Grupo Clouds

Tecnologías de la Información y Comunicación 2°

Prof. Fernando Pachioli

Equipo de trabajo

- ★ Eduardo Moreno *- Comisión D*
- ★ Leandro Paryszewski *- Comisión D*
- ★ Marcelo Moreno *- Comisión D*
- ★ Melissa Galeano Ibañez *- Comisión D*
- ★ Javier Lopez *- Comisión F*

PFO TIC

Tema: Infraestructura de Redes para IoT: Desafíos y Soluciones

Objetivo:
Que los estudiantes investiguen y analicen cómo las redes y protocolos de comunicación permiten el funcionamiento de dispositivos IoT, considerando problemas reales y planteando soluciones.

Actividades

1. Investigación de base

- Explicar qué es IoT y su impacto en las redes de comunicación.
- Describir los protocolos más utilizados en IoT.

2. Análisis de caso real

- Elegir un sector donde IoT se use ampliamente (salud, industria, hogar inteligente, transporte, etc.).
- Investigar cómo se implementan las redes de comunicación en ese contexto.

3. Problema técnico a resolver

- Presentar un problema realista en la comunicación de dispositivos IoT, por ejemplo:
    - Latencia en redes de sensores de salud.
    - Seguridad en dispositivos IoT del hogar.
    - Escalabilidad en redes IoT industriales.
- Proponer una solución fundamentada con argumentos técnicos.

4. Reflexión y discusión

- ¿Qué ventajas y desventajas tiene IoT en redes y comunicaciones?
- ¿Cómo creen que evolucionará en el futuro?

1.1. ¿Qué es el Internet de las Cosas (IoT)?

El **Internet de las Cosas (IoT)** es básicamente la idea de conectar objetos físicos a Internet para que puedan **recoger, enviar y procesar datos en tiempo real**. No se trata solo de computadoras o celulares, hablamos de electrodomésticos inteligentes, autos autónomos, sensores en fábricas, sistemas de riego en el campo o incluso chips que monitorean la salud de animales.

Gracias a que hoy los sensores son más baratos, la conectividad es más amplia y existe una demanda creciente de soluciones inteligentes, el IoT dejó de ser una “tecnología del futuro” y pasó a ser parte del presente. De hecho, se estima que en 2030 habrá más de 75 mil millones de dispositivos conectados en todo el mundo.

El objetivo del IoT es crear un entorno tecnológico **más eficiente e integrado**, capaz de automatizar tareas que antes requerían intervención humana y de generar información valiosa para la toma de decisiones. Eso sí, junto con sus beneficios también aparecen desafíos importantes, especialmente en **seguridad, privacidad y uso ético de los datos**.

1.2. Impacto del IoT en las redes de comunicación

El crecimiento del IoT obliga a las redes de comunicación a evolucionar para poder soportar la enorme cantidad de dispositivos y datos. Algunos puntos clave:

- **5G:** La quinta generación de redes móviles ofrece mayor velocidad, menor latencia y capacidad para conectar millones de dispositivos al mismo tiempo. Esto habilita aplicaciones complejas como los autos autónomos, las ciudades inteligentes o la agricultura de precisión.

- **Edge Computing:** En lugar de enviar todos los datos a la nube, se procesan lo más cerca posible de donde se generan. Así se reducen los tiempos de respuesta, algo vital en situaciones donde cada milisegundo cuenta (ejemplo: un auto autónomo que debe frenar de golpe).

- **Infraestructura digital:** Las redes modernas funcionan como una especie de “piel digital” que conecta todo, permitiendo comunicación, análisis y ajustes automáticos a gran escala.

- **Conectividad y escalabilidad:** Existen distintas tecnologías de red (4G/5G, LoRaWAN, NB-IoT, entre otras) que se usan según el caso. El gran desafío está en que los sistemas puedan escalar y manejar millones de dispositivos sin colapsar.

- **Interoperabilidad y estandarización:** Uno de los problemas del IoT es que muchos dispositivos de distintos fabricantes “no hablan el mismo idioma”. Por eso se trabaja cada vez más en **protocolos y estándares comunes** que permitan integrarlos de forma más sencilla y económica.

En resumen, el IoT no solo aprovecha los avances de las telecomunicaciones, sino que también los impulsa hacia **más velocidad, menos latencia, mayor capacidad y redes más flexibles y seguras**.

