AUDITORIA DE SEGURIDAD IoT

CONCLUSION
OWASP TOP 10
AUDITORIA
MITIGACIONES
ATAQUES
VULN'S
ARQUITECTURA
ESCENARIOS
QUE ES?
AGENDA

- **ARNOLDO JOSE LUIS BENITEZ**
  - *Analista de Sistemas*
  - *Especialista en Seguridad Informática*

Seguridad Informática

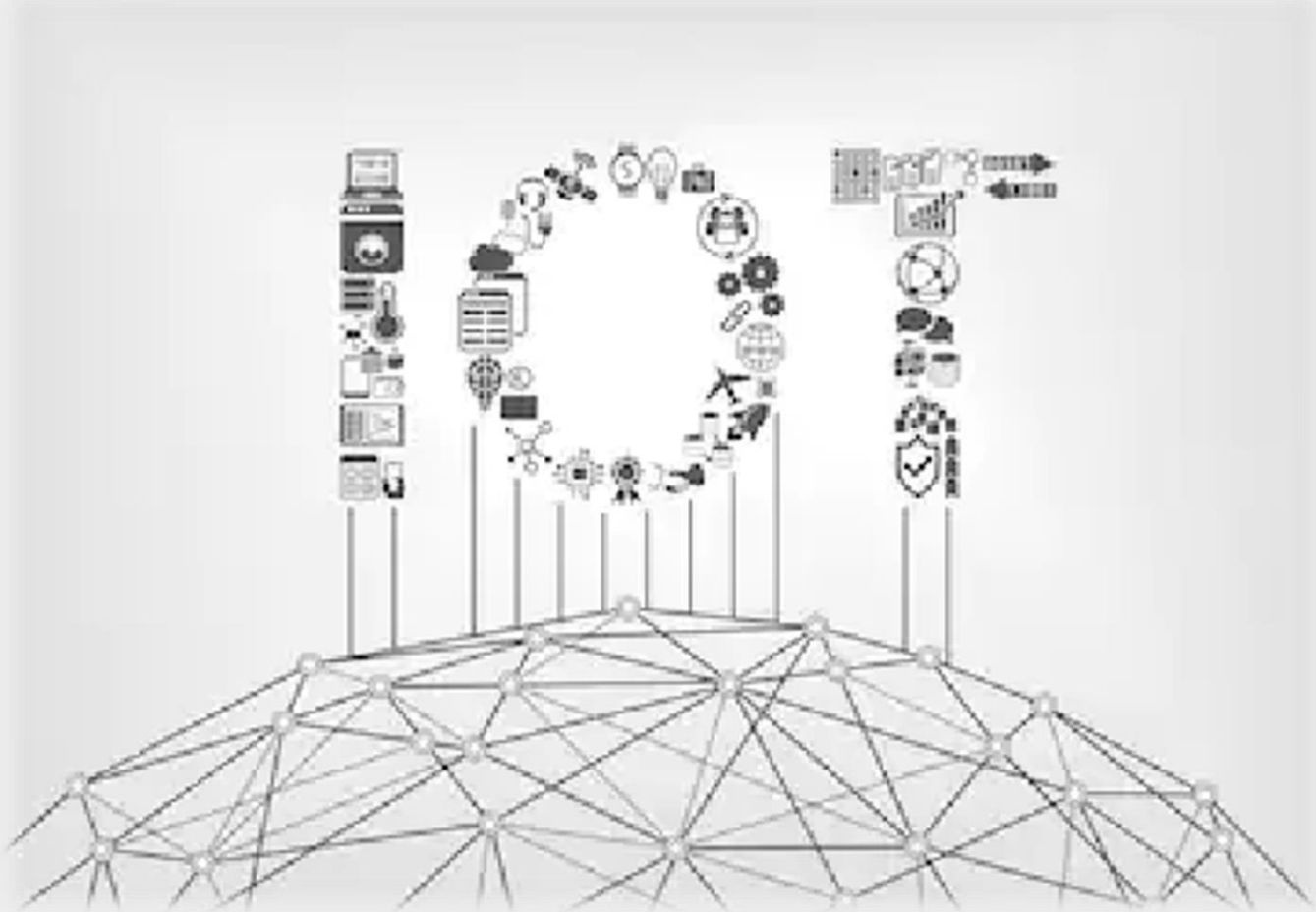
Poder Judicial de Santiago del Estero

CONCLUSION
OWASP TOP 10
AUDITORIA
MITIGACIONES
ATAQUES
VULN'S
ARQUITECTURA
ESCENARIOS
QUE ES?

