué parte del espectro electromagnético emplee para transmitir, podemos distinguir entre:

1. **Microondas terrestres.** Empleando antenas parabólicas de unos 3 metros de diámetro, se emite una señal de microondas que posee un alcance de varios kilómetros, empleando frecuencias de entre 1 y 300 GHz.
2. **Microondas satelitales.** Opera en base al vínculo entre dos o más estaciones base, a través de la intermediación de un satélite suspendido en la atmósfera. Cada satélite posee sus bandas de frecuencia específicas, pero tiene un alcance mucho mayor y una velocidad más alta.
3. **Infrarrojos.** Emplea moduladores de la luz infrarroja no coherente, que al estar alineados directamente o reflejados en una superficie adecuada, alcanzan entre 300 GHz y 384 THz de velocidad de transmisión de datos. Sin embargo, no puede atravesar las paredes.
4. **Ondas de radio.** Emplea ondas en diversas frecuencias (AM, FM, HF, VHF, UHF, etc.) para emitir y recibir las señales de información, logrando una eficacia alta en cortas distancias, incluso a través de paredes, pero perdiéndose a medida que el receptor se aleja físicamente del emisor.

¿Qué beneficios brinda una red inalámbrica Wi-Fi?

Las empresas pueden obtener varias ventajas de una red inalámbrica de Cisco, incluidas las siguientes:

1. **Comodidad:** acceda a los recursos de red desde cualquier ubicación del área de cobertura de la red inalámbrica o desde cualquier zona Wi-Fi.
2. **Movilidad:** no está atado al escritorio, como sí sucede con una conexión cableada. Usted y sus empleados pueden conectarse en las reuniones de sala de conferencias, por ejemplo.
3. **Productividad:** el acceso inalámbrico a Internet y a las aplicaciones y los recursos esenciales de la empresa ayuda al personal a cumplir su trabajo y fomenta la

colaboración.

4. **Fácil configuración:** no hace falta pasar cables, por lo que la instalación puede ser rápida y rentable.
5. **Capacidad de expansión:** puede ampliar fácilmente las redes inalámbricas con los equipos existentes, mientras que una red cableada puede requerir cableado adicional.
6. **Seguridad:** los avances en redes inalámbricas proporcionan sólidas protecciones de seguridad.
7. **Costo reducido:** como las redes inalámbricas eliminan o reducen los gastos de cableado, pueden costar menos que las redes cableadas para su operación.

Cómo implementar una red inalámbrica

Para crear su red inalámbrica, puede elegir entre tres tipos de implementación: implementación centralizada, implementación convergente e implementación basada en la nube. ¿Necesita ayuda para averiguar qué implementación es mejor para su empresa? Hable con un experto.

- **Implementación centralizada**

  El tipo de sistema de red inalámbrica más frecuente, las implementaciones centralizadas se utilizan generalmente en campus en los que los edificios y las redes están cerca. Esta implementación consolida la red inalámbrica, que facilita las actualizaciones y la funcionalidad inalámbrica avanzada. Los controladores se basan en las instalaciones y se instalan en una ubicación centralizada.

- **Implementación convergente**

  Para los campus pequeños o las sucursales, las implementaciones convergentes ofrecen consistencia en las conexiones inalámbricas y por cable. Esta implementación realiza la convergencia de conexión por cable y conexión inalámbrica en un solo dispositivo de red, un switch de acceso, y desempeña dos funciones, la de switch y la de controlador inalámbrico.

- **Implementación basada en la nube**

  Este sistema utiliza la nube para administrar dispositivos de red implementados en las instalaciones, en diferentes ubicaciones. La solución requiere dispositivos administrados en la nube Cisco Meraki, que ofrecen completa visibilidad de la red a través de sus paneles.

Desafíos y Consideraciones de Seguridad

Vulnerabilidades y amenazas

Es habitual que se confundan los términos vulnerabilidad y amenaza informática, ya que ambos se encuentran relacionados. Sin embargo, hay diferencias entre ambos conceptos.

Vulnerabilidades

Una vulnerabilidad es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de esta. Se trata de un “agujero” que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos (por ejemplo, de los sistemas operativos) para poder entrar en los mismos y realizar actividades ilegales, robar información sensible o interrumpir su funcionamiento.

