Ciberseguridad en IoT
Marcos de referencia

Construya seguro, compre seguro, esté seguro

Oscar Giudice

IoT CS LAC

lacnic 37
2-6 de Mayo de 2022

Introducción a IoT

Kevin Ashton en 1999 usa por primera vez el término “Internet de las Cosas”
para referirse a ***un mundo en el que todo estará conectado a internet***.

Según CISCO: Internet de las cosas "nació" entre los años 2008 y 2009

Pero ¿Que es IoT (Internet of Things, Internet de las cosas?)

La interconexión digital de objetos a través de Internet.

La seguridad en IoT

- Programas
- Marcos y
- Estándares

lacnic 37
2-6 de Mayo de 2022

La seguridad en IoT, Contexto general

IoT ≠ IT

Factores técnicos

- Consumo de energía (- / +)
- Potencia de procesamiento restringida (-)
- Poca memoria (-)
- Actualizaciones permanentes (+)
- Ciclo de vida (+)
- Factores mecánicos (+)

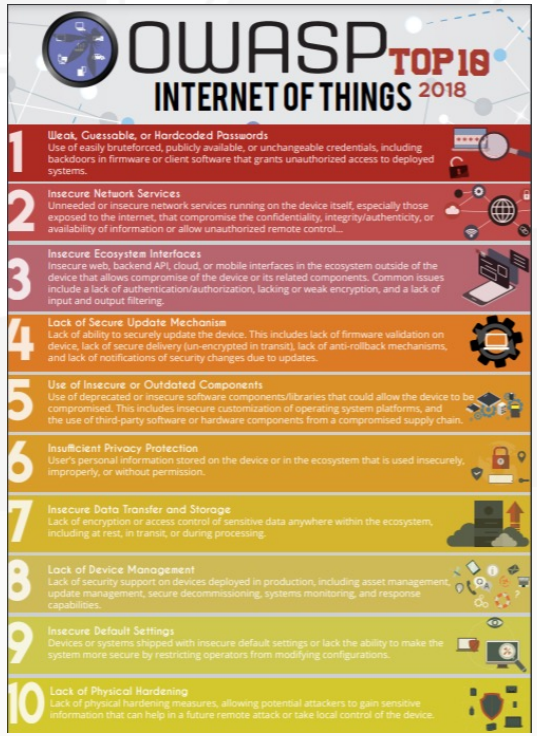
Factores de mercado

- **Acceso rápido a los mercados**
  - ~ Bajo costo
  - ~ Estrategias rápidas de lanzamiento al mercado
  - ~ Falta de experiencia o recursos para implementar seguridad
  - ~ Escasos o inexistente de mecanismos de seguridad
- **Diversidad**
  - ~ El desafío de la interoperabilidad entre estándares y las mejores prácticas al implementar tecnología IoT
  - ~ Distintas regulaciones nacionales

Equilibrio entre mecanismos de seguridad, precios, nuevas características y funcionalidades

La seguridad en IoT:
Principales vulnerabilidades de los dispositivos IoT

1) Contraseñas débiles, predecibles o dentro del código
2) Servicios de red inseguros
3) Ecosistema de interfaces inseguros
4) Falta de mecanismos de actualización seguros
5) Uso de componentes poco seguros o anticuados
6) Insuficiente protección a la privacidad
7) Transferencia y almacenamiento de datos de manera poco seguro
8) Falta de controles de gestión
9) Configuración poco segura por defecto
10) Falta de hardening



ESET: https://www.welivesecurity.com/la-es/2019/01/07/principales-fallos-seguridad-dispositivos-iot/

La seguridad en IoT: distintas propuestas para un mismo problema

El universo de las organizaciones

La seguridad en IoT: En algo nos parecemos

OBJETIVOS GENERALES DE LOS MARCOS DE CIBERSEGURIDAD PARA IOT				
Misión / Organización	IoT SF	ISOC - ISA	NIST	ENISA
Multi stakeholder	+/-	*	*	*
Agnóstico	*	*	*	*
Cultivar confianza en IoT	*	*	*	*
Fomentar la ciberseguridad en IoT	*	*	*	*
Fomentar la innovación	*	*	*	*
Promoción de la adopción de soluciones seguras de IoT	*	*	*	*
Influir / Asistir a los formuladores de políticas y regulaciones	*	*	*	*
Guías de adquisición de IoT	*	*	---	---
Mejorar la capacidad y nivel de seguridad en todo el sector de IoT	*	---	*	*
Brindar valor comercial	*	*	---	---
Empoderar a los usuarios	---	*	---	---