AGENDA

- **Introducción IoT**
  - ✓ Dispositivos
  - ✓ Escenarios / Arquitecturas
  - ✓ Vulnerabilidades
  - ✓ Ataques
  - ✓ Mitigación
- **Auditoría**
  - ✓ Auditoria de IoT OWASP
  - ✓ OWASP Top 10 2018
  - ✓ Ejemplo.
- **Conclusión**
- **Preguntas**

CONCLUSION
OWASP TOP 10
AUDITORIA
MITIGACIONES
ATAQUES
VULN'S
ARQUITECTURA
ESCENARIOS
QUE ES?
INTRODUCCION



…poco nos han contado de sus puntos débiles…

CONCLUSION
OWASP TOP 10
AUDITORIA
MITIGACIONES
ATAQUES
VULN'S
ARQUITECTURA
ESCENARIOS

QUE ES?
AGENDA
ID

Variedad de dispositivos

Todas las personas

En todo momento

En cualquier lugar

En cualquier contexto

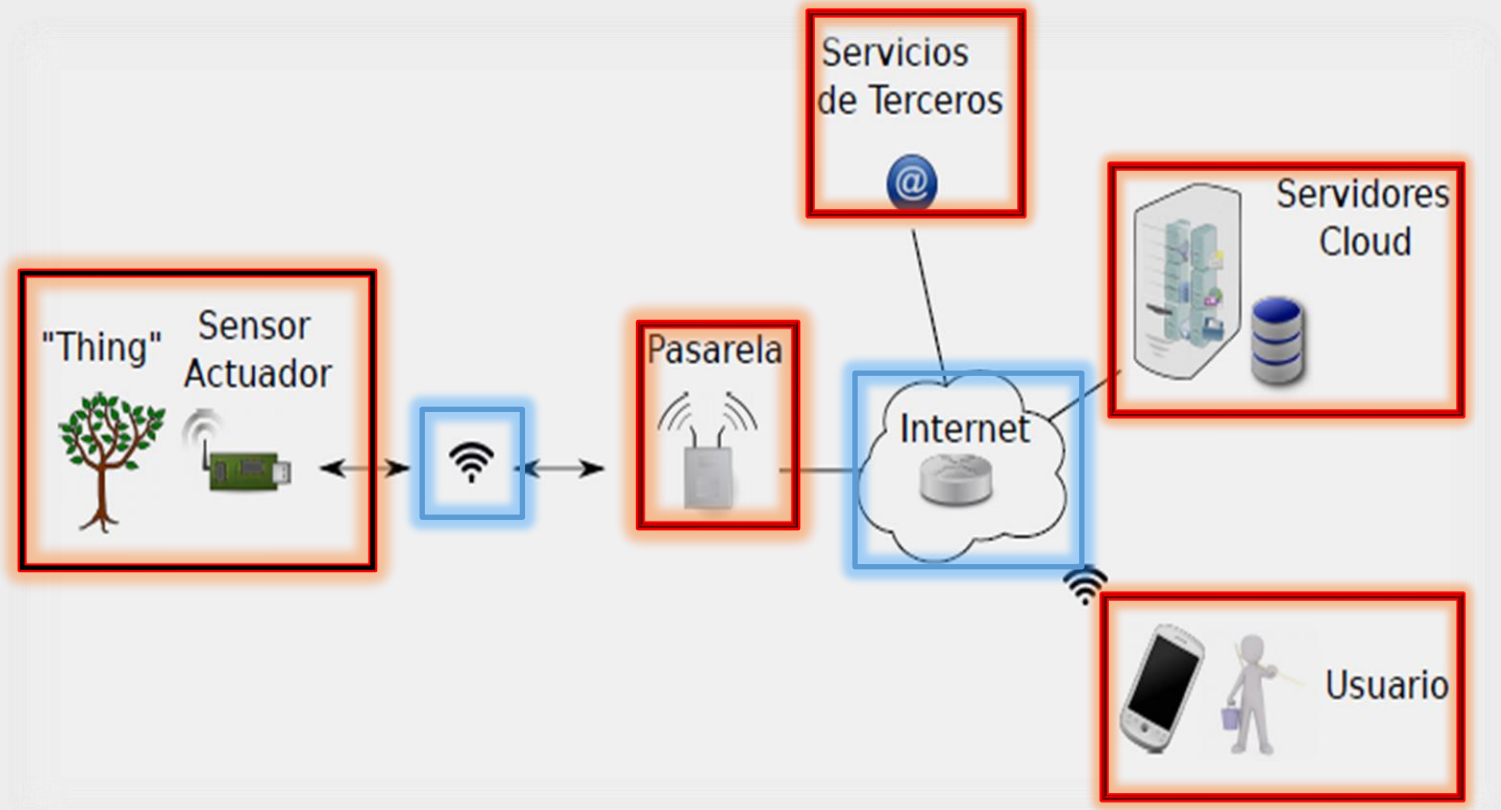
Muchos servicios

