CIBERSEGURIDAD

EN EL

Internet de las Cosas (OIT)

Ciberseguridad en **el Internet de las Cosas (IoT)**

Expertos sostienen que el Internet de las Cosas (IoT, por sus siglas en inglés) hace parte fundamental de la cuarta revolución industrial. También, que su capacidad para cambiarnos el estilo de vida, la forma cómo trabajamos, nos relacionamos, y más aún, la forma como concebimos internet, es alucinante.

Sin embargo, hay quienes, sin demeritar sus bondades, también alertan sobre las consecuencias de esta nueva tecnología que irrumpen sin barreras en la información, seguridad, intimidad y privacidad de las personas y las industrias.

En este e-book leerás un poco de cada punto de vista, conocerás en concreto de qué se habla cuando hablamos de Internet de las Cosas y te llevarás consejos y recomendaciones prácticas, ya que no queremos que te quedes atrás sin probar un poco de esta tecnología que está permeando y seduciendo la mayoría de sectores económicos de la sociedad.

¡Esperamos que tengas una buena lectura!

Contenido

- Definición de Internet de las Cosas.
- Panorama actual de IoT en cifras.
- Dispositivos IoT e industrias que los implementan.
- Ciberseguridad y ciberataque en el entorno IoT.
- Internet de las Cosas sí pero con seguridad: Recomendaciones.

Algunas definiciones de Internet de las Cosas (IoT)

Quisimos reunir diversas definiciones del concepto Internet de las Cosas o Internet de los Objetos (Internet of Things: IoT).

Pero antes, algo de historia: el concepto IoT nació en el Instituto de Tecnología de Massachusetts en 1999 y básicamente consiste en la manipulación inalámbrica de diferentes objetos conectados a Internet, junto con el análisis de la información obtenida a través de ellos. Para el 2000, ya se pasaba de la teoría a la práctica con algunos proyectos; en 2004 ya se estaban haciendo avances con GPS; y hoy la interconexión parece no tener límites: neveras, relojes, parlantes, carros, puertas, bombillas, alarmas, cámaras, zapatos... la lista es larga.

El IoT es una ficha clave en la transformación digital de las empresas —permite mejorar procesos de calidad de producto, entender lo que pasa en las operaciones con datos en tiempo real, optimizar costos, entre otros beneficios— y una tendencia como objeto de deseo de las personas, ya que dentro de sus bondades ofrece: comodidad, practicidad, inmediatez, ahorro, acceso a la información en tiempo real, predictibilidad y automatización, entre otras.

¿Qué es el Internet de las Cosas?

Así lo han definido algunos expertos:

- **Santiago Arreche,** Ingeniero de software, experto en gestión de proyectos y desarrollo de procesos, **a través de Quora** responde:

"El concepto de Internet de las Cosas (IoT) viene de poder interactuar con objetos cotidianos a través de la red. Esto tiene múltiples aplicaciones en diferentes áreas:

- Ciudades inteligentes: gestión del tráfico, estacionamiento, luces.
- Casas inteligentes (domótica): luces, temperatura, cocina, etc.
- Elementos vestibles (wearables): relojes, ropa, zapatillas, etc.

- Industria: cadena de valor, gestión de la producción.
- Salud: control de medicación, comportamiento, etc.

- **Ángel Sánchez, cofundador de Geeksme,** empresa española desarrolladora de IoT, argumenta para un artículo en Retina:

"Cuando hablamos de IoT, hablamos de la próxima frontera de Internet. No se trata de una nueva tecnología atractiva pensada para vender más móviles o un nuevo uso concreto, sino de una nueva forma de entender la aplicación de Internet para mejorar todos los ámbitos de nuestra vida".

- Esta otra definición que rastreamos en la revista **Muy Interesante:**

“Se trata una revolución en las relaciones entre los objetos y las personas, incluso entre los objetos directamente, que se conectarán entre ellos y con la Red y ofrecerán datos en tiempo real. O dicho de otro modo, se acerca la digitalización del mundo físico”.

- Y una definición final que no queremos dejar de citar, del experto **Nicolás Rivera, redactor de la web Hipertextual:**

“Muy resumidamente, el Internet of Things es un concepto que se basa en la interconexión de cualquier producto con cualquier otro de su alrededor. Desde un libro hasta el frigorífico de tu propia casa. El objetivo es hacer que todos estos dispositivos se comuniquen entre sí y, por consiguiente, sean más inteligentes e independientes”.

Hagamos una recapitulación de lo ya dicho y citado: IoT es una tecnología revolucionaria que se impone para "cambiarnos el chip" de cómo ha sido concebido hasta ahora el Internet.

