Seguridad en IoT

Integrantes:

- Franco Balich
- Otto Gonzalez
- Malena Aguillon
- Bárbara Covarrubias

Introducción

¿Como surgió IoT?
¿ Por qué es importante?

¿Qué tecnologías se usan?
Ventajas y Desventajas

¿Dónde utilizar IoT?
Magnitud del IoT

Ecosistema IoT
IoT, ICS, OT

Amenazas/Riesgos
Ataques a empresas

Estándares Actuales
Lo primero que tenes que analizar de un dispositivo IoT

Buenas Practicas
Conclusión

Por: Barbara Covarrubias

¿Cómo surgió el IoT?

Kevin Ashton

Surgió en 1999

¿Cual es el objetivo de IoT?

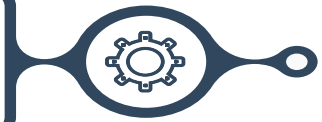
Poder obtener información en tiempo real.

¿Por qué lo llamamos IoT?

¿Cual es el mayor cambio que IoT va a significar en el mundo?

¿Por qué es importante?

Una de las tecnologías más usadas



Seguridad entre dispositivos conectados

Comunicación entre personas, procesos y cosas

Por: Malena Aguillon


Importancia dentro de una empresa
1 Información
2 Productividad
3 Eficiencia
4 Prevención de fallas
5 Mejor visibilidad

En qué ámbitos se usa

Hogares inteligentes

Salud

Agricultura

Seguridad en organizaciones

Industrias

Educación

¿Qué tecnologías se usan en el IoT?

01
Tecnología de miniaturización

02
Tecnología de etiquetado

03
Tecnología de sensores

04
Tecnología de la comunicación

05
Tecnología inteligente

Ventajas

Intercambio de información rápida

Ahorro de energia

Comunicación con el entorno directo

Capacidad de conectarse a la red

Magnitud del IoT

En la actualidad

Existen más de 221.7 millones de casas con múltiples dispositivos IoT.

Por: Franco Balich

Ecosistema IoT

Beneficios de un ecosistema IoT

Proporciona oportunidades para nuevas fuentes de ingreso

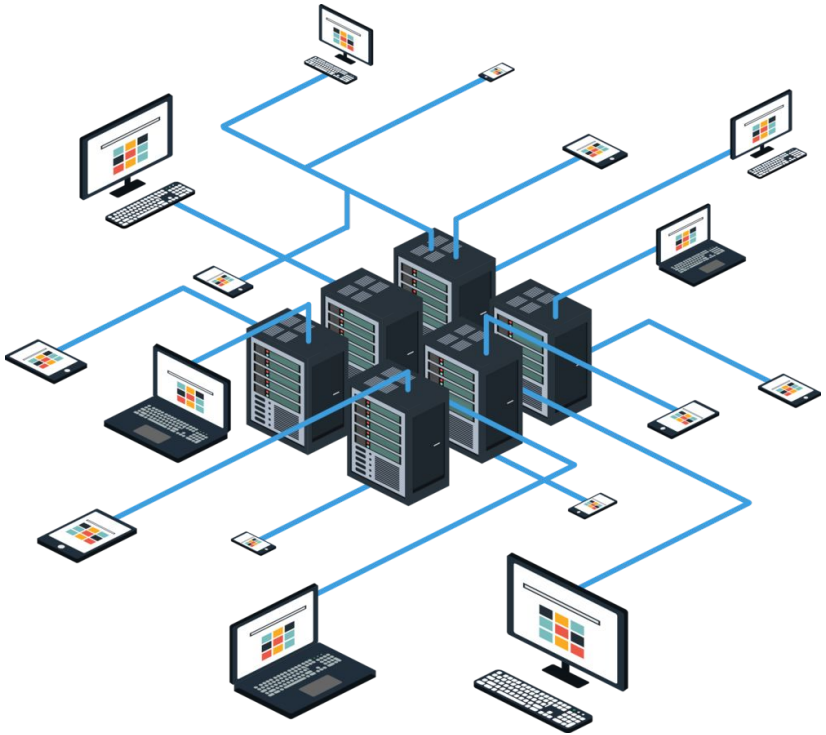
Mejora la experiencia del cliente

Genera nuevos modelos de negocio

Mejora de los conocimientos empresariales

Impulsa la eficiencia

IoT
(Internet of Things)



El Internet de las cosas describe la red de objetos físicos que llevan incorporados sensores, software y otras tecnologías con el fin de conectarse e intercambiar datos con otros dispositivos y sistemas a través de Internet.