Salud

Consumidor (Smart Home)

Ciudades Inteligentes (Smart Cities)

Industria (Internet de las cosas Industrial – IIoT)



- Hardware
- Firmware
- Software
  - Sistemas Operativos
  - Aplicaciones
  - Frameworks

- Comunicaciones
  - Tecnologías
  - Protocolos
  - Estándares

Los dispositivos IoT presentan ***vulnerabilidades de seguridad comunes*** a otras tecnologías similares

- Mecanismos de Autenticación, Autorización y Cifrado
- Interfaces de Gestión y Administración del dispositivo IoT
- Carencias de Actualizaciones

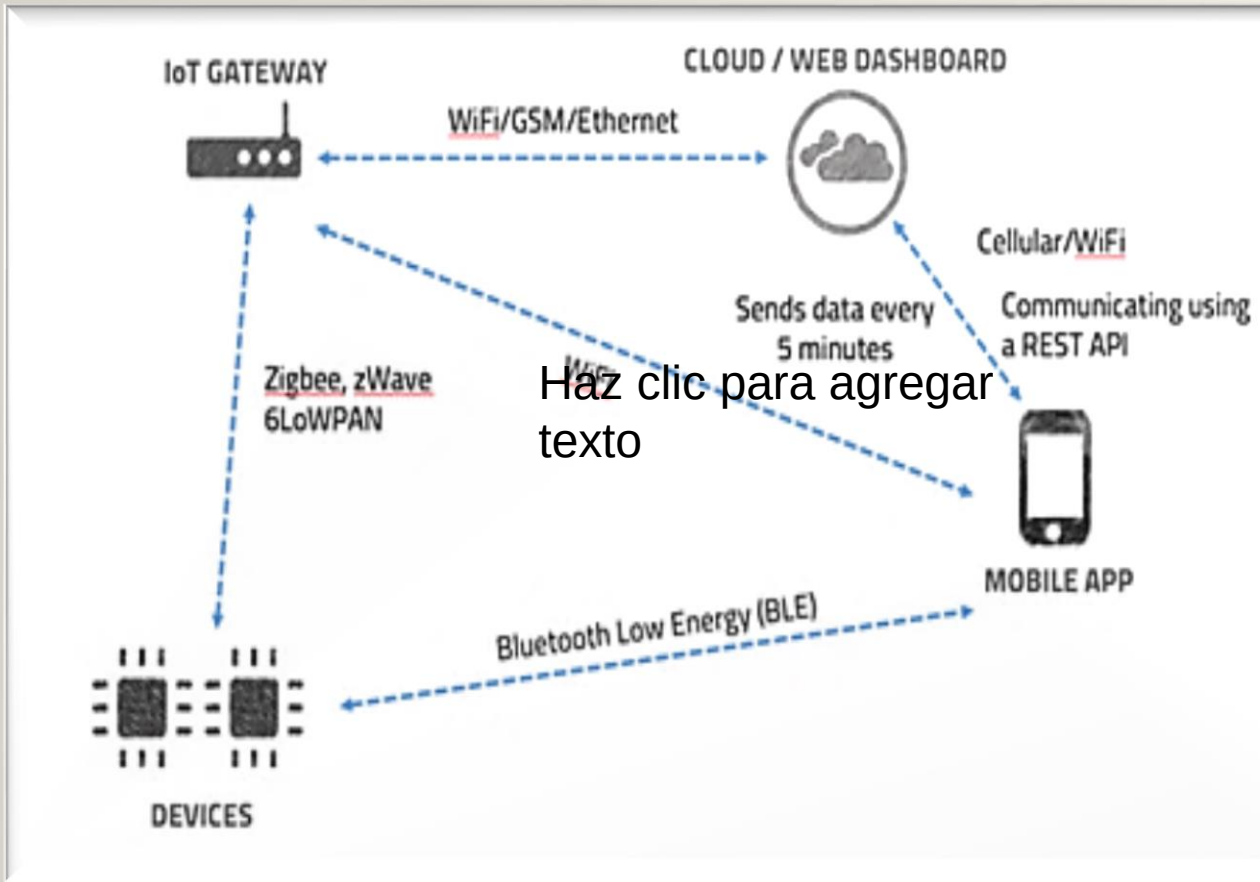
¿No le gustaría a un ladrón en potencia abrir las puertas, apagar las luces y desactivar la seguridad de su hogar?