Las vulnerabilidades son una de las principales causas por las que una empresa puede sufrir un ataque informático contra sus sistemas. Por eso siempre es recomendable actualizar a las últimas versiones, las aplicaciones informáticas, sistemas de protección y sistemas operativos, pues esas actualizaciones contienen muchas correcciones sobre vulnerabilidades descubiertas.

Amenazas informáticas

Se entiende como amenaza informática toda aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático. Las amenazas informáticas para las empresas provienen en gran medida de ataques externos, aunque también existen amenazas internas (como robo de información o uso inadecuado de los sistemas).

Tipos de Vulnerabilidades y Amenazas informáticas en la empresa

Son muchas las vulnerabilidades y amenazas informáticas a las que están expuestas las empresas en la actualidad. Por eso la inversión en ciberseguridad y sistema de protección ha experimentado un gran aumento en los últimos años, siendo los profesionales en ciberseguridad uno de los perfiles más buscados en el sector de la informática.

A continuación, veremos las principales amenazas y vulnerabilidades a las que se exponen las empresas hoy en día:

Amenazas de Programa maligno

Los programas maliciosos son una de las mayores ciber amenazas a la que se exponen las empresas. Dentro del malware existen distintos tipos de amenazas, siendo las principales:

- Virus. Los virus informáticos son un software que se instalan en un dispositivo con el objetivo de ocasionar problemas en su funcionamiento. Para que un virus infecte un sistema es necesaria la intervención de un usuario (intencionada o inintencionadamente).
- Gusanos. Es uno de los malware más comunes que infectan los equipos y sistemas de una empresa, ya que no requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo. El objetivo de los gusanos es el de replicarse e infectar el mayor número de dispositivos posibles utilizando la red para ello. Son una amenaza para las redes empresariales, porque un solo equipo infectado puede hacer que la red entera se vea afectada en un espacio corto de tiempo.
- Troyanos. Los troyanos son programas que se instalan en un equipo y pasan desapercibidos para el usuario. Su objetivo es el de ir abriendo puertas para que otro tipo de software malicioso se instale.
- Ransomware. El ransomware se ha convertido en el malware más temido en la actualidad por las empresas. Consiste en encriptar toda la información de la empresa, impidiendo el acceso a los datos y los sistemas y se pide un rescate para poder liberar la información (normalmente en criptomonedas como bitcoins).
- Keyloggers. Se instalan a través de troyanos y se encargan de robar datos de acceso a plataformas web, sitios bancarios y similares.

Vulnerabilidades del sistema

Los sistemas y aplicaciones informáticos siempre tienen algún error en su diseño, estructura o código que genera alguna vulnerabilidad. Por muy pequeño que sea ese error, siempre podrá generar una amenaza sobre los sistemas y la información, siendo la puerta de entrada para recibir ataques externos o internos. Las principales vulnerabilidades suelen producirse en:

- Errores de configuración.
- Errores en la gestión de recursos.
- Errores en los sistemas de validación.
- Errores que permiten el acceso a directorios.
- Errores en la gestión y asignación de permisos.

Cómo evitar estas amenazas de seguridad

Hemos visto el top 5 de amenazas de seguridad en la actualidad. Ahora vamos a dar una serie de consejos para tener todo en orden y evitar problemas que pueda comprometernos a la hora de usar nuestros dispositivos en Internet.

Tener programas de seguridad

Algo básico para protegernos es contar con herramientas de seguridad. Un buen antivirus puede ayudarnos a prevenir ataques muy variados que comprometan nuestros sistemas. Debemos siempre contar con software que nos proteja, sin importar el tipo de sistema operativo que estemos utilizando.

Mantener todo actualizado

También se esencial tener nuestros sistemas actualizados correctamente. Son muchas las ocasiones en las que pueden surgir vulnerabilidades. Esos problemas pueden ser explotados por piratas informáticos para llevar a cabo sus ataques. Gracias a los parches y actualizaciones podemos protegernos adecuadamente. En Internet hay muchas amenazas y hay que evitarlas.

Descargar de fuentes fiables

Otro consejo interesante es descargar programas y cualquier tipo de archivo únicamente desde fuentes oficiales y fiables. De lo contrario podríamos estar instalando software que ha sido modificado de forma maliciosa por terceros.