Pero en esta categoría de ecosistemas de IoT haremos referencia a los dispositivos domésticos.

ICS

¿Qué son los ICS?

Se encuentran en todas partes, desde máquinas automatizadas que fabrican bienes hasta el sistema de refrigeración de un edificio de oficinas.

Por: Otto Gonzalez

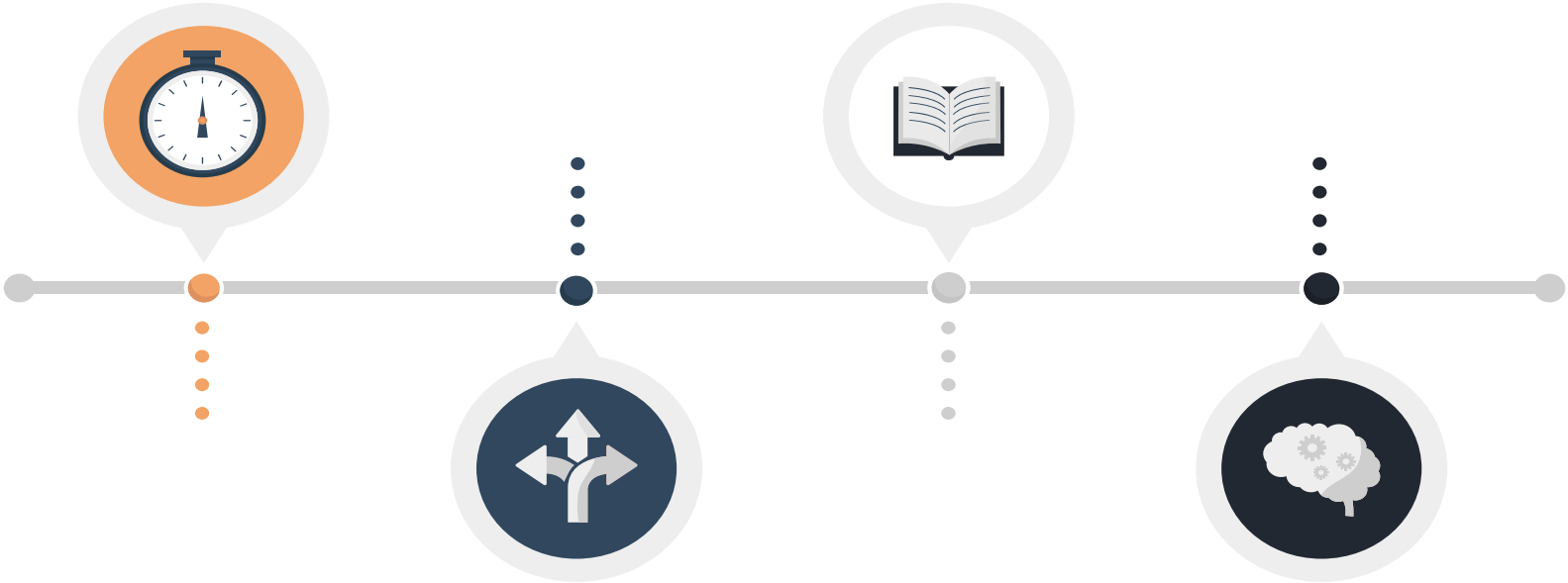
¿Por qué los atacantes eligen atacar ICS?

Motivos financieros, causas políticas u objetivos militares.

- 2005: 13 plantas de fabricación de automóviles de DaimlerChrystler en EE. UU. se desconectaron durante casi una hora. La causa principal fueron las infecciones del gusano Zotob PnP que explotaban un servicio Windows Plug and Play.

