Content Unit

[Internet de las cosas]

Proyecto: B-SAFE
Número: 2018-1CZ01-KA204-048148
Nombre del autor: EDIT VALUE®
Última fecha de procesamiento: 02.09.2020

Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

Internet de las cosas

Introducción

En la cuarta revolución industrial, denominada Industrial 4.0, y con un impacto más directo para el individuo como usuario final, se encuentra Internet de las cosas, comúnmente conocido como IoT (Internet of Things).

El IoT es un sistema de dispositivos informáticos interrelacionados, máquinas mecánicas y digitales, objetos, animales o personas que tienen la capacidad de transferir datos a través de una red sin requerir interacción de persona a persona o de persona a computadora. El primer dispositivo IoT "oficial" fue una máquina de Coca-Cola en el campus de la Universidad Carnegie Mellon en Pittsburgh, Pensilvania, en 1982. Los estudiantes querían saber de antemano si las latas de refresco recién cargadas estaban en su punto más frío, por lo que manipularon la máquina para reportar esta información a un ordenador en una oficina cercana.

A pesar de su antigüedad, la tecnología IoT está en constante evolución, por lo que enfrentamos cambios disruptivos relacionados con nuestros hábitos de vida, ya que hay una gran cantidad de oportunidades y posibles aplicaciones de IoT, ya sea en entornos industriales o en la vida cotidiana.

Si bien proporciona soluciones efectivas y eficientes para muchos problemas del mundo real, existen desafíos importantes con respecto a la seguridad y la privacidad que no deben ignorarse.

Relevancia práctica: esto es para lo que necesitarás el conocimiento y las habilidades

Después de aprender esta unidad de contenido, sabrás qué es Internet de las cosas y cuáles son las principales aplicaciones de esta nueva tecnología.

Además, aprenderás sobre los problemas más comunes relacionados con la seguridad y la privacidad de IoT, así como sobre cómo reaccionar en caso de un ataque cibernético a cualquiera de tus dispositivos inteligentes.

1. Construye conocimiento – Internet de las cosas en la vida cotidiana

Co-funded by the
Erasmus+ Programme
of the European Union

A lo largo de los años, ha habido un rápido crecimiento en el dominio de Internet de las cosas (IoT) en términos de tecnología y crecimiento del mercado. La conexión en red de los ordenadores llamada "Internet" revolucionó la forma en que compartimos la información. El IoT puede considerarse como la próxima revolución en la forma en que percibimos y compartimos la información (Virat, 2018). En el cuadro a continuación puedes acceder a una definición simplificada de IoT:

Definición

Internet de las cosas es el concepto de conectar cualquier dispositivo (siempre que tenga un interruptor de encendido/apagado) a Internet y a otros dispositivos conectados. El IoT es una red gigante de cosas y personas conectadas, todas las cuales recopilan y comparten datos sobre la forma en que se utilizan y sobre el entorno que las rodea.

Los dispositivos y objetos con sensores integrados están conectados a una plataforma de Internet de las cosas, que integra datos de los diferentes dispositivos y aplica análisis para compartir la información más valiosa con aplicaciones creadas para satisfacer necesidades específicas. En la figura a continuación puede encontrar dos buenos ejemplos de una tecnología IoT.

Como hemos visto antes, el IoT es un término amplio que se usa para referirse a la vasta red de dispositivos conectados a Internet que existen hoy en día.