En apariencia, una invención con el propósito de mejorar el estilo de vida de las personas, la producción de las empresas y llevar la transformación digital a la ene potencia, pero ¿a qué costo?, ¿qué pasa con la privacidad de la información a la que pueden acceder estos objetos inteligentes?, ¿qué implicaciones o amenazas trae consigo?, ¿qué papel juega la ciberseguridad en toda esta revolución?

Panorama actual de IoT

Revisemos el panorama actual del Internet de las Cosas a través de cifras, tanto en el ámbito empresarial como de consumo:

- "Ericsson estima que, para 2022, alrededor de 29 mil millones de dispositivos estarán conectados. De estos, 18 mil millones estarán relacionados con IoT y serán de consumo, brindando numerosos beneficios a los hogares". **(Fuente: Eset).**

- Otros van mucho más lejos, Statista estima que para 2025 habrá ya 74.440 millones de objetos IoT a nivel global.

- Así está el interés de los empresarios colombianos por el Internet de las Cosas, según una encuesta de la Andi y la firma analista global IDC:

El **56,3%** de los consultados no conoce bien las aplicaciones del IoT

Solo dos de cada **10** empresas en Colombia utilizan soluciones de IoT

78,5% considera importante **promover el uso en sus empresas**

La inversión en IoT en Colombia es solo de **0,02%,** en comparación con China (26%) y Estados Unidos (27%) (Fuente: La República)

- Sectores que más invirtieron en Internet de las Cosas en Colombia:

    - Industria, con una cifra cercana a los 98 millones de dólares.

    - Seguida de logística, con 80 millones. (Fuente: Resultados Índice de Innovación de la Sociedad 2017, QuISI).

- “En solo veinte años, el 45% de las compañías estarán obsoletas debido al avance de la inteligencia artificial y del Internet de las Cosas”. **(Fuente: Capital Inteligente).**

Objetos inteligentes transformando el mundo

Son varios los sectores de la sociedad que se han "reinventado" gracias a IoT, encontrando en esta tecnología la forma de ahorrar tiempo, dinero, mejorar y optimizar sus procesos. Pero, ¿de qué concretamente hablamos cuando hablamos de Internet de las Cosas?

- "Un objeto no tiene que "nacer" inteligente, sino que puede evolucionar gracias a sensores externos que se acoplan y permiten monitorizar su uso para saber cómo se utilizan realmente [...] ¿Cuántas veces se utiliza una silla en la oficina o el casco en una obra, qué uso hacemos de un colchón en nuestro hogar, es posible que el sillón de mi

casa me avise de que mi familia está segura? Son solo algunas preguntas que podremos responder dentro de poco, gracias al IoT". **(Fuente: Retina)**

Por ahora, conozcamos algunas de las invenciones que ya existen, aunque te advertimos, son solo "algunas", porque de lo contrario la lista sería extensa.

Consumo

- Refrigeradoras que alertan a los usuarios cuando un producto se está acabando o caducando. Incluso, encargan ellas mismas estos productos a los proveedores.

- Altavoces inteligentes, como Alexa o Google Home.

- Automatización o domótica en los hogares: bombillas que se encienden al detectar movimiento, control de las ventanas, temperatura, entre otros.

- Botones inteligentes de Amazon: “La compañía, en acuerdo con varias marcas, ha creado botones inteligentes que permiten encargar los productos que se acaben en tu hogar con tan sólo pulsar el botón. La idea es desprenderse de la lista de la compra. Amazon recibe la orden de compra y la procesa para realizar el envío directamente a tu domicilio”. **(Fuente Geeksme).**

Salud

Dispositivos “wearables” (camisetas, relojes, zapatillas deportivas, pulseras), lanzados al mercado por marcas como FitBit, Nike, Jawbone, Samsung y Apple.

Estos objetos de uso cotidiano están diseñados para que los usuarios obtengan en tiempo real datos sobre su salud, que les permitan tomar decisiones fundamentadas y más acertadas sobre su estado físico, sobre sus rutinas deportivas, y en consecuencia, mejorar su estilo de vida.

Seguridad para empresas y hogar

Para dar un ejemplo sobre este segmento, con las ventajas y bondades de los nuevos componentes tecnológicos, la empresa de seguridad Atlas, se apoyó en los dispositivos IoT para robustecer el componente de seguridad de sus clientes.

Muestra de ello es el servicio **“Ecosistema de Internet de las Cosas”** que consiste

en diferentes soluciones para empresas y hogares, de monitoreo, detección anticipada, expulsión de intrusos y control de cadena de frío, entre otras, fundamentadas en IoT.

