

Workshop GSMA - Capacity building: Un enfoque en IoT y seguridad

Sonia Agnese
Senior Analyst Latin America

ovum.informa.com



7º CONGRESO LATINOAMERICANO
DE TELECOMUNICACIONES
1 - 5 JULIO • CORDOBA • ARGENTINA

The Cybersecurity Act strengthens ENISA



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

- The Cybersecurity Act is the European Commission's attempt to create a harmonized framework for the cybersecurity certification of ICT products and services within the EU.
- The European Union Agency for Cybersecurity is to have a stronger mandate and larger budget to help improve the coordination and cooperation in cybersecurity across EU Member States and EU institutions, agencies and bodies.
- Main ENISA tasks under the new mandate:

Policy development and implementation: to provide support to the European Commission and EU Member States in the development, implementation and review of general cybersecurity policy and in key strategic sectors identified by the NIS directive e.g. energy, transport and finance.

Operational cooperation: to strengthen the existing preventive operational capabilities, support operational cooperation as secretariat of the network of Computer Security Incident Response Teams (CSIRTs) at EU level and provide assistance on request to EU Member States to handle incidents.

Knowledge and information: to provide analyses and advice and to raise awareness, to become the one-stop shop (InfoHub) for cybersecurity information from the EU Institutions and bodies.

Capacity building: to reinforce support to EU Member States in order to improve capabilities and expertise, for instance on the prevention of and response to incidents.

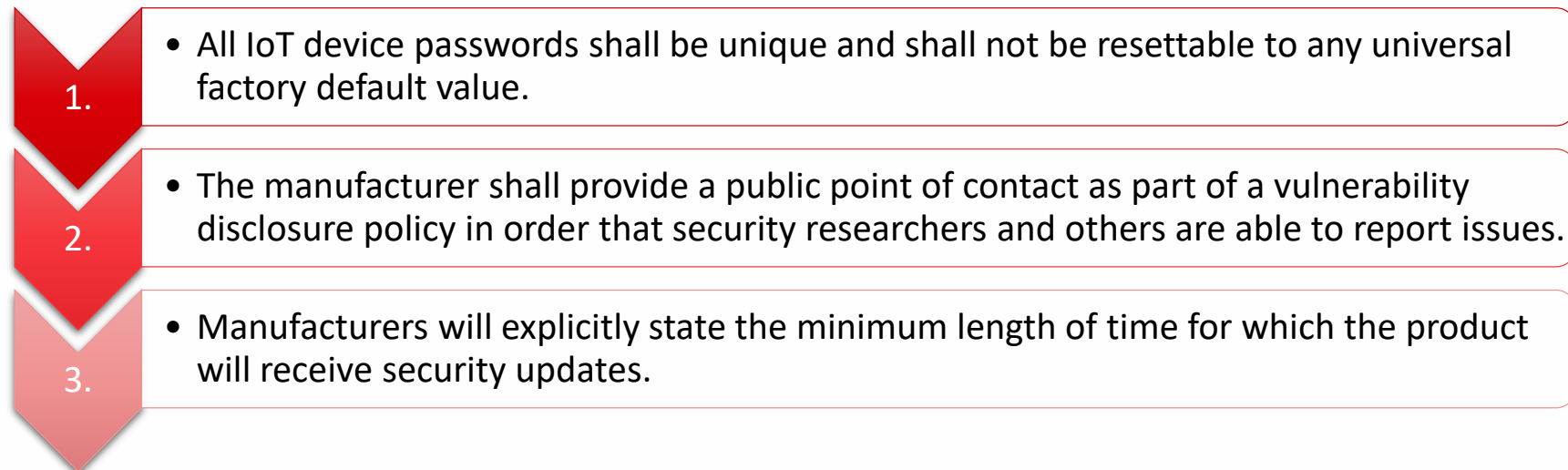
Market-related tasks within the **Cybersecurity Certification Framework** prepare candidate European cybersecurity certification schemes, with the assistance of experts and close cooperation with national certification authorities. Schemes would be adopted by the European Commission together with EU Member States. ENISA will also support policy development in information communications technology (ICT) standardisation.