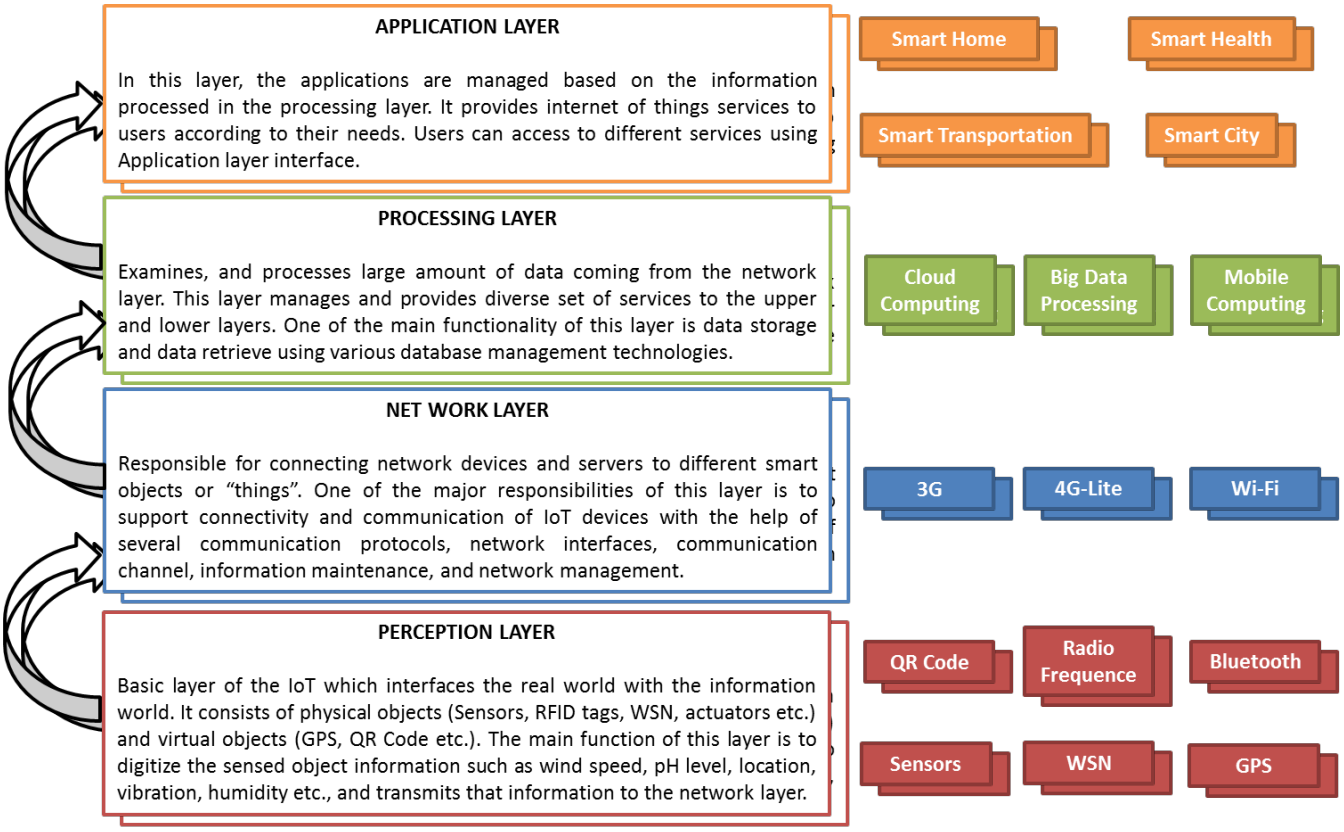
Co-funded by the
Erasmus+ Programme
of the European Union

El Internet de las cosas promete ser el desarrollo tecnológico más importante para los consumidores desde la llegada del teléfono inteligente. Los expertos creen que esta tecnología eventualmente generará más de 123 mil millones de dólares en ingresos anuales para 2021 y las estadísticas señalan que habrá más de 36 mil millones de dispositivos conectados a Internet para fines de 2020.

De hecho, las principales empresas, como Amazon, Google y Tesla ya están trabajando con servicios de desarrollo de software para producir dispositivos IoT de última generación. Se espera que el IoT haga realidad las casas inteligentes avanzadas. Más ejemplos de tecnologías de IoT incluyen automóviles sin conductor, dispositivos portátiles que rastrean marcadores corporales, adherencia del paciente a cambios de comportamiento, asistentes de voz (por ejemplo, Alexa), sistemas de calefacción inteligentes, etc.

Por ello, podemos reconocer fácilmente que la sociedad en general estará en contacto con un dispositivo IoT en cierto momento. Por lo tanto, es muy importante mejorar el comportamiento general de los ciudadanos y su privacidad/seguridad.

Co-funded by the
Erasmus+ Programme
of the European Union



también hacen que IoT sea vulnerable y arriesgado en términos de seguridad y privacidad. Para comprender la complejidad de este desafío, debes comprender la arquitectura básica de IoT, caracterizada por una estructura dinámica. El número de capas que compone la arquitectura de IoT difiere enormemente entre los expertos, pero todos están de acuerdo en que IoT está compuesto por al menos cuatro capas: Percepción, Red, Procesamiento y Aplicación.

Como puedes observar, la capa de aplicación facilita la gestión global de las aplicaciones inteligentes y proporciona servicios específicos al usuario. En la siguiente tabla, se presentan las principales aplicaciones de IoT en la vida cotidiana:

Casa Inteligente	Es un hogar interconectado donde todo tipo de cosas interactúan entre sí a través de Internet. Por ejemplo, en una casa inteligente, puedes encender el aire acondicionado de camino a casa o puedes activar la lavadora mientras estás en el trabajo. Esencialmente, todo está interconectado para hacer su vida más simple y conveniente.
Usables	Estos dispositivos (como Fit Bit) recopilan datos e información sobre el usuario que luego se procesan para extraer información esencial. Estos dispositivos pequeños y altamente eficientes cubren ampliamente los requisitos de acondicionamiento físico, salud y entretenimiento.
Coches Inteligentes/ Conectados	Un vehículo inteligente que puede optimizar su propio funcionamiento, mantenimiento y comodidad de los pasajeros. Estos vehículos se están utilizando en el transporte inteligente, que incluye vías fluviales, ferrocarriles, carreteras, etc., que reciben información en tiempo real sobre carreteras, accidentes, desvíos y cierres de carreteras, de manera que proporciona la máxima seguridad para el conductor y los pasajeros.
Ciudades Inteligentes	Involucra todo lo que compone una ciudad, como la vigilancia, el transporte, los sistemas de gestión de energía, la distribución de agua, la seguridad urbana y el monitoreo ambiental. Por ejemplo, el gobierno puede ser informado automáticamente sobre los niveles medidos de contaminación o la escasez de suministros de energía, etc.
Agricultura Inteligente	Los agricultores están utilizando información significativa de los datos recogidos para obtener un mejor retorno de la inversión. La detección de la humedad y los nutrientes del suelo, el control del uso del agua para el crecimiento de las plantas y la determinación de fertilizantes personalizados son algunos de los usos simples de IoT.
Administración de Energía	Las redes eléctricas del futuro no solo serán lo suficientemente inteligentes sino también altamente confiables. En las redes eléctricas inteligentes, el uso de medidores inteligentes, puertas de enlace domésticas, enchufes inteligentes y electrodomésticos conectados ayuda a conservar los recursos y ahorrar dinero para los consumidores, fabricantes y proveedores de servicios públicos..
Sanidad Inteligente	Un sistema de salud conectado y dispositivos médicos inteligentes representan una revolución para la sociedad, ya que tiene un impacto significativo no solo para las empresas, sino también para el bienestar de las personas en general. La aplicación de IoT en el ámbito de la atención médica incluye la obtención de información sobre

	los parámetros de salud de un individuo, como la presión arterial, la temperatura corporal, las mediciones del latido cardíaco, etc. a través de dispositivos portátiles de bajo consumo de energía, altamente eficientes y de pequeño tamaño. Esta información recopilada se puede compartir con las personas respectivas y los centros de atención médica para que los médicos puedan tomar medidas adicionales.

Co-funded by the
Erasmus+ Programme
of the European Union

1. Aplica conocimiento

Ejercicio ELECCIÓN ÚNICA

Objetivo específico asociado: OE_Internet de las cosas en la vida cotidiana_O1_O1:

Situación: ¿Qué es el "Internet de las cosas"?
Tarea: Por favor, identifica la opción correcta siguiendo el principio de elección única: solo una respuesta es verdadera.

- **IoT es una red de servidores conectados a los que se accede a través de Internet.**
- IoT es la digitalización y automatización de cada parte de la empresa, así como el proceso de fabricación.
- IoT es una red global de área amplia que conecta sistemas informáticos en todo el mundo.
- IoT es una tecnología incipiente que se centra en la interconexión entre cosas o dispositivos entre sí y con humanos o usuarios para lograr algunos objetivos comunes.

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Internet de las cosas en la vida cotidiana_O1_O2:

Situación: ¿Cuáles son las principales aplicaciones de Internet de las cosas?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple. Ninguna, una, más de una o todas las opciones pueden ser verdaderas

- Monitoreo de línea eléctrica y transmisión de energía de red inteligente.
- Gestión de la cadena de suministro de producción al por menor.
- Gestión de la cadena de suministro de producción en la industria transformadora.
- Regulación del agua en la agricultura.

---

2. Construye conocimiento – Internet de las cosas y cuestiones de seguridad y privacidad

Los dispositivos inteligentes de consumo conectados al Internet de las cosas recopilan constantemente información personal de los consumidores. Por lo tanto, una de las mayores preocupaciones relacionadas con la implementación de Internet de las cosas en nuestra vida cotidiana está relacionada con la seguridad y la privacidad de la información personal e incluso confidencial, ya que el robo de información personal puede causar graves daños a las personas, las empresas y en general a la sociedad. IoT es una tecnología ubicua con una arquitectura y estructura complejas. En consecuencia, crea nuevos problemas de seguridad y privacidad, hasta ahora considerados inofensivos o indefinidos. Esas preocupaciones están relacionadas principalmente con:

1. Las tecnologías de IoT tienen una vida útil más larga en comparación con los teléfonos inteligentes y los ordenadores de sobremesa.
2. Hay varios números de fabricantes, la mayoría sin experiencia en tecnología de la información (TI) tradicional, lo que resulta en problemas de interoperabilidad y falta de seguridad en la seguridad.

3. Esta falta de experiencia en TI se extiende a los usuarios finales (que son todos administradores de sistemas de facto).
4. La cantidad de dispositivos y la conexión global exacerban todos los problemas. De hecho, se estima que hay 50 mil millones de dispositivos conectados en este momento.

La seguridad de los datos y la privacidad del usuario son conceptos diferentes, pero no son mutuamente excluyentes. De hecho, un ataque de seguridad o ataque cibernético compromete automáticamente la privacidad del usuario.
Los desafíos que deben superarse para resolver los problemas de seguridad y privacidad de IoT son inmensos. Esto se debe principalmente a las muchas restricciones asociadas a la provisión de seguridad y privacidad en los sistemas IoT. Sin embargo, a continuación se presenta en el cuadro una breve definición de esos conceptos, aplicados a IoT.