Sentido común

Una última recomendación, aunque quizás la más importante, el sentido común. Muchos ataques requieren de la interacción del usuario. Por ejemplo, la descarga de archivos adjuntos maliciosos o los ataques Phishing. Por ello debemos tener siempre presente el sentido común y no cometer errores que nos puedan comprometer.

Privacidad de datos

Las medidas de ciberseguridad existen para proteger la información en el entorno digital y entre esa información a proteger está también la información personal o de carácter confidencial que manejan organizaciones privadas, organismos públicos y también los propios particulares.

Sin esas medidas de ciberseguridad, sería imposible poder garantizar tanto la seguridad en Internet como la privacidad digital. Y, aunque es cierto que no podemos hablar de medidas de seguridad cien por cien infalibles (el riesgo cero nunca existe), sí podemos afirmar que la adopción e implantación de medidas técnicas y organizativas de ciberseguridad contribuyen a mantener privada y confidencial la información (sea esta personal, empresarial, comercial, gubernamental, etc.).

También existen medidas legales, es decir, leyes, normas y reglamentos que obligan a todo tipo de organizaciones a tener en marcha medios y mecanismos que garanticen la ciberseguridad, la seguridad de la información y la privacidad, es decir, recurrir a herramientas y soluciones que protejan la información personal de las personas.

No proteger de manera adecuada los datos personales que manejan diferentes tipos de organizaciones, públicas y privadas, tanto en el mundo físico como en el digital, puede suponer el acceso a los mismos y, a través de ellos, a sus titulares, empleando técnicas de ingeniería social para conseguir alcanzar el objetivo final, que en muchas ocasiones no será el individuo en sí, sino la organización en la que trabaja y el acceso a su red interna y la valiosa información confidencial que posee, así como la posibilidad de llevar a cabo ataques que puedan reportarles beneficios económicos (como el ransomware o el chantaje a cambio de no publicar la información robada).

Riesgos para los usuarios

Cuando se vulnera la protección de datos, los usuarios pueden enfrentar diferentes riesgos, como, por ejemplo:

- Sufrir más ataques de phishing, vishing o smishing
- Sufrir suplantación de identidad
- Perder el control de sus cuentas de usuario
- Estar expuestos a estafas y fraudes digitales
- Sufrir pérdidas económicas (bien por ser víctimas de robos a través de sus apps de banca o por ser víctimas de estafas)
- Sufrir posibles discriminaciones
- Sufrir extorsión o chantajes a cambio de no publicar información personal

Riesgos para las organizaciones

En cuanto a las organizaciones, el principal riesgo que enfrentan derivado de la vulneración de la protección de datos, son ciberataques dirigidos a puestos directivos y responsables de departamento, así como a empleados de niveles inferiores, que, como decíamos más arriba, a través de ataques de ingeniería social dirigidos a ellos, pueden convertirse en el punto de entrada de cibercriminales a la red interna de la organización.

Una vez ganado acceso a esa red interna, los cibercriminales podrán perseguir sus objetivos finales, que pueden ir desde un ataque de ransomware, un chantaje para evitar la exfiltración de información confidencial, el robo de esa información para venderla al mejor postor, hasta llevar a cabo un robo de dinero, por citar algunos de ellos.

Medidas de seguridad

Las implementaciones de IoT presentan nuevos desafíos de seguridad, privacidad y cumplimiento normativo para las empresas de todo el mundo. Mientras la ciberseguridad de la información tradicional gira en torno al software y al modo en el que se implementa,

la seguridad de IoT agrega una capa más de complejidad, ya que convergen el mundo cibernético y el mundo físico.

Una amplia gama de escenarios operacionales y de mantenimiento en el espacio de IoT dependen de la conectividad de dispositivos de extremo a extremo para que los usuarios y servicios puedan interactuar, iniciar sesión, resolver problemas y enviar o recibir datos de los dispositivos. Puede que las compañías quieran aprovechar la capacidad de la IoT, como el mantenimiento predictivo, por ejemplo, pero es fundamental saber qué estándares de seguridad de IoT deben cumplirse, porque la tecnología operacional (OT) es demasiado importante y valiosa como para arriesgarla en el caso de que se produzcan vulneraciones, desastres y otras amenazas.

Aunque los dispositivos IoT pueden parecer demasiado pequeños o demasiado especializados como para ser peligrosos, existe un riesgo en el que son verdaderos ordenadores de uso general conectados a una red que pueden piratear atacantes y dar lugar a problemas más allá de la seguridad de IoT. Incluso el dispositivo más trivial puede llegar a ser peligroso si resulta comprometido en Internet, desde el espionaje con monitores de vigilancia para bebés hasta servicios interrumpidos en equipos sanitarios que salvan vidas.