UK Regulatory proposals for consumer IoT security: Secure by Design

Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security

- Self regulation has been the UK's preferred approach. In October 2018 the government published a Code of Practice for IoT Security, alongside accompanying guidance, to help industry implement good security practices for consumer IoT.
- UK govt began consulting on regulatory proposals for consumer IoT security on May 1, 2019 (now in the process of reviewing the responses).
- The government is proposing to focus on security requirements based on the 'top three guidelines' within the Code of Practice for Consumer IoT Security (requirements will be made mandatory):



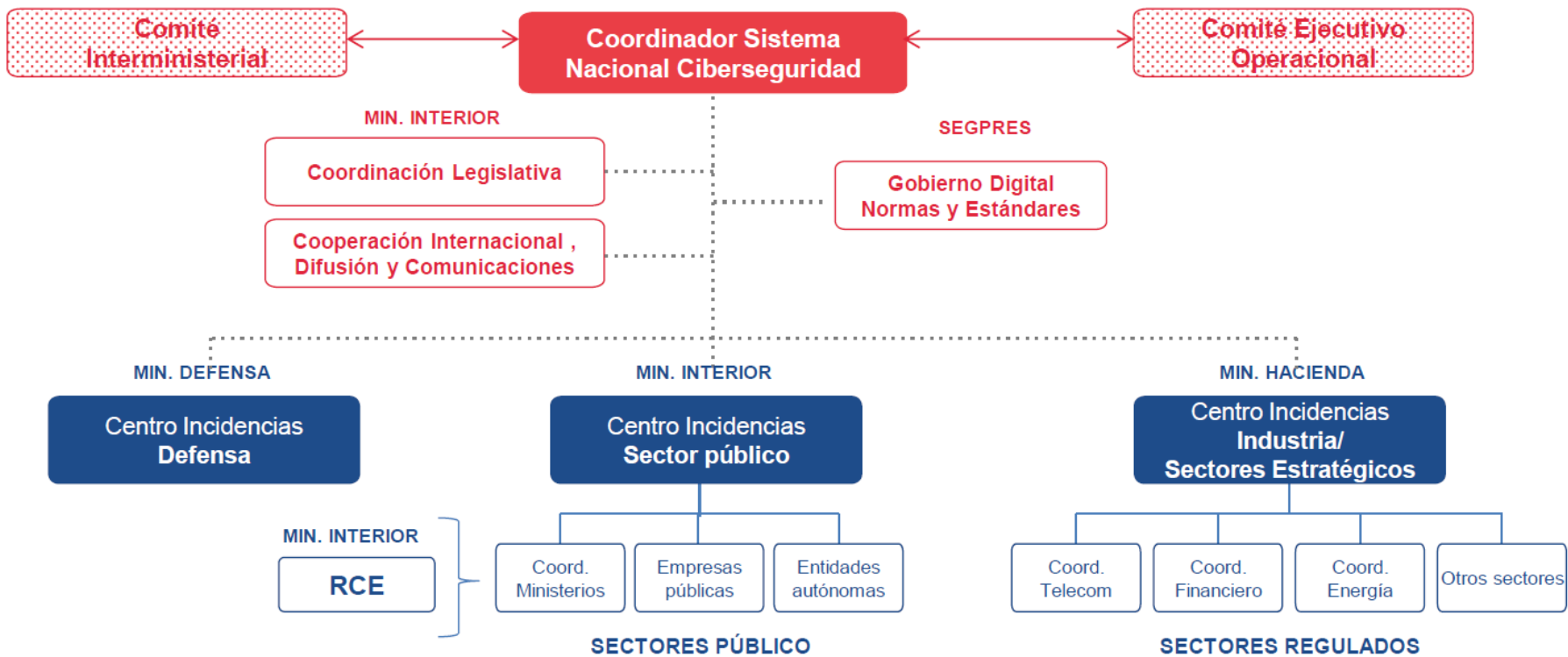
US legislators' attempts at regulating IoT security

- Legislators in the US have attempted to address the issue of IoT security through bills like the [IoT Consumer TIPS Act of 2017](#) and the [SMART IoT Act of 2017](#).
- In 2018 California became the first state in the U.S. to pass a cybersecurity law covering IoT devices: [SB-327](#), set to be put into law in 2020.
- The law requires that manufacturers of a device that connects directly or indirectly to the internet must be equipped with “reasonable” security features that are designed to prevent unauthorized access, modification or information disclosure.
- The bill aims to protect consumers, but could also potentially be applied to larger, enterprise solutions in future.
- The [Internet of Things Cybersecurity Improvement Act of 2019](#) looks to address cybersecurity in connected devices from a federal perspective.
- It would require agencies within the federal government, as well as contractors and vendors providing IoT devices to the government to be more transparent in communicating any cybersecurity vulnerabilities associated with their devices.