“Implementamos IoT de una manera segura”, cuenta Iván Ocampo Rengifo, jefe nacional de Ciberseguridad e Informática en Atlas. “Somos conscientes de los riesgos tecnológicos de este tipo de dispositivos, porque están dentro de una infraestructura de red, y si no se siguen parámetros de seguridad, la tecnología que en un principio se pensó usar en un tema de protección, se convierte por el contrario en un factor de vulnerabilidad para las instalaciones”.

En las ciudades

- Parqueaderos sensorizados para alertar disponibilidad de aparcamiento por zonas.

- Redes de sensores que informan sobre calidad del aire en tiempo real.

- Señales de tráfico: “Aplicando el IoT, si vamos a una velocidad mayor de la que está permitida, nuestro coche la reduciría de forma automática al recibir los datos de alguna de las señales que nos rodean. Esto, paralelamente, facilitará la llegada y expansión de los coches autónomos en nuestras vidas”. **(Fuente: Hipertextual).**

- Redes Eléctricas Inteligentes que controlan el consumo de energía en una localidad o región.

Para la agricultura

- Sensores para monitoreo de cultivos.
- Sensores integrados a estaciones meteorológicas.
- Controlador de calidad del agua de riego con IoT para mejorar la producción de cultivos.

“Esta tendencia, por supuesto, plantea retos, además de oportunidades. Más dispositivos en el hogar o la oficina implica nuevas posibilidades de hackeo y más datos privados recolectados, más información a proteger”, escribe el experto

Ángel Sánchez en un artículo para Retina.

Ciberseguridad y ciberataque en el entorno IoT

El cibercrimen o ciberataque busca, a través de maniobras ofensivas y con fines perjudiciales, "tomar el control, desestabilizar o dañar un sistema informático [...] Un ciberataque utiliza códigos maliciosos para corromper otros códigos, datos privados o

algoritmos, generando consecuencias que comprometen y vulneran la seguridad de los sistemas de información". (Fuente: Wikipedia).

Y, como plantea **Juan David Pineda, coordinador técnico del centro de computación científica Apolo, de la Universidad Eafit,** "todo lo que esté conectado a Internet no deja de ser susceptible de ataque".

¿Qué riesgos trae el Internet de las Cosas?

La ciberseguridad y el Internet de las Cosas se encuentran fuertemente relacionadas, ya que con esta tecnología, la información, los datos y la seguridad están más vulnerables que antes.

El IoT trae consigo un despliegue de dispositivos útiles e innovadores que, al mismo tiempo, están exponiendo desde varios frentes la seguridad de las empresas y las personas.

Así lo expone Moisés Barrio, autor del libro Internet de las Cosas:

> "Además de las preocupaciones en materia de seguridad de los productos y de ciberseguridad en las plataformas,

el Internet de las Cosas también plantea una serie de implicaciones relevantes para la intimidad y la privacidad, en particular y muy significativamente con respecto a los dispositivos de consumo".

Hay otras opiniones al respecto.
Por ejemplo, la de **Miguel Ángel Mendoza, especialista en seguridad informática de Eset Latinoamérica:**

"IoT, como cualquier tecnología, busca ofrecer ventajas a los usuarios, facilitar muchas de las actividades que realizamos de manera cotidiana. Sin embargo, existen personas mal intencionadas que quieren aprovecharse de las fallas asociadas a estos dispositivos, buscarlos desde cualquier punto de la red, intentar explotar esas fallas y llevar a cabo acciones maliciosas

como tomar el control de dichos dispositivos, robar información que esté siendo procesada, vigilar a través de la cámaras o micrófonos, etc".

Y se detiene en la acción maliciosa "tomar el control de dichos dispositivos", para darnos un ejemplo. El jackware, concepto acuñado por **Stephen Cobb,** también **experto e investigador de Eset.**

"Jackware (aún en teoría) es un software malicioso "que intenta tomar el control de un dispositivo cuyo objetivo principal no es el procesamiento de datos ni la comunicación digital. Un automóvil, por ejemplo, sería uno de estos dispositivos, una forma especializada de ransomware cuyo objetivo es bloquearlo hasta que pagues el

rescate". **(Fuente: Jackware, cuando los autos conectados conocen al ransomware).**

Casos de ataques con dispositivos IoT ya han ocurrido.