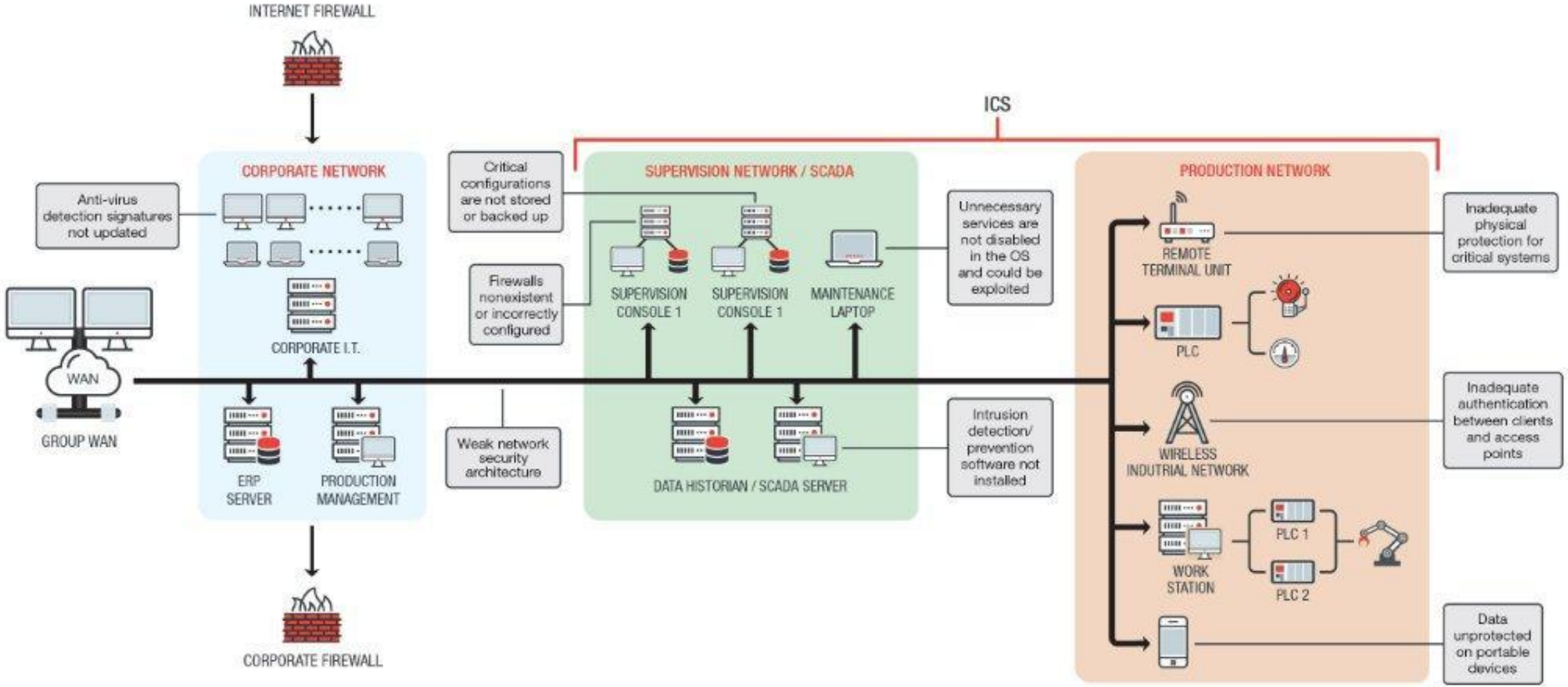
¿Cómo son atacados los ICS?

Reconocimiento -> Tácticas (ataque dirigido) -> Identificación de Vulnerabilidades -> Explotación de vulnerabilidades.