IoT security in Latin America: Chile

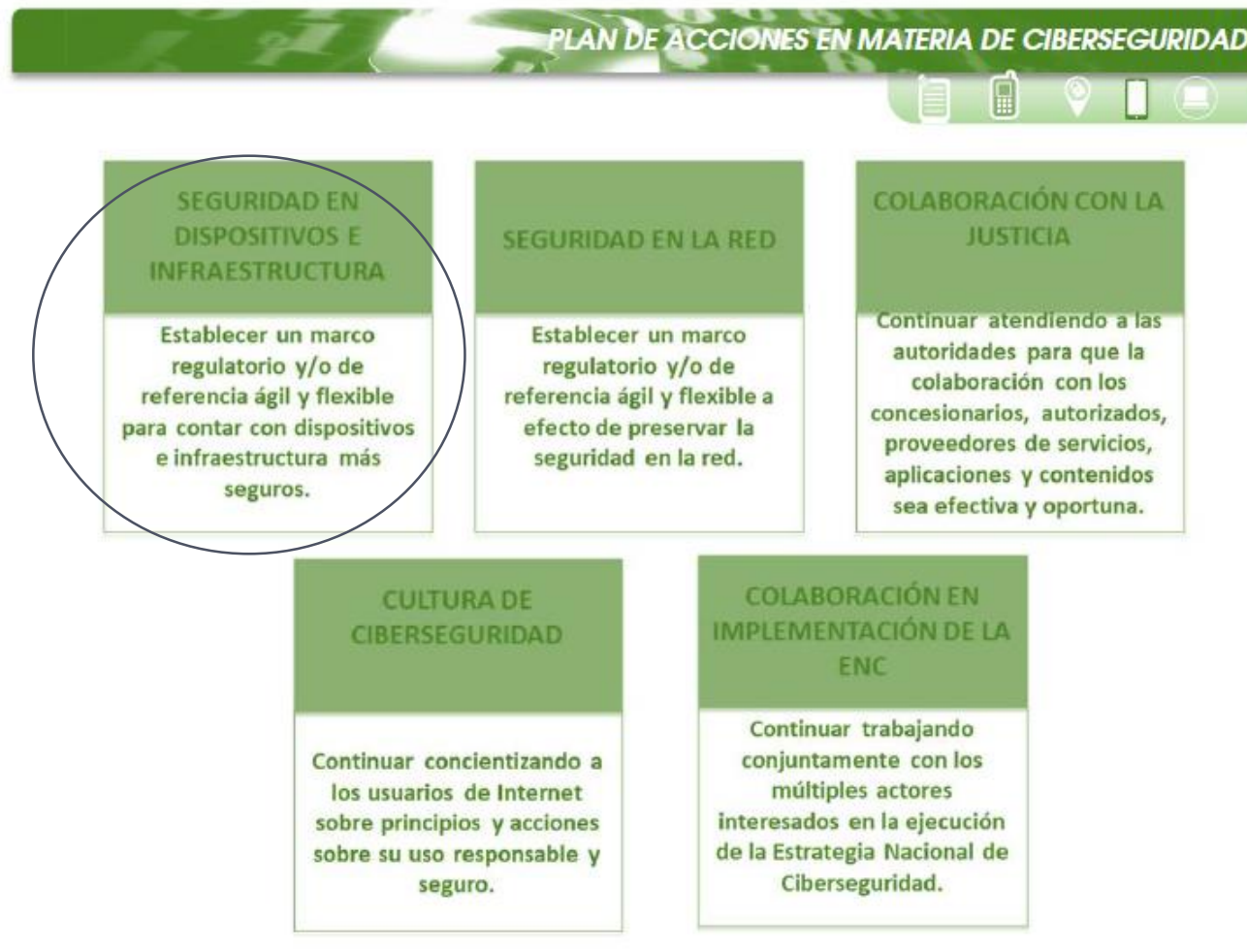
GOBERNANZA PROVISORIA DE CIBERSEGURIDAD



IoT security in Latin America: Mexico



Mexico



IoT security in Communication Service Providers

Telefónica lanzó unidad de ciberseguridad e Internet de las Cosas

By **Dinorah Navarro** - 14 abril, 2019 👁️ 212 💬 0

👍 Me gusta 1



Telefónica lanzó su propia Unidad de Cyberseguridad de IoT, un proyecto enfocado en la seguridad de Internet de las cosas (IoT, por sus siglas en inglés) que buscará hacer frente a las amenazas que enfrentan los dispositivos conectados a Internet e impulsará la adopción de IoT.

Para lograrlo, se basará en su infraestructura de red existente y en los nuevos servicios de administración de Internet de las cosas disponibles en su plataforma Kite, una plataforma de conectividad de dispositivos IoT que permite a los clientes mejorar la eficiencia y la reducción de costos.





Muchas gracias!

Sonia.Agnese@ovum.com