Una vez que los atacantes tienen el control, pueden robar datos, interrumpir la entrega de servicios o cometer cualquier otro cibercrimen que se lleve a cabo con un ordenador. Los ataques que comprometen la infraestructura de IoT causan daños, no solo con brechas de datos y operaciones no confiables, sino también daños físicos en las instalaciones o, peor aún, a las personas que dependen de esas instalaciones

Medidas para proteger las implementaciones de IOT

- **Simplificar la complejidad de la seguridad de IoT.** Intégrala en los equipos y la infraestructura para coordinar una estrategia completa, desde los dispositivos y sensores físicos hasta los datos en la nube.
- **Prepararse específicamente para la seguridad de IoT.** Ten en cuenta los dispositivos con recursos limitados, la distribución geográfica de las implementaciones y el número de dispositivos de la solución de seguridad de IoT.
- **Utilizar tecnología inteligente de análisis de seguridad y corrección.** Supervisa todo lo que esté conectado a tu solución de IoT con la administración de la posición de seguridad. Clasifica las sugerencias en función de la gravedad para decidir qué debe corregirse primero para minimizar el riesgo. Asegúrate de supervisar las amenazas para obtener alertas y solucionar las amenazas de seguridad de IoT con rapidez.
- **Centrarse en la protección de los datos de los clientes y la empresa.** Al mantener un seguimiento de todos los almacenes de datos conectados, los administradores y otros servicios relacionados con IoT, puedes estar seguro de que las aplicaciones de IoT están protegidas y de que tus medidas de seguridad de IoT son efectivas.

Tecnologías clave y mejores prácticas de ciberseguridad

Las siguientes mejores prácticas y tecnologías pueden ayudar a su organización a implementar una fuerte ciberseguridad que reduzca su vulnerabilidad a los ataques cibernéticos y proteja sus sistemas de información fundamentales, sin entrometerse en la experiencia del usuario o del cliente:

- **La Gestión de identidad y acceso (IAM)** define los roles y privilegios de acceso para cada usuario, así como las condiciones bajo las cuales se le otorgan o niegan sus privilegios. Las metodologías IAM incluyen el inicio de sesión único, que permite a un usuario iniciar sesión en una red una vez sin volver a ingresar las credenciales durante la misma sesión; autenticación multifactorial, que requiere dos o más credenciales de acceso; cuentas de usuario privilegiadas, que otorgan privilegios administrativos solo a ciertos usuarios; y gestión del ciclo de vida del usuario, que gestiona la identidad y los privilegios de acceso de cada usuario desde el registro inicial hasta el término.

  Las herramientas de IAM también pueden brindar a sus profesionales de ciberseguridad una visibilidad más completa de la actividad sospechosa en los dispositivos de los usuarios finales, incluidos los puntos finales a los que no pueden acceder físicamente. Esto ayuda a acelerar los tiempos de investigación y respuesta para aislar y contener el daño de una brecha de seguridad.

- **Una plataforma de seguridad de datos integral** protege la información confidencial en varios entornos, incluidos los entornos multinube híbridos. Las mejores plataformas de seguridad de datos brindan visibilidad automatizada y en tiempo real de las vulnerabilidades de los datos, así como supervisión continua que alerta sobre las vulnerabilidades y los riesgos de los datos antes de que se conviertan en brechas de seguridad; también deben simplificar la conformidad regulatoria de la privacidad de datos del gobierno y de la industria. Las copias de seguridad y el cifrado también son vitales para mantener los datos seguros.

- **La gestión de eventos e información de seguridad (SIEM)** agrega y analiza datos de eventos de seguridad para detectar automáticamente las actividades sospechosas de los usuarios y desencadenar una respuesta preventiva o correctiva. Actualmente, las soluciones SIEM incluyen métodos de detección avanzados como la analítica del comportamiento del usuario y la inteligencia artificial (IA).

  La SIEM puede priorizar automáticamente la respuesta a las amenazas cibernéticas de acuerdo con los objetivos de gestión de riesgos de su empresa. Y muchas organizaciones están integrando sus herramientas SIEM con plataformas de orquestación, automatización y respuesta de seguridad (SOAR) que automatizan y aceleran aún más la respuesta a incidentes de ciberseguridad y resuelven muchos sin intervención humana.