La seguridad en IoT: En algo nos parecemos

Algunas Características Técnicas de los marcos de ciberseguridad para IoT				
Características	IoT SF	ISOC - OTA	NIST	ENISA
Seguridad	*	*	*	*
Privacidad	*	*	*	*
Sustentabilidad a largo plazo	*	*	---	*
Confianza por diseño	*	*	*	*
Dispositivos/sensores	---	*	*	*
Comunicaciones	*	*	*	*
Servicios de backend	*	*	*	*
Aplicaciones	*	*	*	*
Múltiples iniciativas (distintos campos)	---	*	*	*

Modelos y Marcos de Seguridad para IoT

NIST

NIST National Institute of Standards and Technology
U.S. Department of Commerce

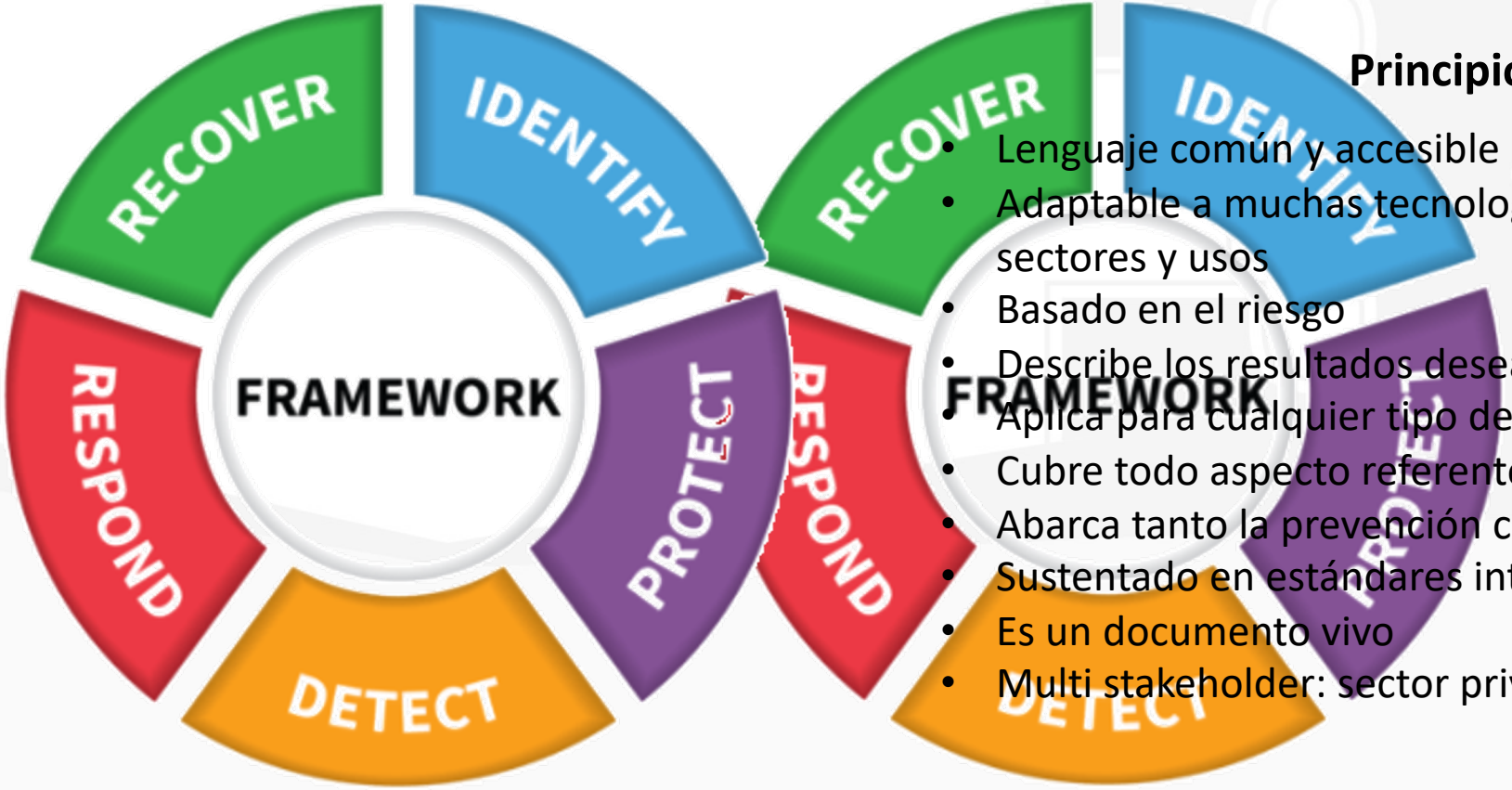
https://www.nist.gov/topics/internet-things-iot