En 2016 se presentaron ataques masivos a portales como Twitter, Spotify, Netflix y Airbnb a través de routers domésticos, cámaras de vigilancia y otros objetos inteligentes que quedaron infectados por un código malicioso que lanzó un ataque de denegación de servicio y dejó estas web fuera de línea. Es un secreto a voces que dispositivos como Alexa y **Google Home escuchan** y graban lo que estamos hablando.

Frente a estas situaciones de seguridad, **Juan Guillermo Lalinde, coordinador de la maestría en ciencia de los datos y analítica de la Universidad Eafit,** nos cuenta:

> “Son pocas las empresas de desarrollo de software que entrenan a sus desarrolladores para hacer desarrollo seguro [...] Los fabricantes, en su gran mayoría, están interesados en llegar con un producto al mercado de consumo, y están llegando a un mercado donde la gente todavía no es consciente de la importancia de la privacidad y el riesgo que tiene el manejo de su información, el límite de la seguridad está desapareciendo”.

Internet de las Cosas sí, **pero con seguridad**

¿Recuerdas que al principio nos planteamos varios interrogante sobre IoT?

¿A qué costo? ¿Qué pasa con la privacidad de la información a la que pueden acceder estos objetos inteligentes? ¿Qué implicaciones o amenazas trae consigo? ¿Qué papel juega la ciberseguridad en toda esta revolución?

En este capítulo final, y con la ayuda de varios expertos, reunimos algunos consejos y recomendaciones de seguridad que apuntan también a dar respuesta a estos cuestionamientos y que recomendamos aplicarse de acuerdo a su finalidad, tanto en ámbitos empresariales como personales.

"Si bien hay una responsabilidad del fabricante del dispositivo, el consumidor también tiene una responsabilidad. Indiferente de dónde se produzca el dispositivo, este debería contar con parámetros de seguridad, pero la persona que comience a usarlo debería verificar estos parámetros y consultar si es seguro o no". **Juan David Pineda, coordinador técnico, del centro de computación científica Apolo, en Eafit.**

“Se debe crear conciencia acerca de los peligros, de los riesgos a los que se expone la seguridad al usar dispositivos IoT, con más información tomamos mejores decisiones. La idea no es dejar de usar la tecnología, hay que utilizarla, pero de una manera más segura, consciente y responsable”. **Miguel Ángel Mendoza, especialista en seguridad informática de Eset Latinoamérica.**

“Los dispositivos IoT vienen con credenciales de acceso por defecto de fábrica, que pueden estar publicadas en un manual en Internet. Hay que eliminar las contraseñas por defecto y generar unas nuevas para el uso del dispositivo, además, que estas contraseñas sean fuertes y no 12345”. **Iván Ocampo Rengifo, jefe nacional de ciberseguridad e informática en Atlas.**

“La mayoría de las empresas, medianas y pequeñas, no son conscientes de la seguridad de la información y no tienen políticas o gestión del riesgo apropiada para la gestión de la seguridad de la información. ¡Eso tiene que cambiar!”
Juan Guillermo Lalinde, coordinador de la maestría en Ciencia de los Datos y Analítica en Eafit.

Tips de seguridad en IoT

- Negociar una licencia antivirus para la empresa, que cubra también el hogar de los empleados. Estos, al tener mayor seguridad en la casa, están contribuyendo a que la empresa esté más alejada de ciberataques.

- Documentarse de lo que se está comprando: ¿qué garantías ofrece?, ¿a qué estoy accediendo a la hora de comprar e instalar este dispositivo?, ¿es un fabricante reconocido o es un fabricante genérico que no te responde por nada de garantías?

- Ser muy cuidadosos: hasta un bombillo inteligente mal desechado o tirado a la basura sin más podría ser hackeado.

- El dispositivo que se instale debe ser coherente con las políticas de seguridad de la organización.

- Mantener software y firmware actualizados: la actualización corrige las fallas y las vulnerabilidades ya identificadas.

- Desconectar de internet los dispositivos cuando no están siendo utilizados, así se reduce la ventana de exposición a este tipo de amenazas.

- Usar herramientas y soluciones de seguridad para estos dispositivos, por ejemplo, Eset lanzó recientemente una solución de seguridad para ciertas marcas de Smart TV. que permite identificar, bloquear y eliminar códigos maliciosos. Además de tener un módulo antiphishing.

Nos gustaría saber qué piensas de este tema o si sabes de otros puntos de vista interesantes que puedan alimentar este contenido. Escríbenos a **info@resetmarketingdigital.com.**

Si quieres seguir leyendo y aprendiendo con nosotros sobre transformación digital, innovación y nuevas tecnologías.

Reset

Una idea Bancolombia