Desarrollos Futuros y Tendencias

Avances tecnológicos

Según un reciente informe publicado por Frost & Sullivan, el número de dispositivos conectados a IoT seguirá aumentando en los próximos años hasta alcanzar los 66.000 millones de unidades en el año 2026. De esta forma, las grandes organizaciones seguirán tratando de recuperarse de la pandemia de la COVID-19 y de convertirse en compañías más eficientes, productivas y conscientes de la importancia de la experiencia del cliente.

Para potenciar su aplicaciones, el IoT trabaja con otras tecnologías punteras, como Big Data, Blockchain, Cloud y Edge Computing, Realidad Aumentada y 5G.

Big Data

Dado que en el IoT genera datos provenientes de miles o millones de sensores, el Big Data permitirá tomar decisiones automáticas (a través de actuadores) o guiadas por las personas (manejando las aplicaciones informáticas desarrolladas a tal efecto) con objeto de controlar, gobernar y optimizar los servicios IoT desplegados. De hecho, podemos decir que actualmente todos los proyectos de IoT contemplan las tecnologías de Big Data como elemento imprescindible de la solución.

Blockchain

La tecnología Blockchain podría aplicarse para resolver los problemas de seguridad a los que se enfrentan las soluciones IoT. A medida que aumentan las conexiones de dispositivos IoT, los puntos de acceso para los hackers también lo hacen. Por ello, la autenticación y la estandarización en cada uno de los elementos IoT son aspectos esenciales para una adopción generalizada.

Entendemos que los esfuerzos para soluciones de Identidad Digital Soberana pueden también aprovecharse en las soluciones IoT, dotando de un identificador único a cada dispositivo y que éste intercambie sólo los datos de identificación y de funcionamiento necesarios en función de qué otro dispositivo o persona esté estableciendo comunicación con él.

Cloud y Edge Computing

Los modelos de “Fog Computing” y de “Edge Computing” surgen para resolver la problemática de comunicaciones que surge con el IoT. Un ejemplo ilustrativo del uso de las tres capas sería el de los vehículos autónomos, donde cada vehículo toma decisiones en tiempo real como pueden ser frenar, acelerar o cambiar de carril en función de parámetros internos del coche -EDGE-, del entorno en que se encuentra -FOG- y de los datos generales de tráfico o meteorológicos, así como de nuevos algoritmos generados desde la nube -CLOUD-.

Los sistemas IoT son, por sus características de multitud de dispositivos y multitud de protocolos, claros candidatos a ser gestionados desde la nube. La mayor sofisticación de los dispositivos, y la necesidad de que se comuniquen entre ellos sin intervención humana, está haciendo que se potencie el uso de Edge Computing.

Se está aplicando este modelo en ámbitos como los vehículos conectados y autónomos, ciudades inteligentes y hogares inteligentes.

Realidad Aumentada

La tecnología de realidad aumentada se puede usar para visualizar datos de cientos de sensores simultáneamente, superponiendo información relevante y procesable sobre el entorno a través de un auricular y de una pantalla semitransparente. Por ejemplo, si se está operando maquinaria pesada, se puede obtener una vista en tiempo real de qué componentes necesitan ser reemplazados.

5G y Mobile IoT

La tecnología 5G, por sus mejoras en velocidad y latencia respecto al 4G, promete un salto cualitativo y cuantitativo en aplicaciones como el coche autónomo o las operaciones quirúrgicas a distancia con robots. Esto hace que aplicaciones que con 4G no podían abordarse, puedan hacerlo ahora.

Por ejemplo, los expertos creen que las redes 5G podrán soportar la enorme cantidad de datos que generarán las ciudades inteligentes. Otro caso donde 5G es imprescindible es en el de los vehículos autónomos. Las innovaciones de 5G podrían permitir que los vehículos autónomos interactúen de manera segura entre sí, con la infraestructura de tráfico e incluso con las carreteras mismas.