Áreas de Superficie de Ataques

- Tomar el Control
- Robar Informacion
- Interrupcion del Servicio

- Cambiar las contraseñas por defecto de fábrica de los dispositivos y establecer contraseñas robustas.
- Si el dispositivo lo permite, deshabilitar la interfaz web
- Adquisición de dispositivos seguros y que permitan actualizaciones de seguridad.
- Habilitar su acceso a la red solo cuando sea necesario
- Evitar configurar el acceso a la red wifi de la organización
- Deshabilitar el acceso remoto a los dispositivos, desde afuera de la red interna de la organización
- Establecer un canal cifrado en las comunicaciones
- Considerar el impacto de la fuga de información que podría causar el dispositivo. ¿Podría afectar a clientes o al nombre de la compañía? Tome medidas en consecuencia.
- Investigar medidas de seguridad del fabricante del dispositivo

OWASP
Internet of Things



Haz clic para agregar texto

Somos **conscientes** de cuales son las **amenazas** que **afectan** a estos dispositivos?

OWASP TOP 10 INTERNET OF THINGS 2018

1 CONTRASEÑAS DÉBILES, PREDECIBLES O DENTRO DEL CÓDIGO

Uso de credenciales fáciles de modificar, disponibles de manera pública y/o fáciles de adivinar mediante fuerza bruta; incluyendo backdoors en firmware o en el software cliente, que permiten obtener acceso no autorizado a sistemas, aprovechando estas contraseñas vulnerables.

2 SERVICIOS DE RED INSEGUROS

Servicios de red inseguros e innecesarios corriendo en el propio dispositivo, *especialmente en aquellos expuestos a Internet*, que comprometen la confidencialidad, autenticidad o disponibilidad de la información o permiten control no autorizado de manera remota.

3 ECOSISTEMA DE INTERFACES INSEGUROS

Problemas de seguridad en interfaces web, móviles, en la nube, o API de backend en ecosistemas que están fuera de los dispositivos y que permiten que tanto los dispositivos como ciertos componentes relacionados puedan ser comprometidos

10 FALTA DE HARDENING

Falta de medidas que permitan robustecer los dispositivos desde el punto de vista físico, lo que permite a potenciales atacantes llegar a información sensible que podría ser de utilidad en un futuro ataque remoto o tomar control local del dispositivo.

6 INSUFICIENTE PROTECCIÓN A LA PRIVACIDAD

Información personal del usuario almacenada en el dispositivo o en el entorno al cual se conecta el dispositivo que es utilizada de manera poco segura, inapropiada o sin permiso.

7 TRANSFERENCIA Y ALMACENAMIENTO DE DATOS DE MANERA POCO SEGURO

Falta de cifrado o control de acceso para datos sensibles que están dentro del ecosistema; incluyendo datos en reposo, en tránsito o durante su procesamiento.

8 FALTA DE CONTROLES DE GESTIÓN

Falta de soporte de seguridad en dispositivos lanzados a producción, incluyendo la gestión de activos, gestión de actualizaciones, desarmado seguro, monitoreo de sistemas y capacidades de respuesta.