El tipo de amenazas y ataques de seguridad y privacidad a los que IoT está sujeto depende de sus capas, ya que cada capa tiene particularidades y tecnologías asociadas diferentes. En la siguiente tabla se muestra un resumen de los ataques cibernéticos más comunes al marco de IoT, así como el grado de impacto en las cuatro capas que componen la arquitectura de IoT:

	Breve descripción	**CAPA DE PERCEPCIÓN**	**CAPA DE RED**	**CAPA DE PROCESAMIENTO**	**CAPA DE APLICACIÓN**
Código malicioso	Cualquier código en cualquier parte de un sistema de software o script que tenga la intención de causar efectos no deseados, violaciones de seguridad o daños a un sistema	**Alto**	**Alto**	**Bajo**	**Alto**
Ataque de DoS	Ataque cibernético en el que el autor intenta hacer que una máquina o recurso de red no esté disponible	**Bajo**	**Alto**	**Alto**	**Bajo**
Información de enrutamiento	Protocolos que los enrutadores pueden usar para intercambiar información de topología de red	**Bajo**	**Alto**	**Alto**	**Bajo**
Espionaje	Es el acto de escuchar en secreto o sigilosamente la conversación privada o las comunicaciones de otros sin su consentimiento.	**Alto**	**Medio**	**Alto**	**Medio**
Robo de identidad	El uso deliberado de la identidad de otra persona generalmente como un método para obtener una ventaja financiera u otra información personal	**Alto**	**Medio**	**Alto**	**Medio**
Ataque de sumidero	Amenaza la seguridad de WSN en casi todas	**Medio**	**Alto**	**Bajo**	**Bajo**

	las capas de su pila de protocolos				
Ataque de suplantación de identidad	Intento fraudulento de obtener información o datos confidenciales típicamente realizados por suplantación de correo electrónico o mensajería instantánea	**Bajo**	**Bajo**	**Medio**	**Alto**

Como puedes observar, existe una gran variedad de posibles ataques que pueden comprometer la seguridad y la privacidad de los dispositivos IoT con un nivel de impacto diferente según la capa. Por lo tanto, hay desafíos considerables que deben ser abordados por todas las partes involucradas: fabricación o desarrollador de IoT, gobierno y usuario final.

2. Aplica conocimiento

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Internet de las cosas en la vida cotidiana_O2_O1:

Situación: en cuanto a la seguridad de los dispositivos IoT y sus usuarios, ¿qué afirmaciones son ciertas?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple. Ninguna, una, más de una o todas las opciones pueden ser verdaderas

- La seguridad de los datos se requiere cuando los datos se generan y almacenan.
- Los requisitos de seguridad para las aplicaciones de IoT deben aplicarse en tres capas: capa de aplicación, capa de red y capa de percepción.
- La probabilidad de que ocurra un ataque de phishing en un dispositivo IoT es mayor en su capa de procesamiento.

- La arquitectura de IoT permite a las entidades maliciosas explotar vulnerabilidades intrínsecas a cada una de las capas de IoT.
- Un código malicioso puede afectar al menos a tres capas.

Ejercicio ELECCIÓN ÚNICA

Objetivo específico asociado: OE_Internet de las cosas en la vida cotidiana_O1_O2:

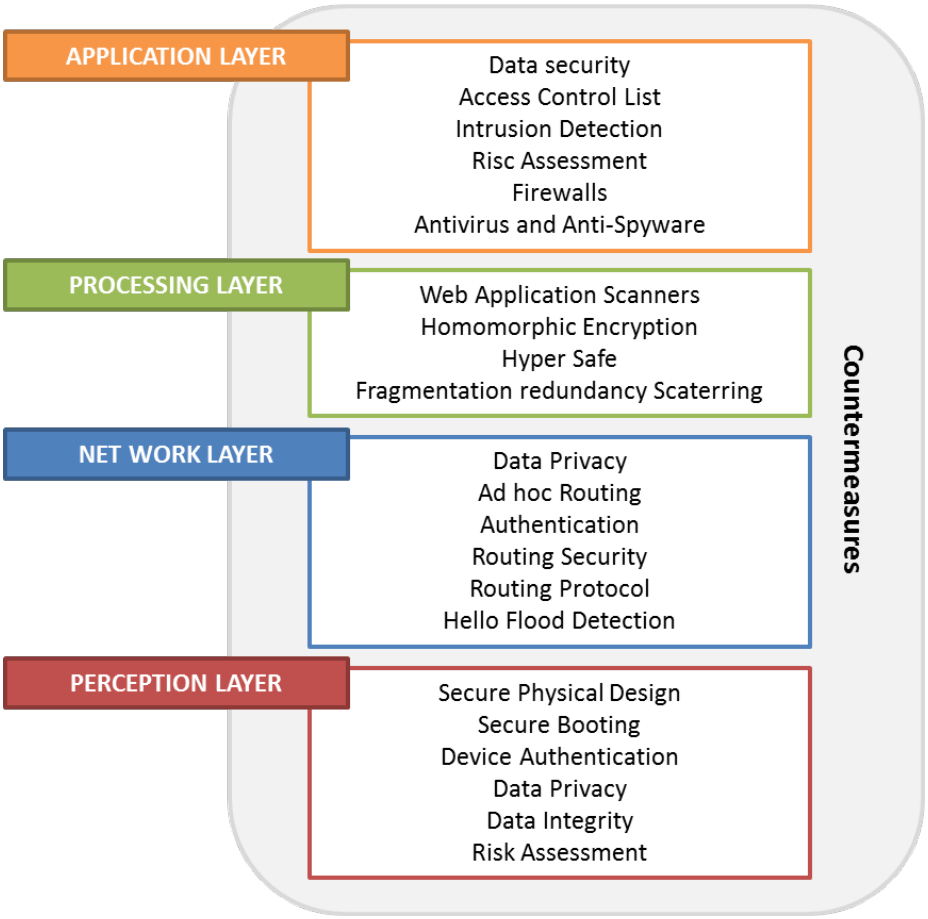
Situación: en consideración de la privacidad del usuario de IoT, ¿qué afirmación es verdadera?
Tarea: Por favor, identifica la opción correcta siguiendo el principio de elección única: solo una respuesta es verdadera.

- El crecimiento significativo que ha demostrado el IoT durante los últimos años ha generado varias preocupaciones de privacidad a medida que disminuye la disponibilidad de datos, patrocinado por las propiedades comunes y habituales del IoT.
- Los artículos necesitan garantizar la protección de la información personal de los usuarios asociada a sus movimientos, hábitos e interacciones.
- La privacidad se refiere a cómo de bien los dispositivos IoT se defienden contra el robo de datos del usuario.
- La privacidad solo está en riesgo en la capa de aplicación.

3. Construye conocimiento – Internet de las cosas y la protección de sus usuarios

A principios del año de 2019, CNN logró acceder a una variedad de transmisiones de cámara utilizando un motor de búsqueda para dispositivos IoT Shodan. Observaron remotamente a niños jugando en el gimnasio de una escuela secundaria en Indonesia, un hombre preparándose para irse a la cama en un apartamento de Moscú, una familia australiana que entraba y salía de su garaje y una mujer que alimentaba a su gato en Japón. Todos parecían ignorar el hecho de que estaban transmitiendo sus vidas en línea cada segundo del día. Según CNN, ninguna de las cámaras había tenido controles de seguridad y estaban abiertas a cualquiera que supiera la dirección correcta.

Para evitar que le ocurra este tipo de situación, existen algunas técnicas, procedimientos y comportamientos que deben ser adoptados tanto por el desarrollador del dispositivo IoT como por el usuario del dispositivo inteligente. A continuación puede ver algunas medidas para reaccionar y evitar ataques cibernéticos en todas las capas que componen los dispositivos IoT.



Como puedes observar, la mayoría de los mecanismos de privacidad y seguridad para IoT deben implementarse. Los desarrolladores de IoT deberían centrar sus esfuerzos en la creación de dispositivos que estén físicamente seguros y protegidos con algoritmos criptográficos, plataformas de puerta de enlace reforzadas, cifrado complejo, antivirus, anti-spyware, anti-adware y técnicas de seguridad avanzadas y actualizadas. Por lo tanto, el usuario depende del mecanismo de seguridad ya integrado en los dispositivos IoT para garantizar su privacidad y seguridad. Sin embargo, hay algunas acciones que, como consumidor de IoT, debes tener en cuenta para afrontar varias amenazas de seguridad y privacidad de IoT:

1º - Lee los requisitos de seguridad y la política de privacidad de los dispositivos

Elige siempre un dispositivo IOT de un fabricante confiable y transparente. Tienes derecho a conocer las técnicas de seguridad implementadas en IoT.

Co-funded by the
Erasmus+ Programme
of the European Union

Además, siempre debes leer la política de privacidad del dispositivo, ya que debes saber cómo funciona tu dispositivo IoT y las razones por las cuales los dispositivos inteligentes IoT recopilan y usan tus datos. En pocas palabras, antes de usar un dispositivo IoT, deberías poder saber si puedes:

1. Acceder, ver y eliminar los datos recopilados a través de IoT;
2. Desconectar tus dispositivos IoT cuando quieras hacerlo;
3. Consentir el almacenamiento de datos personales en el dispositivo IoT.

2º – ¡Deja de usar la contraseña predeterminada!

Lo primero que debes hacer con tu dispositivo IoT es verificar si te permite cambiar las contraseñas predeterminadas. Utiliza siempre una contraseña única y segura para todos y cada uno de los dispositivos que poseas. ¡No olvides cambiar las contraseñas de tu enrutador Wi-Fi también!

3º – Desactivar el acceso remoto (WAN) al dispositivo

Si estás en casa ahora mismo, busca "cuál es mi dirección IP" en tu ordenador. Lo que ves allí es tu dirección IP WAN. Esta dirección es única en Internet en cualquier momento. Si viajas fuera de casa, esa dirección IP es lo que puedes usar para acceder a tus dispositivos domésticos inteligentes de forma remota. Si los dispositivos no están protegidos, la dirección IP es todo lo que se necesita cualquiera que quiera acceder a ellos. De hecho, ¡eso fue lo que CNN usó para acceder a una variedad de cámaras!

4º – Deshabilita las funciones que no se usan

Un dispositivo inteligente confiable es un dispositivo que te permite personalizar sus funciones. Por ejemplo, si no estás utilizando tu reloj inteligente para recopilar tus últimos datos de entrenamiento, deshabilita la conexión Bluetooth; o si no necesita grabar su ruta de desplazamiento, deshabilita el GPS y el rastreo de ubicación.

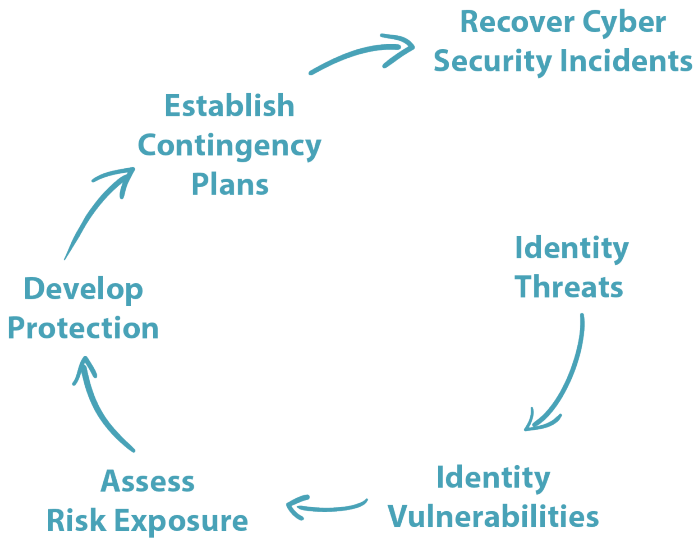
5º – ¡Sé un súper agente de la ciberseguridad!

¿Sabías que el 95% de las infracciones de ciberseguridad se deben a un error humano? Por lo tanto, la alfabetización en ciberseguridad es la forma principal de eliminar los ataques cibernéticos. Para ser un Superagente de Seguridad Cibernética, debes dominar todas las fases del plan de conciencia cibernética:

Ya sea porque uses dispositivos de Internet de las cosas en su vida diaria, o seas el propietario o gerente de un negocio que use tecnología e Internet en las actividades cotidianas, debes aumentar las posibilidades de detectar un ataque de seguridad o privacidad antes de que se active por completo, minimizando el daño y reduciendo el coste de recuperación.

A estas alturas, cuentas con todos los conocimientos básicos para tener éxito en la identificación de amenazas y vulnerabilidades, en la evaluación de riesgos y en la protección del dispositivo. Pero, ¿qué pasa si, a pesar de toda la prevención y cuidado, sigues siendo víctima de un ciberataque mientras usas Internet de las cosas? La respuesta se basa en las 4 preguntas: quién, qué, cuándo y cuál.

Co-funded by the
Erasmus+ Programme
of the European Union



QUIÉN
Haga una lista de a quién llamar en caso de un incidente. Es fundamental que sepa quién tomará la decisión de iniciar los procedimientos de recuperación y quién será el contacto principal con el personal policial apropiado.

QUÉ
Asegúrese de tener un plan sobre qué hacer con sus datos en caso de un incidente.
Esto puede incluir apagar y reiniciar todos sus sistemas de IoT.

CUÁNDO
Determine cuándo alertar al personal de emergencia, profesionales de ciberseguridad, proveedores de servicios o proveedores de seguros.

CUÁLES
Su plan de respuesta debe aclarar los tipos de actividades que constituyen un incidente de seguridad de la información. En lo que respecta a una organización, eso incluye incidentes como que su sitio web esté inactivo durante más de un período de tiempo especificado o evidencia de robo de información.

No olvide involucrar a su familia, amigos y/o empleados en el plan de concientización cibernética, ya que la ciberseguridad es una responsabilidad de todos los usuarios de IoT.

3. Aplica conocimiento

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Internet de las cosas en la vida cotidiana_O3_O1:

Situación: ¿Qué medidas de seguridad debes implementar para evitar ataques cibernéticos en tus dispositivos IoT?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple. Ninguna, una, más de una o todas las opciones pueden ser verdaderas

- Instalar cifrado homomórfico.
- Instalar cortafuegos.
- Crear dispersión de redundancia de fragmentación.
- Cambiar las contraseñas predeterminadas del enrutador.
- Desactivar funciones en mi dispositivo inteligente que no se están utilizando.
- Desactivar el acceso remoto al dispositivo inteligente.

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_Internet de las cosas en la vida cotidiana_O3_O2:

Situación: para convertirse en un súper agente de ciberseguridad, ¿qué debes hacer?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple. Ninguna, una, más de una o todas las opciones pueden ser verdaderas

- Aprender a programar para cifrar dispositivos IoT.
- Establecer un plan contingente siguiendo las 4 preguntas: "¿Qué se está generando?", "¿Dónde se almacenan los datos?", "¿Cuándo se usan los datos?" Y "¿Con quién se comparten los datos?"
- Establece un plan contingente siguiendo las 4 preguntas: "¿A quién llamar?" "¿Cuál es mi curso de acción?", "¿Cuándo alertar a otros?" Y "¿Qué actividades son incidentes?"
- Involucrar a toda mi familia, compañeros y empleados en la conciencia de seguridad cibernética.
- Desarrollar el plan de respuesta a la incidencia solo después de sufrir una brecha de seguridad, ya que es la única forma de conocer las acciones correctas para los incidentes que están por venir.

Sources

Analytics Vidhya (August 26, 2016). *10 Real World Applications of Internet of Things (IoT) – Explained in Videos.* Retrievd from https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/

Clark, J. (November 17, 2016*). What is the Internet of Things (IoT)?* Retrieved from https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

Evans, D. (2011). *The internet of things how the next evolution of the internet is changing everything.* Cisco White Paper, 1–11. Retrieved from

https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Griffiths, J. (February 2, 2019). *'Internet of things' or 'vulnerability of everything'? Japan will hack its own citizens to find out.* Retrived from https://edition.cnn.com/2019/02/01/asia/japan-hacking-cybersecurity-iot-intl

Kelbert, J. (September 24, 2019). *5 Interesting Facts About the IoT.* Retrieved from https://blog.flexis.com/5-interesting-facts-about-the-internet-of-things-iot

Co-funded by the Erasmus+ Programme of the European Union

Mena, D. M., Papapanagiotou, I. and Yang, B. (2018) *Internet of things: Survey on security.* Information Security Journal: A Global Perspective, 27:3, 162-182, DOI: 10.1080/19393555.2018.1458258

Finance Monthly (September 5, 2019). *The Worst And Weirdest IoT Hacks Of All Times.* Retrived from https://www.finance-monthly.com/2019/09/the-worst-and-weirdest-iot-hacks-of-all-times/

Ngo, D. (December 22, 2015). *Home networking explained, part 9: Access your home computer remotely.* Retrieved from https://www.cnet.com/how-to/home-networking-explained-part-9-access-your-home-computer-remotely/

Oorschot, P. C and Smoth, S. W. (2019). *The Internet of Things: Security Challenges.* IEEE Security and Privacy Magazine, 17(5):7-9. DOI: 10.1109/MSEC.2019.2925918

Spencer, T. (August 8, 2019). *How to Respond to a Cyber Attack.* Retrived from https://www.industryweek.com/sponsored/article/22028042/how-to-respond-to-a-cyber-attack

Viriat, M. S. et al. (2018). *Security and Privacy Challenges in Internet ofn Things*. Proceedings of the 2nd International Conference on Trends in Electronics and Informatics. IEEE Conference Record: # 42666; IEEE Xplore ISBN:978-1-5386-3570-4

Images
https://innovationatwork.ieee.org/low-power-low-latency-healthcare-iot/
https://messinaconstruction.com/smart-homes/smart-home-technology

Afianza conocimiento

Internet de las cosas, o simplemente IoT, es una palabra de moda en estos días. El IoT indudablemente cambiará la forma en que las personas interactúan con el mundo y la tecnología que las rodea. Esta red de dispositivos conectados a Internet tendrá muchos impactos positivos.

IoT representa una revolución en la forma en que interactuamos entre nosotros. De hecho, IoT creó nuevos tipos de interacción, ya que es una tecnología que permite la conexión entre cosas, procesos, personas, animales y casi todo lo que vemos a través del uso de Internet.

A pesar de ser un concepto simple, IoT necesita una arquitectura elaborada para funcionar correctamente. La arquitectura IoT se compone de al menos cuatro capas, a saber, capa de percepción, capa de red, capa de procesamiento y capa de aplicación. Es en esta última capa donde se encuentra la percepción de la utilidad de IoT, ya que representa aplicaciones inteligentes y dispositivos inteligentes que podrían usarse en muchos campos, haciéndolos "más inteligentes": hogares inteligentes, agricultura inteligente, ciudades inteligentes, atención médica inteligente, y muchos otros.