Integración con inteligencia artificial

Inteligencia artificial (IA) e Internet de las cosas (IoT) son términos que proyectan una imagen futurista y de ciencia ficción; se han identificado ambos como causantes de la disrupción en los negocios en 2017. De hecho, ambos conceptos son más reales hoy de lo que lo han sido en ningún momento en el pasado. Sin embargo, para que las empresas sean conscientes del pleno potencial de la IoT, necesitan combinarla con las tecnologías de IA que avanzan rápidamente, lo que permite a las “máquinas inteligentes” simular comportamiento inteligente y tomar decisiones con pleno conocimiento de causa y con una intervención humana mínima o inexistente.

La IA se puede aplicar en muchos ámbitos dentro del Internet de las Cosas, desde los más cotidianos hasta los más técnicos y profesionales. Por eso a continuación comentaremos algunos de ellos:

- **Sensores más especializados** que permitan a los ordenadores “escuchar” obteniendo la información en formato audio.

- **Macrodatos visuales**, por ejemplo, permitirán a los ordenadores obtener un conocimiento más profundo de imágenes en la pantalla con las nuevas aplicaciones de IA que entienden el contexto de las imágenes.
- **Sistemas cognitivos** que crearán nuevas recetas que atraerán el sentido del gusto del usuario, creando menús optimizados para cada persona y adaptándose de forma automática a los ingredientes locales.
- **Operaciones conectadas y remotas.** Con operaciones de almacén inteligentes y conectadas, los trabajadores ya no tendrán que deambular por el almacén recogiendo productos de las estanterías para cumplimentar un pedido. En su lugar, las estanterías se moverán por los pasillos guiadas por pequeñas plataformas robóticas que entregan el inventario adecuado en el lugar correcto, evitando colisiones por el camino. Cumplimentar un pedido es más rápido, seguro y más eficaz.
- **Mantenimiento preventivo y predictivo.** Ahorrará a las empresas millones antes de una avería o fuga al predecir y prevenir los lugares y el momento en el que estas situaciones podrían tener lugar.

Retos en la implementación

1. **Compatibilidad:** la IoT es una recopilación de muchas partes y sistemas que son fundamentalmente diferentes en tiempo y espacio.
2. **Complejidad:** la IoT es un sistema complicado con muchas partes móviles y un flujo incesante de datos, lo que lo convierte en un ecosistema muy complicado.
3. **Confidencialidad/Seguridad (CS):** la CS supone siempre un problema con todas las nuevas tecnologías o conceptos, ¿en qué medida puede ayudar la IA sin poner en peligro la CS? Una de las nuevas soluciones para este problema es el uso de la tecnología de cadena de bloques (blockchain).
4. **Cuestiones éticas y jurídicas:** Es un nuevo mundo para muchas empresas en el que no hay precedentes y constituye un territorio que no ha sido probado con nuevas leyes y casos que emergen con rapidez.
5. **Estupidez artificial:** de vuelta al sencillo concepto de GIGO (Garbage In Garbage Out), la IA sigue necesitando “formación” para entender las reacciones/emociones humanas para que la decisión tenga sentido.

Conclusiones

En un mundo cada vez más conectado y digitalizado, la ciberseguridad y la privacidad de datos se han convertido en aspectos críticos para individuos y organizaciones. La primera parte de este documento se centró en identificar las principales amenazas de seguridad en la actualidad, desde el malware y los ataques de ransomware hasta el phishing y el

robo de identidad. Para enfrentar estas amenazas, se destacó la importancia de contar con programas de seguridad, mantener los sistemas actualizados y descargar software solo de fuentes confiables. Además, se resaltó la necesidad de ejercer el sentido común y no caer en trampas que podrían comprometer nuestra seguridad en línea.

La privacidad de datos también se reveló como un elemento fundamental, tanto para individuos como para organizaciones. Las regulaciones legales obligan a las empresas a proteger los datos personales, y no hacerlo puede tener graves consecuencias, desde ataques de phishing hasta la pérdida de control de cuentas de usuario y discriminación. En cuanto a las organizaciones, la falta de protección de datos puede exponerlas a ciberataques dirigidos y amenazas que van desde el ransomware hasta el robo de información confidencial. Para protegerse contra estos riesgos, se destacó la necesidad de adoptar medidas de seguridad efectivas.