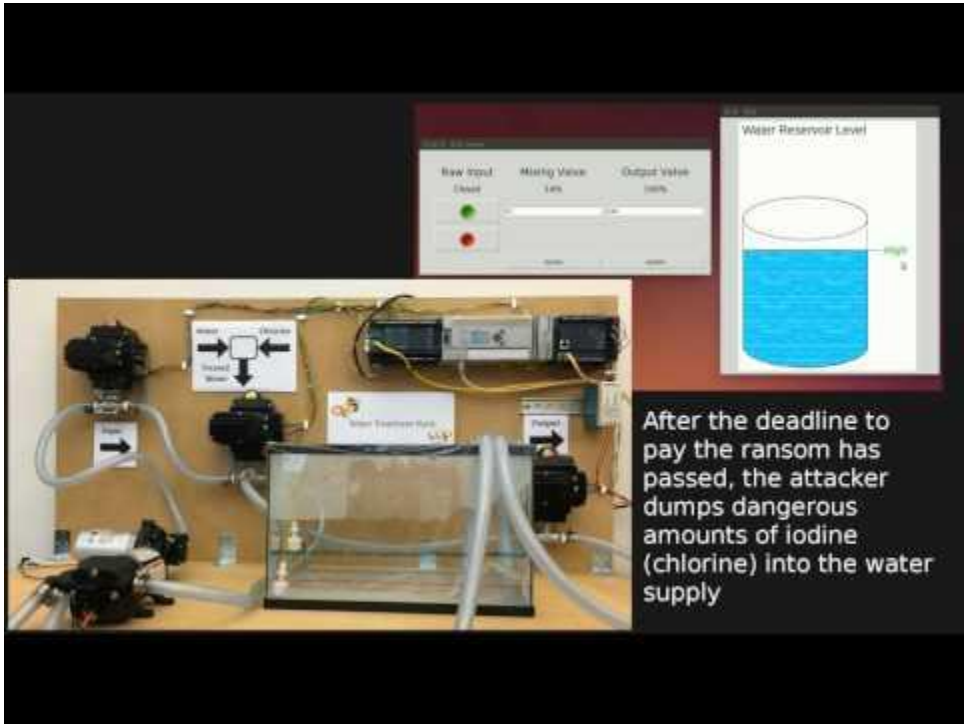


¿Qué vulnerabilidades se explotan en ICS?

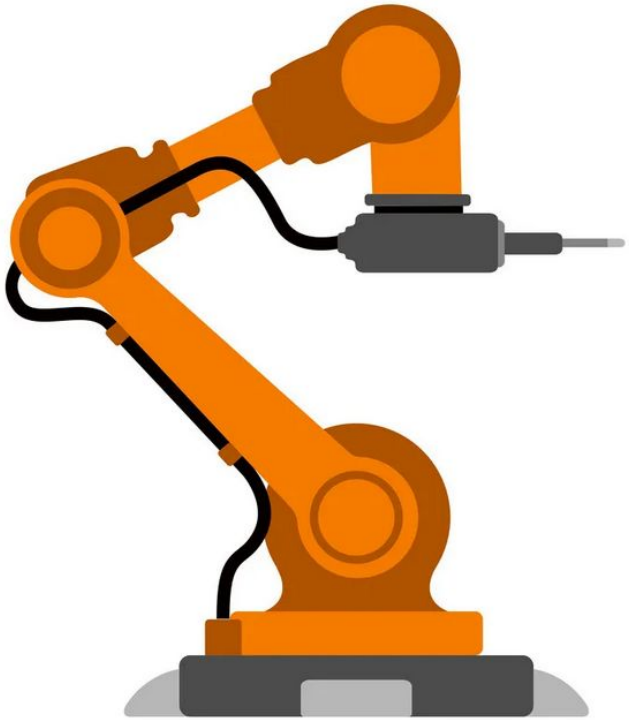
1. *Políticas y Procedimientos*
2. *Configuración de Plataforma.*
3. *Vulnerabilidades del Software de la plataforma.*
4. *Vulnerabilidades de Protección de Malware.*
5. *Vulnerabilidades en Configuración de redes.*
6. *Vulnerabilidades en el hardware de red.*
7. *Vulnerabilidades en el perímetro de la red.*
8. *Vulnerabilidades de Comunicación*
9. *Vulnerabilidades de conexión inalámbrica.*
10. *Vulnerabilidades en el monitoreo y registros de red.*