La dinámica, la inteligencia y la movilidad de IoT lo convierten en una tecnología de alta demanda, pero también hace que IoT sea vulnerable y arriesgado en términos de seguridad y privacidad. Todas las capas de IoT están sujetas a diferentes ataques cibernéticos. Por lo tanto, los diseñadores de dispositivos inteligentes deben participar activamente en el desarrollo de medidas efectivas de seguridad y privacidad, lo que hace que IoT sea más robusto en términos de seguridad.

Sin embargo, la principal causa de vulnerabilidad de IoT es la falta de conciencia de seguridad. Las personas, las empresas y la sociedad en general deben participar en la mejora de la alfabetización en seguridad cibernética para eliminar la causa número uno de las infracciones de seguridad cibernética: el error humano.

¡Recuerda siempre, sé un Superagente de Ciberseguridad!

Co-funded by the
Erasmus+ Programme
of the European Union

Las respuestas correctas están marcadas en negrita

Situación: ¿Qué es el "Internet de las cosas"?
Tarea: Por favor, identifica la opción correcta siguiendo el principio de elección única: solo una respuesta es verdadera.

- IoT es una red de servidores conectados a los que se accede a través de Internet.
- IoT es la digitalización y automatización de cada parte de la empresa, así como el proceso de fabricación.
- IoT es una red global de área amplia que conecta sistemas informáticos en todo el mundo.
- **IoT es una tecnología incipiente que se centra en la interconexión entre cosas o dispositivos entre sí y con humanos o usuarios para lograr algunos objetivos comunes.**

Situación: ¿Cuáles son las principales aplicaciones de Internet de las cosas?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple. Ninguna, una, más de una o todas las opciones pueden ser verdaderas

- **Monitoreo de línea eléctrica y transmisión de energía de red inteligente.**
- **Gestión de la cadena de suministro de producción al por menor.**
- **Gestión de la cadena de suministro de producción en la industria transformadora.**
- **Regulación del agua en la agricultura.**

Situación: en cuanto a la seguridad de los dispositivos IoT y sus usuarios, ¿qué afirmaciones son ciertas?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple. Ninguna, una, más de una o todas las opciones pueden ser verdaderas

- **La seguridad de los datos se requiere cuando los datos se generan y almacenan.**
- Los requisitos de seguridad para las aplicaciones de IoT deben aplicarse en tres capas: capa de aplicación, capa de red y capa de percepción.
- La probabilidad de que ocurra un ataque de phishing en un dispositivo IoT es mayor en su capa de procesamiento.
- **La arquitectura de IoT permite a las entidades maliciosas explotar vulnerabilidades intrínsecas a cada una de las capas de IoT.**
- **Un código malicioso puede afectar al menos a tres capas.**

Situación: en consideración de la privacidad del usuario de IoT, ¿qué afirmación es verdadera?
Tarea: Por favor, identifica la opción correcta siguiendo el principio de elección única: solo una respuesta es verdadera.

- El crecimiento significativo que ha demostrado el IoT durante los últimos años ha generado varias preocupaciones de privacidad a medida que disminuye la disponibilidad de datos, patrocinado por las propiedades comunes y habituales del IoT.
- **Los artículos necesitan garantizar la protección de la información personal de los usuarios asociada a sus movimientos, hábitos e interacciones.**
- La privacidad se refiere a cómo de bien los dispositivos IoT se defienden contra el robo de datos del usuario.
- La privacidad solo está en riesgo en la capa de aplicación.

Situación: ¿Qué medidas de seguridad debes implementar para evitar ataques cibernéticos en tus dispositivos IoT?

Co-funded by the
Erasmus+ Programme
of the European Union

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple. Ninguna, una, más de una o todas las opciones pueden ser verdaderas

- a) Instalar cifrado homomórfico.
- b) Instalar cortafuegos.
- c) Crear dispersión de redundancia de fragmentación.
- **d) Cambiar las contraseñas predeterminadas del enrutador.**
- **e) Desactivar funciones en mi dispositivo inteligente que no se están utilizando.**
- **f) Desactivar el acceso remoto al dispositivo inteligente.**

Situación: para convertirse en un súper agente de ciberseguridad, ¿qué debes hacer?
Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple. Ninguna, una, más de una o todas las opciones pueden ser verdaderas

- Aprender a programar para cifrar dispositivos IoT.
- Establecer un plan contingente siguiendo las 4 preguntas: "¿Qué se está generando?", "¿Dónde se almacenan los datos?", "¿Cuándo se usan los datos?" Y "¿Con quién se comparten los datos?"
- **Establece un plan contingente siguiendo las 4 preguntas: "¿A quién llamar?" "¿Cuál es mi curso de acción?", "¿Cuándo alertar a otros?" Y "¿Qué actividades son incidentes?"**
- **Involucrar a toda mi familia, compañeros y empleados en la conciencia de seguridad cibernética.**
- Desarrollar el plan de respuesta a la incidencia solo después de sufrir una brecha de seguridad, ya que es la única forma de conocer las acciones correctas para los incidentes que están por venir.