Principios del programa de ciberseguridad para IoT

Comprensión del riesgo	Con foco en como las características de que IoT afectan la ciberseguridad del sistema y el riesgo organizacional.
Visión del Ecosistema	Ningún dispositivo existe en forma aislada
A medida de la organización	Permitir diversidad de enfoques y soluciones para todas las industrias, verticales y casos de uso
Enfoque basado en resultados	Especifica los resultados de ciberseguridad deseados y no cómo lograrlos. *Permite elegir la mejor solución para cada dispositivo de IoT y/o su entorno empresarial*
Partes interesada	NIST trabaja y colabora con diversas partes interesadas para promover la ciberseguridad de IoT. Proporciona las herramientas, la orientación, los estándares y los recursos necesarios

https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/principles

Atributos clave del marco del marco de ciberseguridad para IoT



Principios del marco

- Lenguaje común y accesible
- Adaptable a muchas tecnologías, distintas fases del ciclo de vida, sectores y usos
- Basado en el riesgo
- Describe los resultados deseados
- Aplica para cualquier tipo de gestión de riesgos
- Cubre todo aspecto referente a la ciberseguridad.
- Abarca tanto la prevención como la reacción.
- Sustentado en estándares internacionales
- Es un documento vivo
- Multi stakeholder: sector privado, academia, sector público

https://www.nist.gov/cyberframework/online-learning/five-functions

Las cinco funciones del marco

Identificar	Comprender la cultura de la organización para la gestión del riesgo de ciberseguridad de los activos: sistemas, datos, procesos y capacidades.
Proteger	Desarrollar e implementar las protecciones apropiadas para garantizar la entrega de servicios
Detectar	Desarrollar e implementar los mecanismo y actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.
Responder	Desarrollar e implementar las actividades apropiadas para tomar acción en relación con un evento de ciberseguridad detectado
Recuperar	Desarrollar e implementar las actividades apropiadas para mantener planes para la resiliencia y para reestablecer cualesquiera capacidades o servicios que hayan sido afectados durante un evento de ciberseguridad

https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide

Referencias Informativas

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Iniciativas relacionadas con la ciberseguridad de IoT

NIST

- → BLE Bluetooth
- → Cloud security
- → Cyber Threat Information Sharing
- → Cybersecurity for Cyber Physical Systems
- → Cybersecurity for Smart Grid Systems
- → **Cybersecurity Framework**
- → Cybersecurity Framework Profile for Manufacturing
- → Digital Identity Guidelines
- → NCCoE Use Case: Capabilities Assessment for Securing Manufacturing Industrial Control Systems
- → Network of Things
- → Privacy Engineering Program
- → Report on State of International Cybersecurity Standards for IoT
- → Security and privacy concerns of intelligent virtual assistances
- → RFID Security Guidelines
- → Galois IoT Authentication & PDS Pilot
- → GSMA Trusted Identities Pilot
- → Guide to Industrial Control Systems (ICS) Security
- → Lightweight Encryption
- → Low Power Wide Area IoT
- → Mitigating IoT-Based DDoS/Botnet Report
- → National Vulnerability Database
- → NCCoE IoT-Based Automated Distributed Threats
- → Security Content Automation Protocol (SCAP) Standards and Guidelines
- → Security of Interactive and Automated Access Management Using Secure Shell (SSH)
- → Security Systems Engineering
- → Software Assessment Management Standards and Guidelines
- → Supply Chain Risk Management
- → Vehicle-to-vehicle transportation
- → Wireless Medical Infusion Pumps

Links

Algunos estándares y guías disponibles

- **Gran variedad**: Bluetooth, canales de venta, criptografía, etc.
- Considerations for a Core IoT Cybersecurity Capabilities Baseline (Draft)
- **NISTIR 8228** - Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks
- **Draft NISTIR 8259** - Core Cybersecurity Feature Baseline for Securable IoT Devices (fabricantes)
- **Draft NISTIR 8267** - Security Review of Consumer Home Internet of Things (IoT) Products
- ***NIST SP 800-53***
  Security and Privacy Controls for Federal Information Systems and Organizations

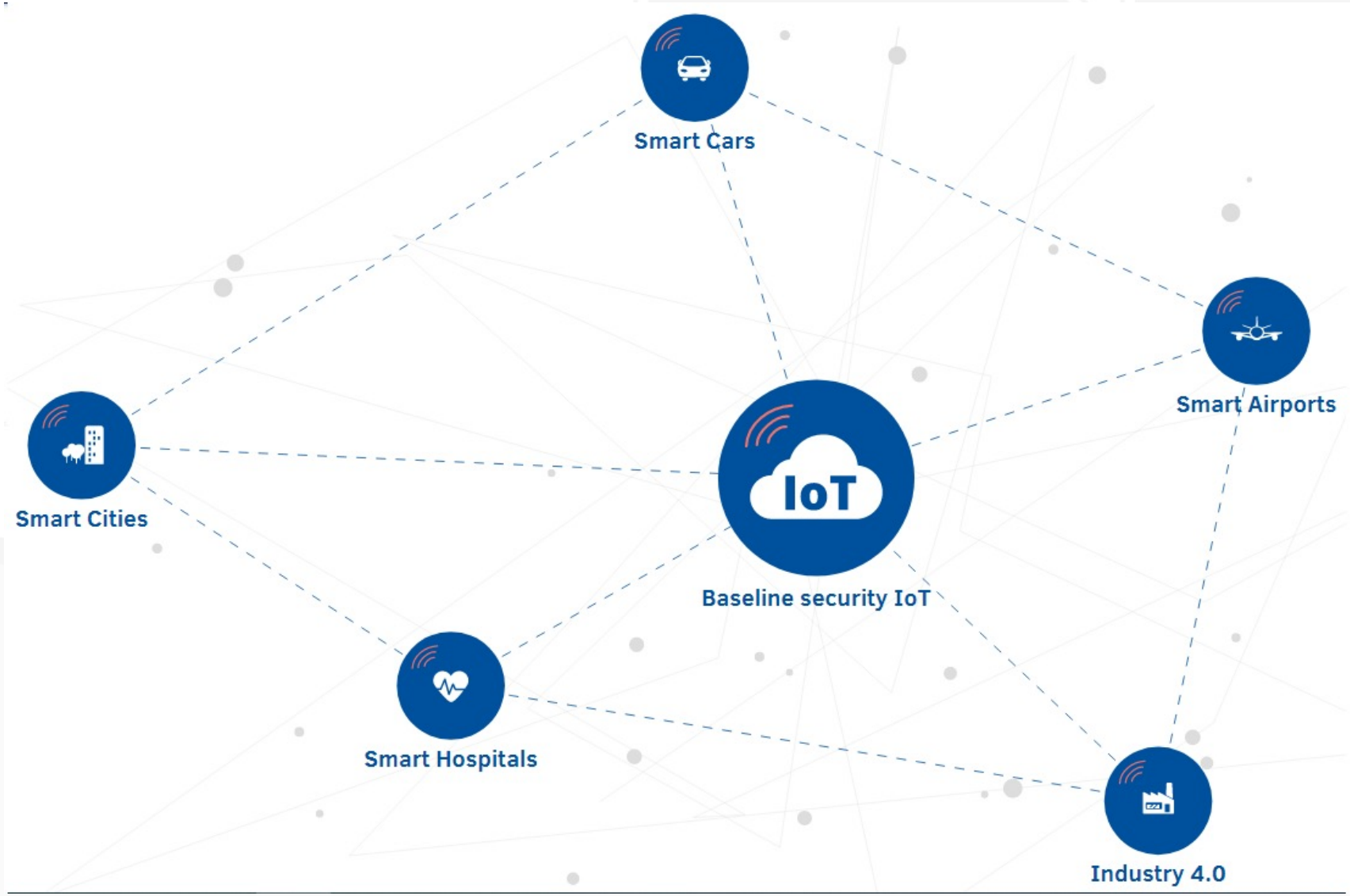
Mas información en: https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

Modelos y Marcos de Seguridad para IoT

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Herramienta de buenas prácticas para IoT y las infraestructuras inteligentes



https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

Como funciona

ENISA Good practices for IoT and Smart Infrastructures Tool

This tool intends to provide an aggregated view of the ENISA Good Practices for IoT and Smart Infrastructure that have been published the last years.