INTERNET FIREWALL
ICS
CORPORATE NETWORK
Anti-virus detection signatures not updated
CORPORATE I.T.
WAN
GROUP WAN
ERP SERVER
PRODUCTION MANAGEMENT
CORPORATE FIREWALL
Critical configurations are not stored or backed up
Firewalls nonexistent or incorrectly configured
Weak network security architecture
SUPERVISION NETWORK / SCADA
SUPERVISION CONSOLE 1
SUPERVISION CONSOLE 1
MAINTENANCE LAPTOP
DATA HISTORIAN / SCADA SERVER
Unnecessary services are not disabled in the OS and could be exploited
Intrusion detection/ prevention software not installed
PRODUCTION NETWORK
REMOTE TERMINAL UNIT
PLC
WIRELESS INDUTRIAL NETWORK
WORK STATION
PLC 1
PLC 2
Inadequate physical protection for critical systems
Inadequate authentication between clients and access points
Data unprotected on portable devices

Impacto Potencial



OT (Operational Technology)



¿Que es?

¿Seguridad en OT?

Componentes y dispositivos

TI vs TO

Mejores prácticas para seguridad en OT

1. Identificar, clasificar.

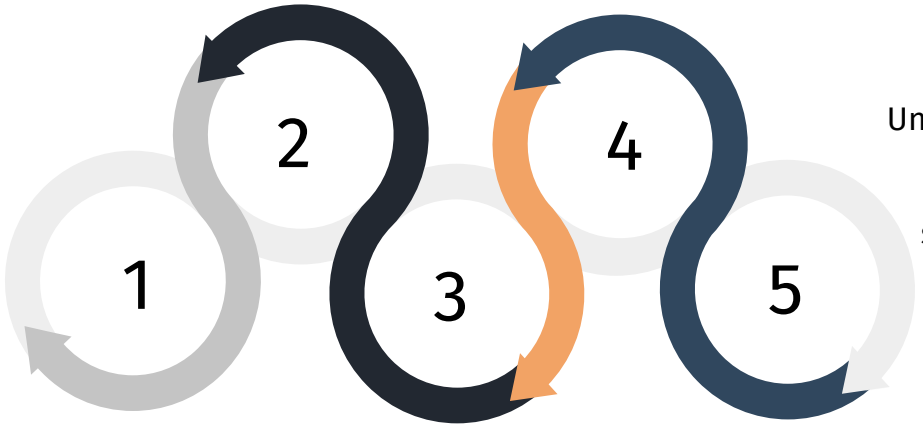
2. Segmentar la Red

3. Analizar Tráfico.

4. Control de Identidad y acceso.

5. Asegurar Accesos.

Amenazas/Riesgos Comunes



Problemas en la implementación

Uno de los principales fallos que se cometen a hora de implementar soluciones IoT es porque no se segmenta adecuadamente la red.

Acceso a la plataforma administrativa del dispositivo

No cuentan con elementos para interactuar entre sí.

Acceso físico al dispositivo

Si un ciberdelincuente consigue un acceso físico podría robarlo o destruirlo

Vulnerabilidades

- Mala gestión de dispositivos de producción
- Servicios de red innecesarios
- Uso de configuraciones por defecto
- Mal uso de contraseñas
- Herramientas externas con configuraciones no verificables.
- Mala gestión de la información personal.
- Falta de controles sobre el acceso al dispositivo Físico

Por: Barbara Covarrubias

Amenazas en IoT

Fragmentación y seguridad

Robo masivo de datos sensibles

Ataques de manipulación de dispositivos que puedan tener un impacto ciberfisico

Variedad de tipos de conectividad

Ataques de denegación de servicio distribuidos contra servicios de terceros en internet.

Contraseñas débiles, adivinables o no modificables.

Ataques a empresas.

2016- Ataque de la botnet Mirai

2018- malware VPNFilter

2020- Pirateo del tesla ModelX

2021: Pirateo de las cámaras de Verkada

Chrysler

Estándares Actuales

- ISO/IEC 30141
- ISO/IEC 27400 & 274002
- ISO/IEC 30149
- IEEE P1912
- IEEE P2413
- ISO/IEC 30161-1 & 301615
- ISO/IEC 30149
- ISO/IEC 21823
- IEEE 1451-99

Por: Otto Gonzalez

Que buscar en dispositivos IoT

Buscadores

Shodan o Cencys

Configuraciones Inseguras

Protocolos no cifrados

Http, etc.