La segunda parte de este documento exploró las tendencias y desarrollos futuros en tecnología, centrándose en Internet de las Cosas (IoT) y la inteligencia artificial (IA). Se reveló que el IoT continuará creciendo exponencialmente, con un aumento en el número de dispositivos conectados. Para aprovechar al máximo estas aplicaciones, se recalcó la importancia de tecnologías complementarias, como el Big Data, la Blockchain, la computación en la nube (Cloud) y Edge Computing. Estas tecnologías permiten el control y la gestión de datos generados por una amplia gama de dispositivos IoT y prometen hacer que nuestras vidas sean más eficientes y seguras.

La IA, por su parte, se ha convertido en un aliado poderoso para la IoT, permitiendo desde sensores más especializados hasta la automatización de tareas y la toma de decisiones inteligentes. La combinación de ambas tecnologías presenta oportunidades emocionantes en campos como la atención médica, la logística y la automatización industrial.

Sin embargo, también existen desafíos en la implementación de IoT y IA, incluyendo la compatibilidad, la complejidad, la seguridad, las preocupaciones éticas y la necesidad de entrenar a las máquinas para comprender el comportamiento humano.

En conclusión, en un mundo digital en constante evolución, la ciberseguridad, la privacidad de datos y las tecnologías emergentes como IoT e IA son temas críticos. La conciencia de las amenazas actuales y futuras, junto con la adopción de medidas de seguridad, son esenciales para mantenernos protegidos en línea. Mientras exploramos las oportunidades emocionantes que ofrece la tecnología, también debemos abordar los desafíos y consideraciones éticas que conlleva.

Referencias

- *¿Cómo funciona el IoT?* (s. f.). ¿Cómo funciona el IoT? https://courses.minnalearn.com/es/courses/emerging-technologies/the-internet-of-things/how-does-iot-work/

- *¿Qué es el Internet de las cosas (IoT) y cómo funciona?* (s. f.). https:

//www.redhat.com/es/topics/internet-of-things/what-is-iot

- *¿Qué es IoT? - Explicación del Internet de las cosas - AWS.* (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/iot/#:~:text=El%20t%C3%A9rmino%20IoT%2C%20o%20Internet,como%20entre%20los%20propios%20dispositivos

- *¿Qué es la ciberseguridad?* — IBM. (s. f.). https://www.ibm.com/mx-es/topics/cybersecurity

- *¿Qué es una red inalámbrica? - cableada frente vs. inalámbrica.* (2022, 25 marzo). Cisco. https://www.cisco.com/c/es_mx/solutions/small-business/resourcecenter/networking/wireless-network.html

- *6 tecnologías que potencian el internet de las cosas.* (2022, November 18). Fundación Innovación Bankinter. https://www.fundacionbankinter.org/noticias/las-6-tecnologias-que-estan-potenciando-el-internet-de-las-cosas/?_adin=02021864894

- Equipo editorial, Etecé. (2021, 16 julio). *Red inalámbrica - qué es, tipos, ventajas, desventajas y ejemplos.* Concepto. https://concepto.de/red-inalambrica/

- Itop. (2021). *La relación entre el Internet de las Cosas y la Inteligencia Artificial.* Itop.es. https://www.itop.es/blog/item/la-relacion-entre-internet-de-las-cosas-y-la-inteligencia-artificial.html

- Jiménez, J. (2023, 18 mayo). Top 5 de amenazas en la red actualmente y cómo evitarlas. *RedesZone.* https://www.redeszone.net/noticias/seguridad/principales-amenazas-red-consejos-seguridad/

- Molina, D. (2022, November 24). *Tendencias del internet de las cosas (IoT) en 2023.* Thinking for Innovation. https://www.iebschool.com/blog/tendencias-internet-de-las-cosas-tecnologia/

- *OpenMind.* (2017, July 18). OpenMind. https://www.bbvaopenmind.com/tecnologia/mundo-digital/por-que-internet-de-las-cosas-necesita-inteligencia-artificial/

- Ramírez, H. (2023, 31 julio). *Relación entre privacidad y ciberseguridad en la protección de datos.* Grupo Atico34. https://protecciondatos-lopd.com/empresas/ciberseguridad-privacidad/

- *Seguridad de IoT: ciberseguridad de IoT* — Microsoft Azure. (2023). Microsoft.com. https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-iot/security

- School, T. (2023, 14 julio). *El internet de las cosas: su evolución en los últimos años*. Tokio School. https://www.tokioschool.com/noticias/internet-de-las-cosas-evolucion/

- Team, A. (s. f.). *Tipos de vulnerabilidades y amenazas informáticas.* https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas