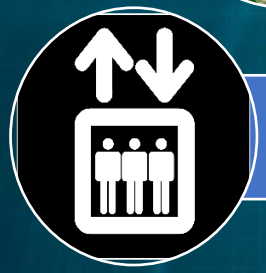
Importancia de la seguridad de la información en el Sector Salud


COURTESY: WIRED
PROFESSIONAL HACKERS SHOW HOW EASY
IT IS TO HIJACK A CAR'S COMPUTER


MPH
FEET

Edificios inteligentes

Gestión y demanda de energía



Elevadores

Automatización de salas

Seguridad Física

Aire acondicionado e iluminación

Monitoreo y control en tiempo real

Redes de comunicaciones para voz y datos

Administración de activos e instalaciones

Control y señalamiento en estacionamientos

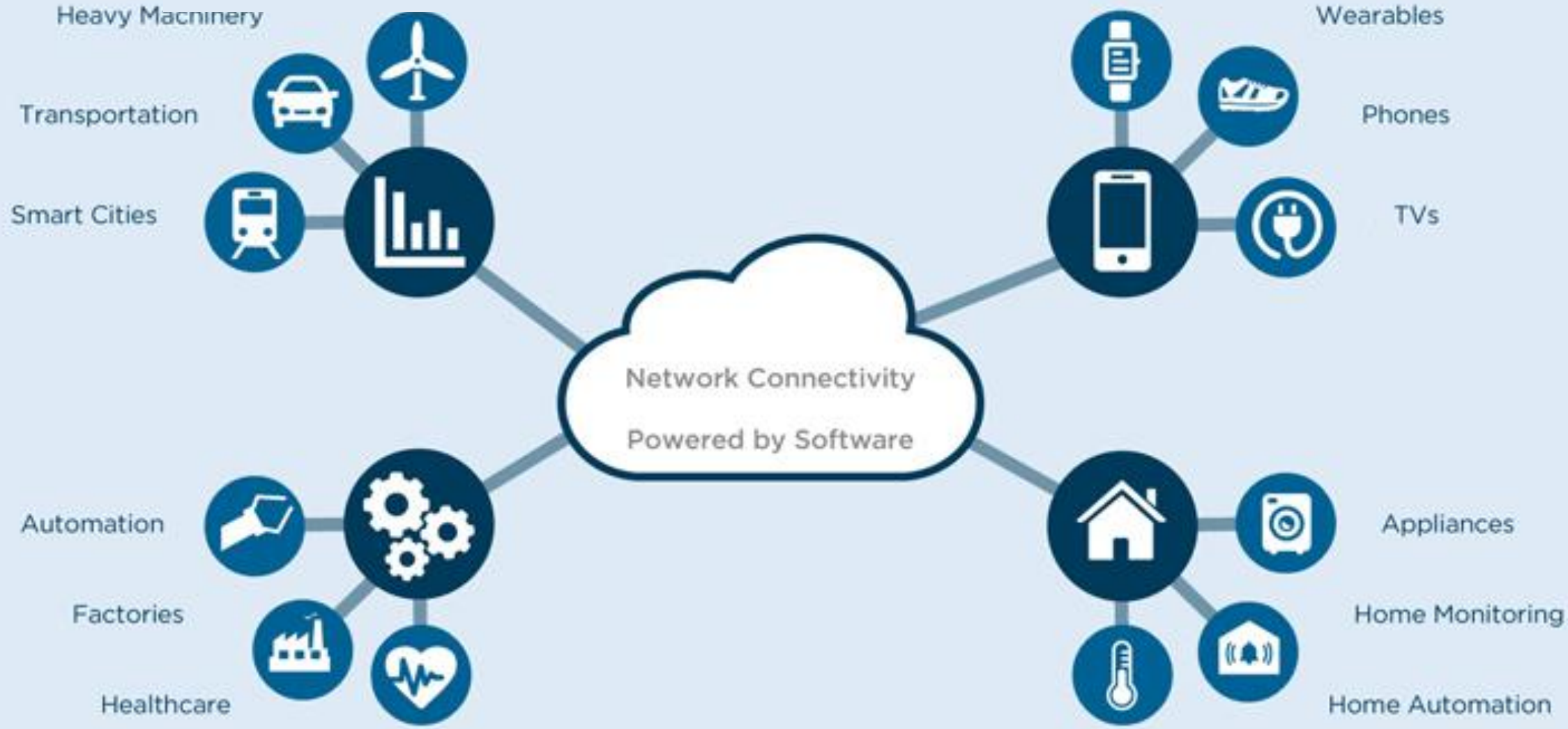
Equipo contra incendio

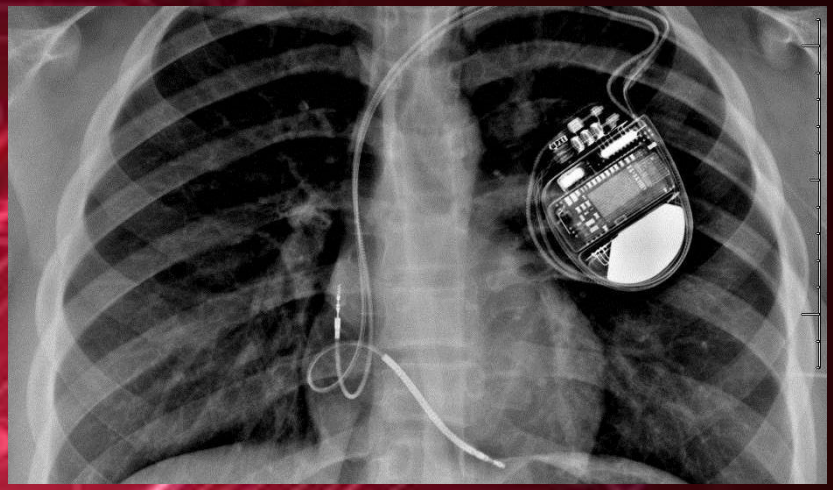

Smart Parking
Smart Health
Public Safety
Smart Buildings
Waste Management
Open Data
Education
Traffic Management
Smart Environment
Electromagnetic Emissions
Internet of Things
Smart Energy
Smart Street Lights
Gas & Water Leak Detection
SMART CITY
Air Pollution
Water Quality
Smart Home
Intelligent Shopping
Electric Vehicle Charging


Bathroom
Doctors will be able to give you virtual medical checks
Toilets will analyse waste for medical problems such as colon cancer.
Roof
Power collected through solar panels and stored in backup resources to power house and car.
Bedroom
Smart books interact with the house's 3D and virtual reality system, bringing to life what you read.
Bedroom
Clothes made with smart fabrics regulate your temperature and monitor your health
E-commerce will become F-commerce - online consumers will be able to enjoy a tailored shopping experience based on Facebook 'Likes'.
Kitchen
Smart surfaces identify what's on them and have the ability to react accordingly - keeping coffee cups warm and iced-tea cold.
Refrigerators will advise on recipes based on whats in stock and creates personal diets.
PLUSNET ROAD
Living Room
All appliances connected through invisible networking system
Entertainment system creates life like sounds, images and experiences to completely envelop you in near 4D experience.
Garage
Camera at entrance has facial recognition software which is linked to criminal database
Car which is able to drive itself.
Office
See-through electronics, screens, touch panels and tactile displays deliver 3D holographic experiences
Contact lenses allow you to access infinite information resources instantly before your eyes.

Dispositivos de Control Industrial (IIoT e ICS)

Dispositivos de Consumo (IoT)

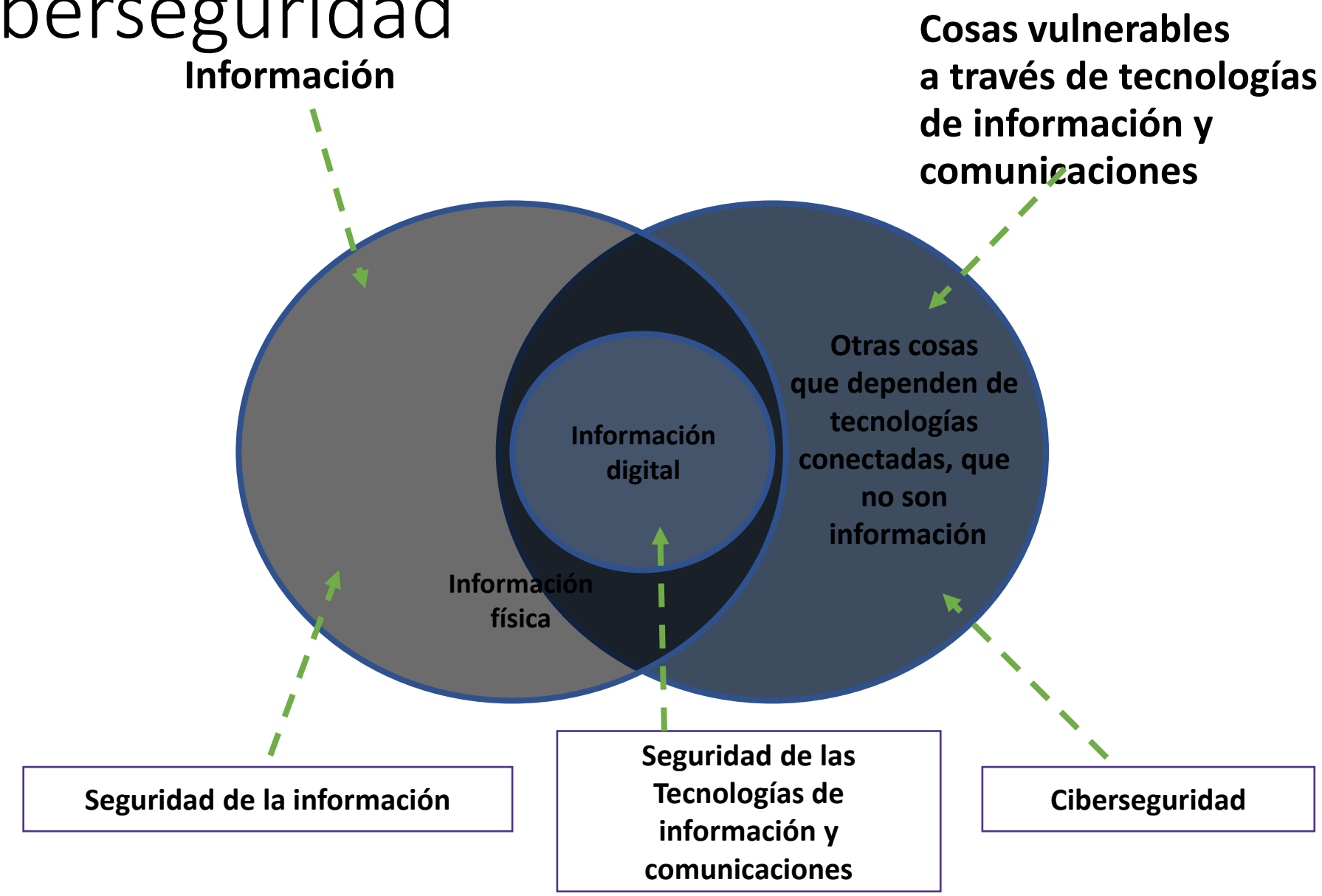


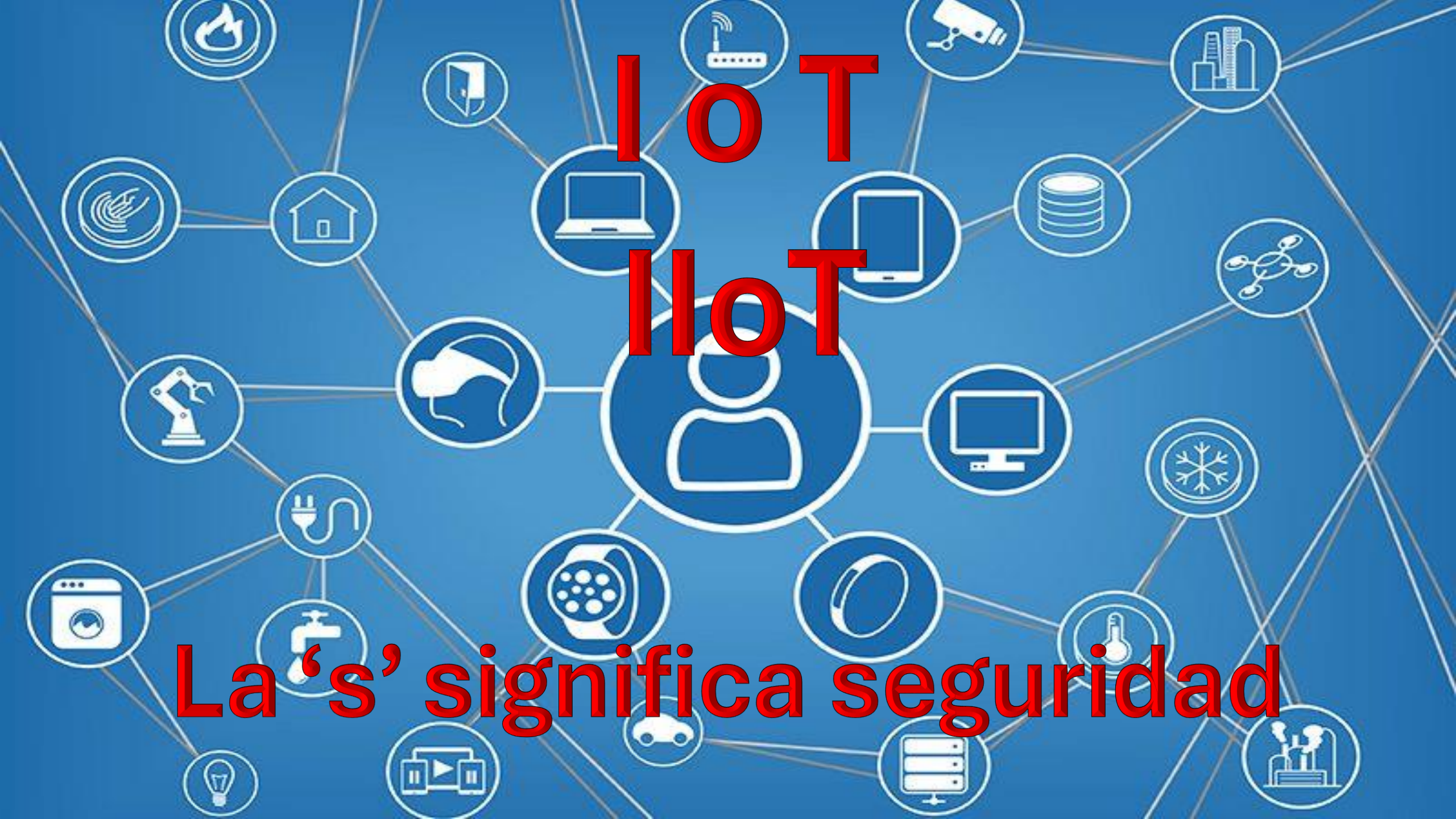


IoT en el cuerpo humano


Cloud
Mobile
PC
Remote Server
Database

Ciberseguridad




I o T
IIoT
La ‘s’ significa seguridad

Desafíos en la Infraestructura de Red

- Aumento de dispositivos conectados
- Gestión de identidades y accesos
- Protección de datos en tránsito
- Manejo de altos volúmenes de información

¿ Qué datos personales tienen las empresas de ti?

- Nombre
- Edad
- Fecha de nacimiento
- Estado civil
- Hábitos
- Teléfono
- Trayectoria académica
- Fotografía
- Nacionalidad
- E-mail
- Religión
- Dirección de correo electrónico
- Foto de perfil
- Lugar de residencia
- Lugar de nacimiento
- Creencias ideológicas y religiosas
- Idiomas
- Sexo
- Estado Civil y situación sentimental así como si se tienen hijos
- Intereses
- Empresa en la que trabaja
- Historial de empresas trabajadas
- Formación (escuela, colegio, universidad…)
- Habilidades profesionales
- Cruce datos con contactos para alimentar el perfil de manera automática

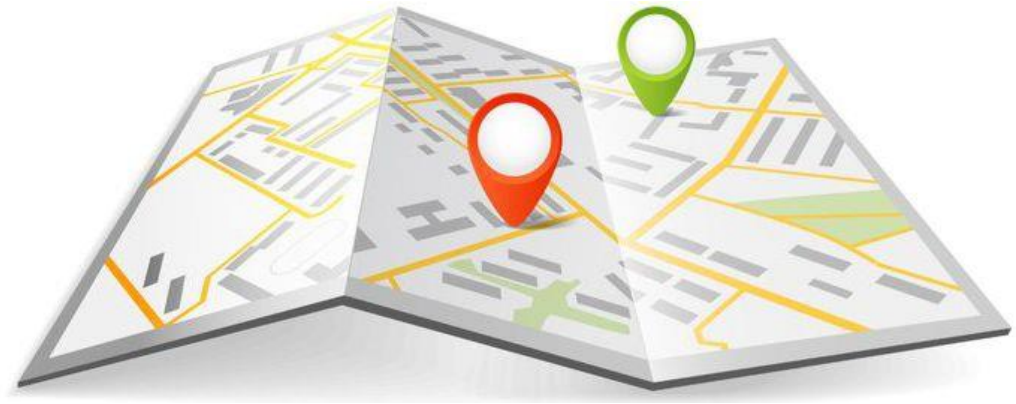
- Geolocalización
- Cruce con eventos locales, regionales, reacciones y comentarios en publicaciones
- Reconocimiento de imágenes (lugar de la foto, las personas que están en ella…)
- Teléfono que tienes y las apps que tienes (WhatsApp, Instagram, AirBnB…)