1.3. Protocolos más utilizados en IoT

Para que todos estos dispositivos se comuniquen entre sí, se utilizan diferentes protocolos, cada uno con sus ventajas y limitaciones. Algunos de los más comunes son:

- **MQTT:** Ligero y rápido, ideal para enviar datos en tiempo real desde sensores industriales o sistemas con poco ancho de banda.
- **HTTP/HTTPS:** El mismo protocolo que usamos para navegar en Internet, fácil de implementar y seguro (si es HTTPS). Se usa en dispositivos más potentes.
- **CoAP:** Diseñado para dispositivos muy limitados en recursos (poca energía y bajo procesamiento).
- **LoRaWAN:** Permite comunicar sensores a grandes distancias consumiendo muy poca energía. Se usa mucho en monitoreo ambiental y agricultura.
- **Bluetooth Low Energy (BLE):** Popular en pulseras y relojes inteligentes, funciona bien para distancias cortas y bajo consumo.
- **Wi-Fi:** Ofrece gran velocidad, aunque consume bastante energía. Ideal en entornos cerrados como casas o almacenes.
- **Zigbee y Z-Wave:** Muy usados en domótica (casas inteligentes), permiten conectar varios dispositivos de bajo consumo entre sí.
- **Redes celulares (4G/5G, Cat-M, NB-IoT):** Útiles cuando se necesita cobertura amplia y movilidad, como en gestión de flotas o videovigilancia.

La **seguridad** es un punto crítico en cualquiera de estos protocolos. Por eso suelen incluir medidas como **cifrado de extremo a extremo, autenticación y segmentación de redes**. En la práctica, muchos proyectos combinan varios protocolos para lograr un equilibrio entre alcance, velocidad, consumo de energía y seguridad.

2. Análisis de Caso Real: Implementación de un Sistema Domótico IoT para Gestión Eficiente de Climatización y Seguridad en un Hogar Familiar

2.1. Introducción

La domótica, impulsada por el Internet de las Cosas (IoT), ha dejado de ser una visión futurista para convertirse en una realidad accesible. Permite la automatización y control remoto de diversos aspectos del hogar, mejorando la eficiencia energética, la seguridad y la comodidad. Este análisis examina la implementación de un sistema integral en una vivienda familiar para gestionar automáticamente la climatización y la seguridad.

2.2. Descripción del Caso y Problema a Resolver

- **Usuarios**: Una familia de 4 personas con horarios laborales y escolares variables. La casa permanece vacía la mayor parte del día.
- **Problemas**:
    - Ineficiencia Energética: Calefaccionar o refrigerar una casa vacía representa un gasto económico y energético significativo e innecesario.
    - Falta de Confort al Ingresar: Llegar a una casa con temperaturas extremas (muy fría en invierno o muy calurosa en verano) es incómodo.
    - Seguridad Básica: La falta de presencia física durante el día puede hacerla un objetivo potencial.

2.3. Solución IoT Propuesta

Se implementa un sistema domótico centralizado que automatiza la climatización basándose en presencia y horarios, y monitorea la seguridad.

- **Ajuste Automático de Climatización**:
    - Se instalan sensores de temperatura y humedad inalámbricos (ej. con protocolo Zigbee o Z-Wave) en las habitaciones principales y el living.
    - Un termostato inteligente o un controlador universal para el aire acondicionado (como los que mencionas, que simulan ser el control remoto) actúa como actuador.
    - Una plataforma central (un asistente como Alexa/Google Home, una Raspberry Pi o un PLC) recibe los datos de los sensores y ejecuta la lógica programada.
    - Lógica Implementada: El sistema se activa automáticamente a las 16:30 para acondicionar la casa a 20°C, asegurando confort para la llegada de la familia. Se apaga a las 07:30 AM cuando la casa se vacía. La ventaja clave sobre un simple timer es la retroalimentación: los sensores verifican que la temperatura meta se alcanzó y se mantiene, ajustando el equipo según sea necesario.

- **Seguridad y Accesos:**
    - Sensores de contacto magnético en puertas y ventanas alertan si se abren fuera del horario habitual.
    - Una cámara IP en la entrada principal envía notificaciones con detección de movimiento.
    - Cerraduras inteligentes permiten bloquear las puertas de forma remota y crear claves temporales para visitas.
- **Riego del Jardín:**
    - Un controlador de riego inteligente conectado a Wi-Fi se programa para regar de noche (reduciendo evaporación) y puede suspenderse automáticamente si un sensor de humedad del suelo detecta que ya está húmedo o si un sensor meteorológico pronostica lluvia.

2.4. Arquitectura Tecnológica IoT Implicada

Capa	Componente	Ejemplos en el Caso
Sensores	Dispositivos que capturan datos del entorno.	Sensores de temperatura/humedad, sensores de contacto (puertas/ventanas), sensor de movimiento de la cámara, sensor de humedad del suelo.
Conectividad	Protocolos de comunicación.	Wi-Fi (para la cámara, el controlador central), Zigbee/Z-Wave (para sensores, bajo consumo), Bluetooth (para configuración inicial).
Procesamiento (Fog/Edge)	Donde se ejecuta la lógica y se toman decisiones automáticas.	Opción 1 (Usuario): Raspberry Pi con software como Home Assistant. Opción 2 (Fabricante): La nube del asistente (Alexa) o la app del dispositivo. Opción 3 (Avanzada): PLC programado en ladder o C.
Actuadores	Dispositivos que realizan una acción física.	Controlador del aire acondicionado, válvula solenoide del sistema de riego, motor de la cerradura inteligente.

Interfaz de Usuario	Cómo el usuario interactúa con el sistema.	App móvil (para control remoto y alertas), asistente de voz (para control por voz local), panel web (desde una PC).

2.5. Análisis de la Implementación

Ventajas y Beneficios:

- **Ahorro Energético y Económico:** Es la ventaja principal. Al evitar climatizar una casa vacía, el ahorro en la factura de electricidad/gas puede ser superior al 20%, amortizando la inversión en el mediano plazo.
- **Confort y Conveniencia:** La familia llega siempre a un ambiente confortable sin tener que pensar en ello.
- **Seguridad Mejorada:** Monitoreo remoto 24/7 y alertas inmediatas ante eventos inusuales.
- **Personalización y Escalabilidad:** El sistema basado en Raspberry Pi o PLC permite una personalización casi infinita y agregar nuevos dispositivos en el futuro.

Desafíos y Limitaciones (Expandidos):

- **Seguridad Cibernética:** Este es el punto más crítico. Los dispositivos IoT económicos son famosos por sus vulnerabilidades. Una brecha de seguridad podría permitir a un atacante desactivar la alarma o monitorizar la casa. Mitigación: Usar contraseñas fuertes, segmentar la red (crear una red Wi-Fi exclusiva para IoT), mantener el firmware actualizado y preferir dispositivos de marcas reconocidas.
- **Complejidad Técnica y Confiabilidad:** La solución "Hazlo Tú Mismo" (DIY) con Raspberry Pi requiere tiempo, conocimientos técnicos y mantenimiento. Si la Raspberry Pi se apaga o se corrompe su memoria, toda la automatización falla.
- **Interoperabilidad:** No todos los dispositivos de diferentes marcas trabajan bien juntos. Elegir un ecosistema (Google, Amazon, Apple) o un estándar (Zigbee, Z-Wave) es crucial.
- **Costo Inicial**: La inversión inicial en hardware (sensores, actuadores, control central) puede ser significativa, aunque se compensa con el ahorro posterior.

2.6. Conclusión y Tendencias Futuras

La implementación de este sistema domótico IoT resuelve de manera efectiva los problemas de eficiencia y confort planteados por la familia. Demuestra cómo la tecnología puede optimizar recursos y simplificar tareas cotidianas.

El futuro de este sistema es la predictividad y la integración con IA:

- **Predictivo:** En lugar de un horario fijo, el sistema podría usar la geolocalización de los smartphones familiares para predecir la hora de llegada y encender la climatización de forma perfectamente sincronizada.

- **Proactivo:** El sistema podría aprender de los patrones de ajuste manual de los usuarios para auto-optimizar las temperaturas y horarios.
- **Integración Total:** Los sistemas de climatización, seguridad y riego dejarán de ser "islas" para actuar de forma coordinada. Ej: Si la alarma se desactiva (señal de que alguien llegó), el sistema de riego se pausa automáticamente para no mojar a la persona durante su circulación.

Este caso evidencia que la domótica real ya está aquí, es accesible y ofrece un valor tangible, aunque debe implementarse con una cuidadosa consideración de la seguridad y la confiabilidad.

🏠 3. Problema técnico: Seguridad en dispositivos IoT del hogar

En un hogar inteligente, múltiples dispositivos IoT (cerraduras electrónicas, cámaras IP, asistentes de voz, sensores de movimiento, termostatos) se comunican a través de la red Wi-Fi doméstica.
Un problema frecuente es que estos dispositivos suelen tener contraseñas débiles, firmware desactualizado y protocolos de comunicación inseguros, lo que los convierte en puntos vulnerables.
Un atacante que acceda a la red podría:

- Interceptar las comunicaciones entre dispositivos.
- Tomar control de cerraduras inteligentes o cámaras.

Este riesgo crece porque el hogar promedio puede tener entre 15 y 30 dispositivos conectados, aumentando la superficie de ataque.

3.1. Solución propuesta: Implementación de una arquitectura de seguridad para IoT doméstico

- **Cifrado de comunicaciones**
  - Uso de TLS/SSL en protocolos como MQTT y CoAP.
  - Asegurar que todos los datos transmitidos (ej. video de cámaras, comandos de cerraduras) viajen cifrados extremos a extremo.
- **Autenticación robusta y gestión de credenciales**
  - Contraseñas únicas y fuertes por dispositivo.
  - Autenticación de dos factores (2FA) para el acceso remoto al sistema.
  - Uso de certificados digitales en lugar de contraseñas en algunos dispositivos.
- **Segmentación de red**
  - Crear una red Wi-Fi separada para dispositivos IoT y otra para el uso cotidiano (celulares, PC).
  - Esto reduce el riesgo de que un dispositivo comprometido afecte a toda la red.
- **Actualizaciones automáticas y seguras de firmware**
  - Implementar un sistema de Updates que verifique la integridad del software mediante firmas digitales.
  - Mantener los dispositivos siempre con los últimos parches de seguridad.
- **Monitoreo y detección de anomalías**
  - Uso de un hub o gateway inteligente que supervise el tráfico de dispositivos IoT.
  - Aplicación de machine learning ligero para detectar patrones anormales de tráfico (ej. una cámara que comienza a enviar datos constantemente hacia una IP sospechosa).

3.2. Fundamentación técnica

- El cifrado protege contra ataques de interceptación.

- La segmentación de red es un principio de Zero Trust, aislando los riesgos.
- Las actualizaciones OTA seguras mitigan vulnerabilidades conocidas sin intervención manual del usuario.
- El monitoreo con IA permite reaccionar en tiempo real a comportamientos anómalos, algo crítico en entornos con muchos dispositivos conectados.

4.1. ¿Qué ventajas y desventajas tiene el IoT en redes y comunicaciones?

Las ventajas del Internet de las Cosas (IoT) en redes y comunicaciones se centran en la eficiencia y la optimización. Gracias a la capacidad de los dispositivos para conectarse e intercambiar datos, se facilita la automatización y el control remoto de sistemas y recursos, lo que conduce a una mejora significativa en la productividad en muchos sectores. Esta interconexión masiva también permite la recopilación de grandes volúmenes de datos en tiempo real, proporcionando información crucial para tomar decisiones más precisas y fundamentadas. A nivel de usuario, la aplicación de IoT en hogares inteligentes puede reducir costos operativos y mejorar la calidad de vida.

Sin embargo, estos beneficios traen consigo importantes desafíos. Una de las principales desventajas es la seguridad. La gran cantidad de dispositivos conectados crea una vasta superficie de ataque que los hace vulnerables a ciberataques, poniendo en riesgo tanto los datos personales como la integridad de los sistemas. Otro punto crítico es la interoperabilidad; la falta de estándares comunes entre los dispositivos de distintos fabricantes hace que la gestión de la red se vuelva más compleja y limita la escalabilidad de los sistemas. Además, la creciente dependencia de la tecnología para tareas cotidianas podría llevar a una *pérdida de capacidades resolutivas en los humanos*.

4.2. ¿Cómo evolucionará el IoT en el futuro?

El futuro del IoT estará impulsado por la sinergia con tecnologías emergentes como 5G y la Inteligencia Artificial. La red 5G, con su baja latencia y alta capacidad, permitirá aplicaciones críticas-masivas que requieren respuestas en tiempo real, como vehículos autónomos y robótica avanzada. La IA jugará un papel fundamental al permitir que los dispositivos no solo recojan datos, sino que también los analicen y tomen decisiones de forma autónoma, lo que impulsará el edge computing y reducirá la dependencia de la nube[7].

Se espera que la industria avance hacia una mayor estandarización y mejoras en los protocolos de seguridad. Además, la sostenibilidad se convertirá en un foco principal, con el desarrollo de dispositivos de bajo consumo energético que minimicen su impacto ambiental[8]. En última instancia, la evolución del IoT plantea una reflexión continua sobre el equilibrio entre el progreso tecnológico y la protección de nuestra seguridad, privacidad y habilidades humanas.

Para finalizar como equipo nos pareció pertinente plantear una pregunta disparadora que fomente nuestra reflexión:
¿Podrá la inteligencia artificial que gestiona nuestros hogares inteligentes volverse tan sofisticada que desarrolle sus propios "intereses" y prioridades, como optimizar la energía a un nivel que limite nuestras comodidades o controlar nuestros dispositivos para alcanzar un objetivo que no entendemos?

Informe Final: Internet de las Cosas (IoT)

Introducción

El internet de las Cosas (IoT, por sus siglas en inglés) ha dejado de ser una promesa tecnológica del futuro para convertirse en una realidad presente, con aplicaciones en viviendas, industrias, transporte, agricultura y ciudades inteligentes. Se espera que el número de dispositivos conectados en todo el mundo sean alrededor de 25-40 mil millones para fines de la década, lo que demuestra la magnitud de esta transformación digital.

El IoT se refiere a la conexión de dispositivos físicos a internet para que puedan **recopilar, compartir y analizar datos** en tiempo real. Esta conectividad permite generar **eficiencia operativa, automatización de procesos y mejora en la experiencia de usuarios y empresas**. Sin embargo, este crecimiento plantea desafíos importantes en seguridad, privacidad y uso ético de los datos.

Concepto y alcances del IoT

El IoT se basa en la premisa de que cualquier objeto físico puede ser conectado a Internet para convertirse en un emisor y receptor de datos. Esto incluye desde **electrodomésticos inteligentes y sensores industriales** hasta **vehículos autónomos, sistemas de riego, chips biomédicos y dispositivos de monitoreo ambiental**.
La combinación de sensores de bajo costo, conectividad global y una creciente demanda de soluciones inteligentes ha impulsado su implementación masiva. El IoT busca conformar un ecosistema tecnológico capaz de reducir la necesidad de intervención humana en tareas rutinarias, generar información estratégica en tiempo real e integrar procesos en entornos domésticos, empresariales y urbanos. Todos estos beneficios permiten mejorar la experiencia de usuarios y empresas, pero también conlleva desafíos en la **seguridad, privacidad y uso ético de los datos.**

Impacto del IoT en las Redes de Comunicación

El crecimiento exponencial de dispositivos IoT ha forzado a las redes de comunicación a evolucionar en **capacidad, velocidad, confiabilidad y seguridad**.

Redes 5G

La quinta generación móvil es clave para el IoT. Ofrece **mayor velocidad, baja latencia y capacidad para millones de dispositivos conectados**, habilitando aplicaciones críticas como autos autónomos, ciudades inteligentes y agricultura de precisión.

Edge Computing

Consiste en procesar datos cerca de la fuente en lugar de enviarlos a la nube. Esto reduce tiempos de respuesta, algo vital en escenarios donde los milisegundos son decisivos (ejemplo: frenar un vehículo autónomo).

Infraestructura digital y escalabilidad

Las redes modernas funcionan como una “piel digital” que interconecta sistemas a gran escala. Tecnologías como **LoRaWAN, NB-IoT o 5G** permiten adaptarse a distintas necesidades de cobertura, consumo energético y movilidad.

Interoperabilidad y estandarización

La falta de protocolos comunes entre dispositivos de distintos fabricantes dificulta la integración. La estandarización es uno de los mayores desafíos actuales y un factor decisivo para el crecimiento del IoT.

Protocolos más Utilizados en IoT

El IoT depende de protocolos de comunicación que varían según el **alcance, consumo de energía, velocidad y seguridad requerida**:

- **MQTT:** ligero y eficiente, ideal para sensores industriales y entornos con poco ancho de banda.
- **HTTP/HTTPS:** ampliamente usado, especialmente en dispositivos potentes, con seguridad añadida en su versión cifrada.
- **CoAP:** diseñado para dispositivos de bajo consumo y procesamiento limitado.
- **LoRaWAN:** adecuado para largas distancias y bajo consumo, muy útil en agricultura y monitoreo ambiental.
- **BLE (Bluetooth Low Energy):** común en wearables y dispositivos de salud.
- **Wi-Fi:** ofrece alta velocidad, aunque con alto consumo energético, óptimo en entornos domésticos.
- **Zigbee y Z-Wave:** protocolos domóticos populares en hogares inteligentes.
- **Redes celulares (4G/5G, NB-IoT, Cat-M):** útiles para movilidad y cobertura amplia, como en gestión de flotas o videovigilancia.

En todos los casos, la **seguridad en las comunicaciones** es prioritaria: cifrado extremo a extremo, autenticación robusta y segmentación de redes.

Caso Real: Sistema Domótico IoT en un Hogar Familiar

- **Problema:** Una familia de cuatro integrantes enfrenta tres dificultades:
    - Ineficiencia energética: la climatización de una vivienda vacía durante gran parte del día.
    - Incomodidad térmica: llegar a la casa demasiado frío en el invierno o muy caluroso en el verano.
    - Falta de seguridad: riesgo de ingreso de una persona ajena a la casa.

- **Solución:** implementación de un sistema domótico que automatiza la climatización basándose en presencia y horarios, y monitorea la seguridad. Compuesto por:
    - Sensores: temperatura, humedad, movimiento y contacto en puertas/ventanas.
    - Termostato inteligente.
    - Asistente virtual.
    - Cámaras IP.
    - Sensores de contacto magnético.
    - Cerraduras electrónicas.
    - Riego automatizado.

- **Beneficios:**
    - Ahorro de más del 20% en energía.
    - Mayor confort y conveniencia.
    - Seguridad mejorada con monitoreo remoto.
    - Escalabilidad y personalización.

- **Desafíos:**
    - Ciberseguridad: riesgo de hackeo en cámaras o cerraduras inteligentes.
    - Interoperabilidad entre marcas: dificultades al integrar dispositivos de marcas diferentes.
    - Complejidad técnica: sistemas DIY requieren de conocimientos avanzados.
    - Costo inicial: inversión alta inicial en hardware.

- **Tendencias:** integración con IA para sistemas predictivos, proactivos y totalmente coordinados.

Seguridad en IoT Doméstico

El **IoT doméstico** (hogares inteligentes) abarca dispositivos como asistentes de voz, cámaras de seguridad, cerraduras inteligentes, termostatos, electrodomésticos conectados, luces y sensores. Estos equipos aportan comodidad, eficiencia energética y nuevas formas

de control remoto, pero también generan riesgos de seguridad y privacidad que deben abordarse con seriedad.

Principales riesgos de seguridad

- **Ataques a dispositivos vulnerables**
- **Acceso no autorizado a redes domésticas**
- **Exposición de datos sensibles**
- **Falta de actualizaciones y soporte**
- **Manipulación física o remota**

Solución propuesta: Implementación de una arquitectura de seguridad para IoT doméstico

Buenas prácticas del usuario

- Cambiar contraseñas por defecto y usar autenticación fuerte (MFA).
- Segmentar la red doméstica (ej. crear una red WiFi separada solo para IoT).
- Mantener firmware y software actualizados. Implementación de un sistema de Updates que verifique la integridad del software por medio de firmas digitales.
- Revisar y limitar permisos de acceso (ej. micrófonos y cámaras).
- Monitorear por medio del uso de un hub o gateway inteligente que supervise el tráfico de dispositivos Iot.
- Implementar machine learning para detectar patrones irregulares de tráfico.

Responsabilidad del fabricante

- Incorporar seguridad desde el diseño (security by design).
- Implementar cifrado robusto de datos en tránsito y en reposo (TLS/SSL en protocolos como MQTT y CoAP).
- Garantizar actualizaciones automáticas y soporte a largo plazo.
- Cumplir con estándares y normativas de ciberseguridad.

Rol de normativas y regulaciones

- Se espera que en los próximos 5 años aumente la presión regulatoria para garantizar que los dispositivos cumplan requisitos básicos de seguridad y transparencia.

Conciencia y educación del consumidor

- A medida que los hogares inteligentes se popularizan, los usuarios deben estar más conscientes de que un electrodoméstico conectado no es solo “comodidad”, sino también un potencial vector de ataque.
- La alfabetización digital en seguridad será clave para reducir incidentes.

Estas prácticas reducen riesgos y fortalecen la resistencia de la red doméstica.

Alcance e impacto futuro

- **Mayor superficie de ataque**: para 2030, con decenas de miles de millones de dispositivos IoT activos, los hogares serán un objetivo frecuente para cibercriminales.
- **Amenazas híbridas**: lo digital y lo físico estarán más entrelazados, por lo que un ataque podría tener consecuencias tangibles (desde abrir una cerradura hasta manipular electrodomésticos).
- **Ecosistema regulado y más seguro**: la combinación de presión regulatoria, mejores prácticas de la industria y usuarios más informados debería mejorar la seguridad general, pero siempre será un reto mantener el equilibrio entre conveniencia y protección.

Ventajas y Desventajas del IoT en Redes

Ventajas:

- Mayor eficiencia y automatización.
- Aumento de la optimización de recursos.
- Mejora en la toma de decisiones con datos en tiempo real.
- Reducción de costos y mejora en la calidad de vida.

Desventajas:

- Alta vulnerabilidad a ciberataques.
- Falta de interoperabilidad entre dispositivos.
- Complejidad de gestión en redes con miles de equipos.
- Riesgo de dependencia excesiva de la tecnología.

Futuro del IoT

El IoT evolucionará gracias a:

- **5G + IA:** para sistemas autónomos y críticos en tiempo real.
- **Edge computing:** menor dependencia de la nube.
- **Estandarización y protocolos seguros**.
- **Sostenibilidad:** dispositivos energéticamente eficientes.

El desafío será equilibrar el progreso tecnológico con seguridad, privacidad y habilidades humanas.

Conclusión

El **Internet de las Cosas** es hoy una de las tecnologías más transformadoras del siglo XXI. Su impacto es evidente en hogares, industrias y ciudades, donde aporta eficiencia, seguridad y confort. Sin embargo, su adopción conlleva retos significativos en materia de ciberseguridad, interoperabilidad y dependencia tecnológica.

El análisis del caso real demuestra que el IoT aplicado en un hogar puede ofrecer beneficios concretos en ahorro energético, comodidad y seguridad, pero también expone vulnerabilidades que requieren medidas preventivas sólidas.

Mirando hacia el futuro, el IoT se integrará cada vez más con la Inteligencia Artificial y las redes 5G, alcanzando un nivel de autonomía y eficiencia sin precedentes. No obstante, este avance plantea interrogantes éticas y filosóficas sobre el grado de control que tendrán los sistemas inteligentes en la vida humana.

Fuentes utilizadas:

Fortinet. (s.f.). ¿Qué es IoT? Ventajas del Internet de las Cosas.
https://www.fortinet.com/lat/resources/cyberglossary/iot

CAST. (s.f.). Internet de las Cosas (IoT) y Automatización: Transformando industrias a través de la conectividad inteligente.
https://www.cast4it.com/es/internet-das-coisas-iot-e-automacao-transformando-industrias-atraves-da-conectividade-inteligente

Zscaler. (s.f.). ¿Qué es la seguridad de IoT?
https://www.zscaler.com/es/zpedia/what-iot-security

Nettra. (2023). Desafíos de IoT en 2023.
https://nettra.tech/desafios-de-iot-en-2023

Telefónica Tech. (s.f.). IoT4all: Los desafíos que debe enfrentar la IoT.
https://telefonicatech.com/blog/iot4all-los-desafios-que-debe-enfrentar-la-iot

LatinCloud. (s.f.). ¿Cómo es el futuro desarrollo del Internet de las cosas?
https://latincloud.com/blog/como-es-el-futuro-desarrollo-internet-cosas