For further help on how to use the tool please consult this help guide.

Baseline security IoT | Smart Cars | Smart Hospitals | Smart Airports | Smart Cities | Industry 4.0

Here you can find in a consolidated web format all the baseline security measures and good practices as they are listed in ENISA's report: Baseli
that was published in 2017.

You shall be able to find the Good practices you seek for, according to specific filters, such as Security Measures Category, Security Domains, Th
Standards (see references column).

Publicaciones de buenas prácticas para IoT y las infraestructuras inteligentes

- Securing Machine Learning Algorithms (December 14, 2021)
- Foresight Challenges (November 22, 2021)
- Recommendations for the security of CAM (May 05, 2021)
- Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving (February 11, 2021)
- Artificial Intelligence Cybersecurity Challenges (December 15, 2020)
- Cybersecurity Stocktaking in the CAM (November 20, 2020)
- **Guidelines for Securing the Internet of Things** (November 09, 2020)
- ENISA good practices for security of Smart Cars (November 25, 2019)
- Good Practices for Security of IoT - Secure Software Development Lifecycle (November 19, 2019)
- Industry 4.0 - Cybersecurity Challenges and Recommendations (May 20, 2019)
- **IoT Security Standards Gap Analysis** (January 17, 2019)
- Good Practices for Security of Internet of Things in the context of Smart Manufacturing (November 19, 2018)
- Towards secure convergence of Cloud and IoT (September 17, 2018)
- **Baseline Security Recommendations for IoT** (November 20, 2017)
- Cyber Security and Resilience of smart cars (January 13, 2017)
- Securing Smart Airports (December 16, 2016)
- Cyber security and resilience for Smart Hospitals (November 24, 2016)
- Architecture model of the transport sector in Smart Cities (January 12, 2016)
- Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations (January 12, 2016)
- Security and Resilience of Smart Home Environments (December 01, 2015)

Links

- **Industry 4.0 - Cybersecurity Challenges and Recommendations**

  May 20, 2019

- **IoT Security Standards Gap Analysis**

  January 17, 2019

- **Good Practices for Security of Internet of Things in the conte*t of Smart Manufacturing**