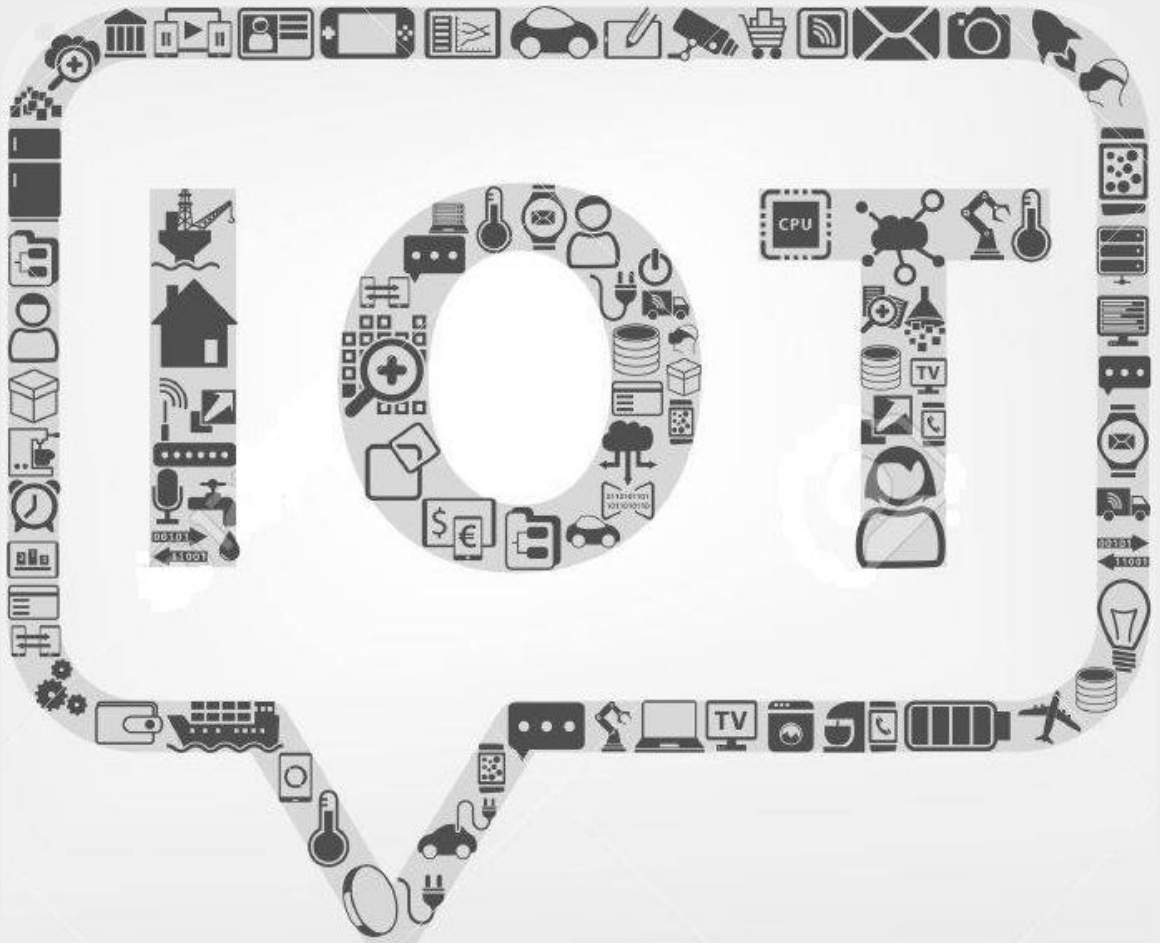
9 CONFIGURACIÓN POCO SEGURA POR DEFECTO

Dispositivos o sistemas lanzados con configuraciones por defecto poco seguras o sin la posibilidad de hacer más seguro al sistema mediante la aplicación de restricciones a partir de cambios en la configuración.

10 FALTA DE HARDENING

Falta de medidas que permitan robustecer los dispositivos desde el punto de vista físico, lo que permite a potenciales atacantes llegar a información sensible que podría ser de utilidad en un futuro ataque remoto o tomar control local del dispositivo.

Conocer la forma en que un atacante podría poner en peligro un sistema, ayuda a tomar las medidas de seguridad necesarias desde el principio, para lo cual es importante **conocer** las **amenazas**, **vulnerabilidades** y **ataques** de los sistemas y dispositivos utilizados en Internet de las Cosas.



Preguntas?

Gracias por su Atención

Arnoldo José Luis Benitez: abenitez@jussantiago.gov.ar

Seguridad Informática Poder Judicial Sgo. del Estero: seguinfo@jussantiago.gov.ar