

# [CSIOT] Tema 3: Seguridad de dispositivos IIoT: Hardware, Firmware y Middleware

- La IoT Security Foundation (IoTSF) establece directrices básicas y un enfoque para autocertificación
  - Proporciona una guía de buenas prácticas y clasifica los dispositivos en sensores, actuadores y gateways
  - Establece áreas que se deben considerar:
    - Clasificación de los datos
    - Seguridad física
    - Arraque seguro de los dispositivos
    - Sistema operativo seguro
    - Seguridad de las aplicaciones
    - Gestión de credenciales
    - Cifrado
    - Conexión de red
    - Securitización de las actualizaciones de software
    - Registro
    - Política de actualización de software
    - Evaluar el proceso de arranque seguro
    - Imágenes y firmas de las actualizaciones de software
    - Ataques de canal lateral
- La Platform Security Architecture (PAS) se centra en sistemas basados en MCU y MPU. Está diseñado para mejorar la seguridad de los dispositivos IoT.
  - Los dispositivos:
    - Tiene que ser identificables de manera única
    - Soportan un ciclo de vida de seguridad
    - Son verificables de forma segura
    - garantizan que solo se puede ejecutar software autorizado
    - soportan actualizaciones seguras
    - soportan aislamiento
    - soportan interacción sobre las fronteras de aislamiento
    - soportan un conjunto mínimo de servicios de confianza y operaciones criptográficas.
- Security Evaluation Standard for IoT Platforms (SESIP)
- Internet of Secure Things (IoXt)

## Panorama de amenazas y enfoque sistemático

### Modelado de amenazas

Proceso de:

1. Comprender un sistema
2. Identificar amenazas a este
3. Clasificar las amenazas en función a impacto y probabilidad

En el caso del modelo de microsoft este proceso es algo diferente:

1. Identificar activos
2. Describir arquitectura
3. Descomponer la aplicación
4. Identificar amenazas
5. Documentar amenazas
6. Clasificar amenazas (STRIDE):
  1. Spoofing: El atacante puede acceder con una identidad falsa
  2. Tampering: El atacante puede modificar los datos que fluyen a través de la aplicación
  3. Repudiation: Un atacante puede bloquear una acción
  4. Information Disclosure: Un atacante puede acceder a datos privados o perjudiciales
  5. Denial of Service: Un atacante puede producir fallos o reducir la disponibilidad del sistema
  6. Elevation of privilege: Un atacante puede tomar la identidad de un usuario privilegiado.

From:

<https://knoppia.net/> - **Knoppia**

Permanent link:

[https://knoppia.net/doku.php?id=master\\_cs:csiot:tm3&rev=1747947916](https://knoppia.net/doku.php?id=master_cs:csiot:tm3&rev=1747947916)

Last update: **2025/05/22 21:05**