API's Publicas

Mars is actually a cold place

Metadatos

Ingeniería Inversa

JADX

GET http://192.168.1.113:8008/setup/eureka_info


```
{
  "bssid": "00:23:cd:c5:[redacted]",
  "build_version": "124602",
  "cast_build_revision": "1.32.124602",
  "closed_caption": {},
  "connected": true,
  "ethernet_connected": false,
  "has_update": false,
  "hotspot_bssid": "FA:8F:CA:6D:[redacted]",
  "ip_address": "192.168.1.113",
  "locale": "es",
  "location": {
    "country_code": "AR",
    "latitude": 255,
    "longitude": 255
  },
  "mac_address": "38:8B:59:23:[redacted]",
  "name": "Google Mini",
  "noise_level": -92,
  "opt_in": {
    "crash": true,
    "opencast": false,
    "stats": true
  },
  "public_key":
    "[redacted]
    /uwAp1sgjnEsf9irBWJHDNy6RlNJFQPpvDRqcEPxqWFB1Qn3pf
    /3Prhed/JM9V+967lkqvMH3mwWAbw
    /5wxODuuqCOfQQ4Qi4AyxisFoycsY1oTXZ4ZrNOIOBPxZH
    +x0yoJVxd4dPpXmeZe2gAefzEtCQ3wIfDUrZqMgZnCvkJOdGPnBk
    +WmzwMgZ8b82O
    [redacted]
    POrTZnZF1T6ho94UuPynB5TSqyw
    +QCbNKv3QbDfOwEuz2nKZf4qOI5jJFOJR7UQIDAQAB",
  "release_track": "stable-channel",
  "setup_state": 60,
  "setup_stats": {[redacted]},
  "signal_level": -1,
  "ssdp_udn": "0f080ed9-f9d6-072d-ae8b-2f41562384d6",
  "ssid": "Fibertel WiFi 666 2.4GHz",
  "time_format": 2,
  "timezone": "America/Argentina/Buenos_Aires",
  "tos_accepted": true,
  "uma_client_id": "192267a8-6d40-4fe7-b5a4-1b55cd9b7912",
  "uptime": 1564.75,
  "version": 9,
  "wpa_configured": true,
  "wpa_id": 0,
  "wpa_state": 10
```

Buenas prácticas de seguridad en IoT

Mantener el dispositivo y el software actualizados

Cambiar el nombre del router

Cambiar las contraseñas por defecto en los dispositivos IoT

Utilizar un método de cifrado de Wi-Fi seguro

Utilizar contraseñas seguras en todos los dispositivos.

Buenas prácticas de seguridad en IoT

Configurar una red de invitados

Controlar los ajustes de privacidad de sus dispositivos IoT

Activar la autenticación de varios factores

Conocer qué dispositivos IoT hay en su red doméstica

Realice un seguimiento de las funciones disponibles del dispositivo

Conclusiones

Por lo visto en toda la presentación podemos concluir que si bien **el IoT** tiene un **altísimo potencial** para facilitarnos la vida,pero **la creación de tanta información sobre nosotros** puede resultar **ser un peligro** para nuestra privacidad debido a que si no se realizan buenas prácticas y se establecen formas correctas de almacenar la información recolectada, esta puede ser **vulnerada fácilmente**.

Ahora continuamos con las preguntas

Preguntas

1. ¿Cómo surgió el IoT?
2. ¿Qué tecnologías se usan en IoT?
3. ¿Qué beneficios se pueden obtener al implementar sistemas IoT?
4. ¿Qué es un ecosistema IoT?
5. De ejemplos de buenas prácticas de seguridad en IoT

Preguntas

6. ¿Cuáles son los principales problemas para los consumidores?
7. Nombrar un ataque de empresa en IoT
8. ¿Cómo se pueden proteger los dispositivos IoT?
9. ¿Cómo se agrupan los estándares de IoT?
10. ¿Cuál es la diferencia entre TI y TO?

¿Dudas?