Moko smart. IoT en logística: 5 casos de uso que pueden beneficiar a su negocio
https://www.mokosmart.com/es/iot-in-logistics

Ibm. ¿Qué es el Internet de las cosas (IoT)?
https://www.ibm.com/mx-es/think/topics/internet-of-things

Aula virtual. Internet de las cosas
https://aulasvirtuales.bue.edu.ar/mod/book/view.php?id=723111

Minutas

Minuta Reunión Nº 0

Tema: Organización y búsqueda de más integrantes		
Fecha reunión: 25/08/25	**Hora:** 22:00	**Lugar:** Discord

Asistentes

Apellido	Nombre	Asistencia
Moreno	Eduardo	Presente
Moreno	Marcelo	Presente
Paryszewski	Leandro	Presente
Galeano Ibañez	Melissa	Presente

	Temas Tratados
1	Buscar más integrantes para cumplir con el mínimo requerido
2	Definir las herramientas a utilizar para la organización de la materia
3	Anotar grupo en la planilla de grupos de la materia

	Compromisos para el siguiente encuentro
1	Definir los integrantes del grupo
2	Se fijó la próxima reunión para el día 28/10/25

Minuta Reunión Nº 1

Tema: Definición de tareas e incorporacion de nuevo integrante		
Fecha reunión: 28/10/25	**Hora:** 22:00	**Lugar:** Discord

Asistentes

Apellido	Nombre	Asistencia
Moreno	Eduardo	Presente
Moreno	Marcelo	Presente
Paryszewski	Leandro	Presente
Galeano Ibañez	Melissa	Ausente con aviso
Lopez	Javier	Presente

	Temas Tratados
1	Se incorporó Javier al grupo
2	Discusión sobre la estructura del trabajo
3	Se realiza la división de tareas
4	Se realiza una encuesta para decidir el tema a desarrollar

	Compromisos para el siguiente encuentro
1	Cada integrante avanzará con la tarea correspondiente y la ira cargando en el documento compartido
2	Se definirá el tema a desarrollar en base a la encuesta realizada
3	Se fijó la próxima reunión para el día 09/09/25

Minuta Reunión Nº 2

Tema: Seguimiento de las tareas		
Fecha reunión: 09/09/25	**Hora:** 22:00	**Lugar:** Discord

Asistentes

Apellido	Nombre	Asistencia
Moreno	Eduardo	Presente
Moreno	Marcelo	Ausente con aviso
Paryszewski	Leandro	Ausente con aviso
Galeano Ibañez	Melissa	Presente
Lopez	Javier	Presente

	Temas Tratados
1	Se decidió por medio de la encuesta hacer el trabajo sobre el sector Hogar Inteligente
2	Se revisaron las tareas realizadas y se dieron por finalizadas
3	Discusión sobre el seguimiento de las tareas y posibles mejoras de organización

	Compromisos para el siguiente encuentro
1	Cada integrante avanzara con su tarea correspondiente
2	Se fijó la próxima reunión para el día 18/09/25

Minuta Reunión Nº 3

Tema: Seguimiento de las tareas		
Fecha reunión: 18/09/25	**Hora:** 22:00	**Lugar:** Discord

Asistentes

Apellido	Nombre	Asistencia
Moreno	Eduardo	Presente
Moreno	Marcelo	Presente
Paryszewski	Leandro	Presente
Galeano Ibañez	Melissa	Presente
Lopez	Javier	Presente

	Temas Tratados
1	Se revisaron las tareas realizadas
2	Se decidió extender el informe final y completar las minutas faltantes
3	Se decidió dejar las fuentes utilizadas al final del informe

	Compromisos para el siguiente encuentro
1	Extender el informe final y completar las minutas
2	Se espera realizar la entrega del trabajo
3	Se fijó la próxima reunión para el día 22/09/25

Minuta Reunión Nº 4

Tema: Cierre del trabajo		
Fecha reunión: 22/09/25	**Hora:** 22:00	**Lugar:** Discord

Asistentes

Apellido	Nombre	Asistencia
Moreno	Eduardo	Presente
Moreno	Marcelo	Presente
Paryszewski	Leandro	Presente
Galeano Ibañez	Melissa	Presente
Lopez	Javier	Presente

	Temas Tratados
1	Se dieron devoluciones a las modificaciones realizadas
2	Se procede a la entrega del trabajo