  November 19, 2018

- **Towards secure convergence of Cloud and IoT**

  September 17, 2018

- **Baseline Security Recommendations for IoT**

  November 20, 2017

- **Security and Resilience of Smart Home Environments**

  December 01, 2015

https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool

Modelos y Marcos de Seguridad para IoT

IoT Security Foundation

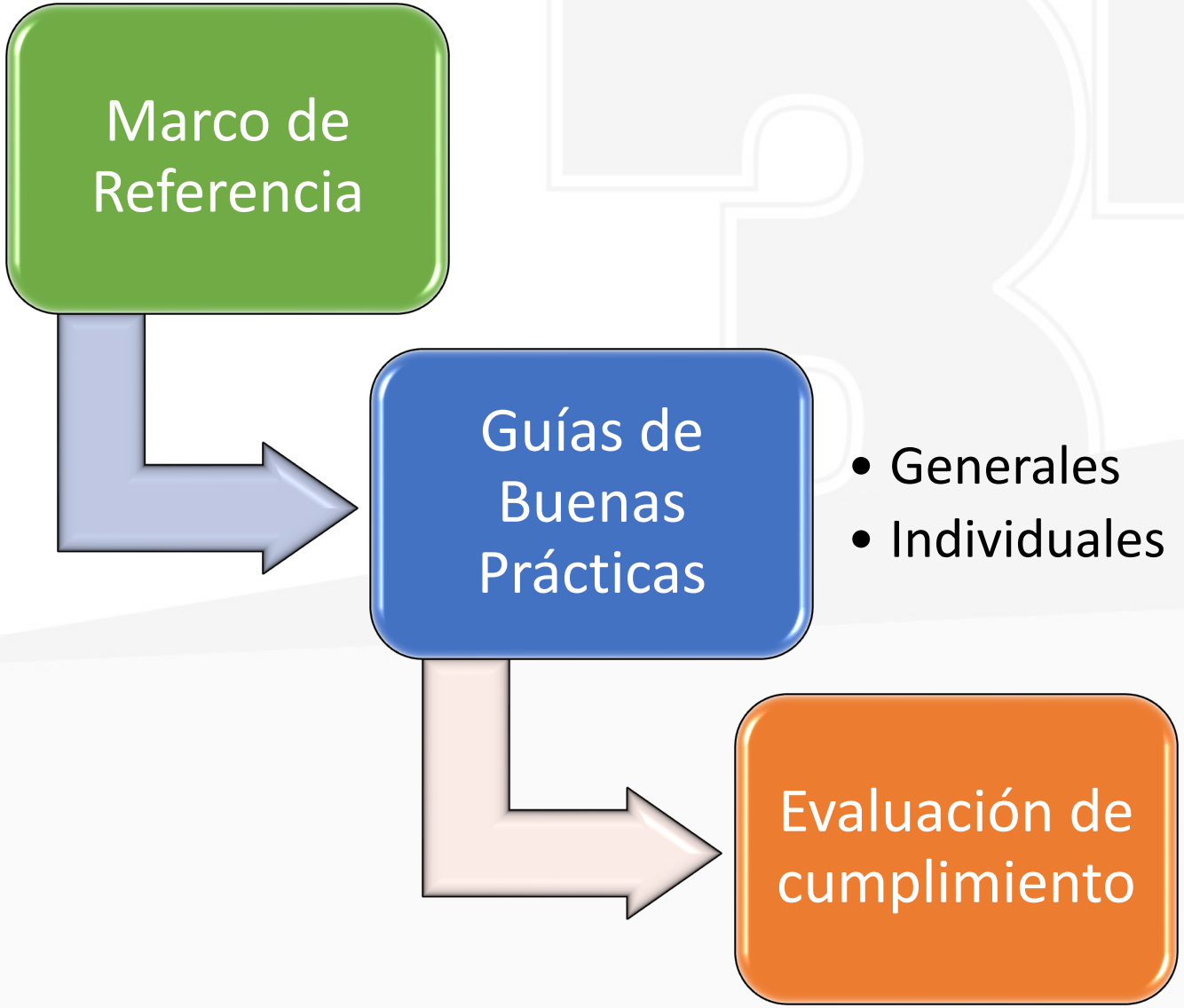
https://www.iotsecurityfoundation.org

Secure Design - Best Practice Guide

A. Clasificación de datos
B. Seguridad física
C. Inicio (Boot) seguro de los dispositivos
D. Seguridad de los sistemas operativos
E. Seguridad de las aplicaciones
F. Gestión de credenciales
G. Cifrado
H. Conexiones de red
I. Actualizaciones seguras de software
J. Registro de eventos
K. Política de actualización de software

https://www.iotsecurityfoundation.org/best-practice-guidelines

Como funciona



- Generales
- Individuales

Como funciona

Herramientas

- IoT Security Assurance Framework R 3.0 (Nov 2021)
- Secure Design Best Practice Guides R 2.0 (Nov 2019)
- IoTSF Compliance Questionnaire R 2.0 (Dec 2018)
- Otro Material de Apoyo

Como uso la Best Practice User Mark

- La marca puede ser usada por quienes implementan el Marco de Cumplimiento de Seguridad de IoT y la documentación de orientación asociada
- Sirve para
  - Comunicar que se ha considerado la seguridad de los productos o servicios y se han tomado las medidas necesarias para implantarlas
  - Demuestra que la empresa entiende que es consciente de sus responsabilidades como proveedor de productos o servicios de IoT de manera segura
- La marca de usuario puede ser usada en: material de marketing, hojas de datos de productos, embalaje, etc.
- No hace falta ser miembro de la IoTSF para usar la marca de usuario
- Uso gratuito
- ¿Cómo puedo demostrar que he utilizado el Framework?
  - Mediante un cuestionario que se usa para recopilar y registrar evidencia para respaldar la auto certificación contra el Marco; video explica cómo usarlo.

https://www.iotsecurityfoundation.org/best-practice-guidelines

Publicaciones de IoT SF

IoTSF Compliance Checklist

Security Foundation

- Assessment Steps
- Compliance Class
- Business Process
- Device Hardware
- Device Software
- Device OS
- Device Interfaces
- Authentication & Authorisation
- Encryption & Key Management
- Web User Interface
- Mobile Application
- Privacy
- Cloud and Network Elements
- Secure Supply Chain Production
- Configuration
- Device Ownership Transfer
- Notes

¡GRACIAS!

Thank you! Obrigado!

lacnic 37

2-6 de Mayo de 2022

IoT CiberSec LAC Forum 2022

Nuevas oportunidades de desarrollo

25 y 26 de agosto

lacnic37
2-6 de Mayo de 2022