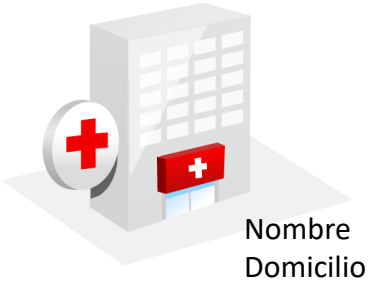
ticketmaster

Nombre
E-mail
No. tarjeta
CVV
Preferencias
Historia de eventos

Nombre
E-mail
Ubicación
No. tarjeta
CVV
Celular
Historial

UBER





Nombre
Domicilio
E-mail
Teléfono
Estado de salud
No. tarjeta
CVV

Nombre
E-mail
Ubicación
Frecuencia cardiaca

Nombre
E-mail
No. tarjeta
CVV

City Water Supply

By Ryan Naraine
February 8, 2021

Hacker Remotely Increased Sodium Hydroxide Levels in City's Water from 100 Parts Per Million to 11,100 Parts Per Million.

Colonial Pipeline Cyber Incident

Office of Cybersecurity, Energy Security, and Emergency Response

On May 7, 2021, the Colonial Pipeline Company proactively shut down its pipeline system in response to a ransomware attack. On May 13, 2021, Colonial Pipeline announced the company restarted their entire pipeline system and product delivery commenced to all markets.

During the Colonial Pipeline incident, the Department of Energy (DOE) Energy Response Organization was activated to coordinate with industry, interagency, and state partners, providing situational awareness, analysis of impacts, and supporting response efforts. DOE coordinated a whole-of-government response to help support Colonial resume operations quickly and safely, while moving fuel supplies to impacted areas to mitigate impacts to consumers.

SECURITY & PRIVACY

Medical nightmare: electronic health devices can be hacked with deadly results

BY KIM KOMANDO, KOMANDO.COM • JUNE 28, 2019 SHARE:

Cyberattacks target more than companies and governments. Millions of Americans using high-tech

Most Popular

Diferencia entre el Qué y el Cómo

Estándares de Seguridad de la Información y ciberseguridad

ISO/IEC 27014:2013 Information technology -- Security techniques -- Governance of information security

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection -- Information security management systems -- Requirements

ISO/IEC 27002:2022

Information security, cybersecurity and privacy protection — Information security controls

ISO 27799:2016

Health informatics — Information security management in health using ISO/IEC 27002

ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity

ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018:2019 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27019:2017 Information technology -- Security techniques -- Information security controls for the energy utility industry

Controles en 27002 y otros estándares

Disposal of media

- ISO/IEC 27040:2015 Information technology -- Security techniques -- Storage security

Access control and communication security

- **Network Security**
  - ISO/IEC 27033-1:2015 Security techniques -- Network security -- Part 1: Overview and concepts
  - ISO/IEC 27033-2:2012 Security techniques -- Network security -- Part 2: Guidelines for the design and implementation of network security
  - ISO/IEC 27033-3:2010 Security techniques -- Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues
  - ISO/IEC 27033-4:2014 Security techniques -- Network security -- Part 4: Securing communications between networks using security gateways
  - ISO/IEC 27033-5:2013 Security techniques -- Network security -- Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

Backup and media handling

- ISO/IEC 27040:2015 Information technology -- Security techniques -- Storage security

System acquisition, development and maintenance

- **Application Security**
  - ISO/IEC 27034-1:2011 Security techniques -- Application security -- Part 1: Overview and concepts
  - ISO/IEC 27034-2:2015 Security techniques -- Application security -- Part 2: Organization normative framework
  - ISO/IEC 27034-3:2018 Application security -- Part 3: Application security management process
  - ISO/IEC CD 27034-4 Application security -- Part 4: Validation and verification
  - ISO/IEC 27034-5:2017 Security techniques -- Application security -- Part 5: Protocols and application security controls data structure
  - ISO/IEC 27034-6:2016 Security techniques -- Application security -- Part 6: Case studies
  - ISO/IEC 27034-7:2018 Application security -- Part 7: Assurance prediction framework

Intrusion Detection and Prevention

- 13.1.1 Network controls
  14.1.2 Securing application services on public networks
  14.1.3 Protecting application services transactions
  - ISO/IEC 27039:2015 Security techniques -- Selection, deployment and operations of intrusion detection and prevention systems (IDPS)

Supplier relationships

- ISO/IEC 27036-1:2014 Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts
- ISO/IEC 27036-2:2014 Security techniques -- Information security for supplier relationships -- Part 2: Requirements
- ISO/IEC 27036-3:2013 Security techniques -- Information security for supplier relationships -- Part 3: Guidelines for information and communication technology supply chain security
- ISO/IEC 27036-4:2016 Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services

Information security incident management

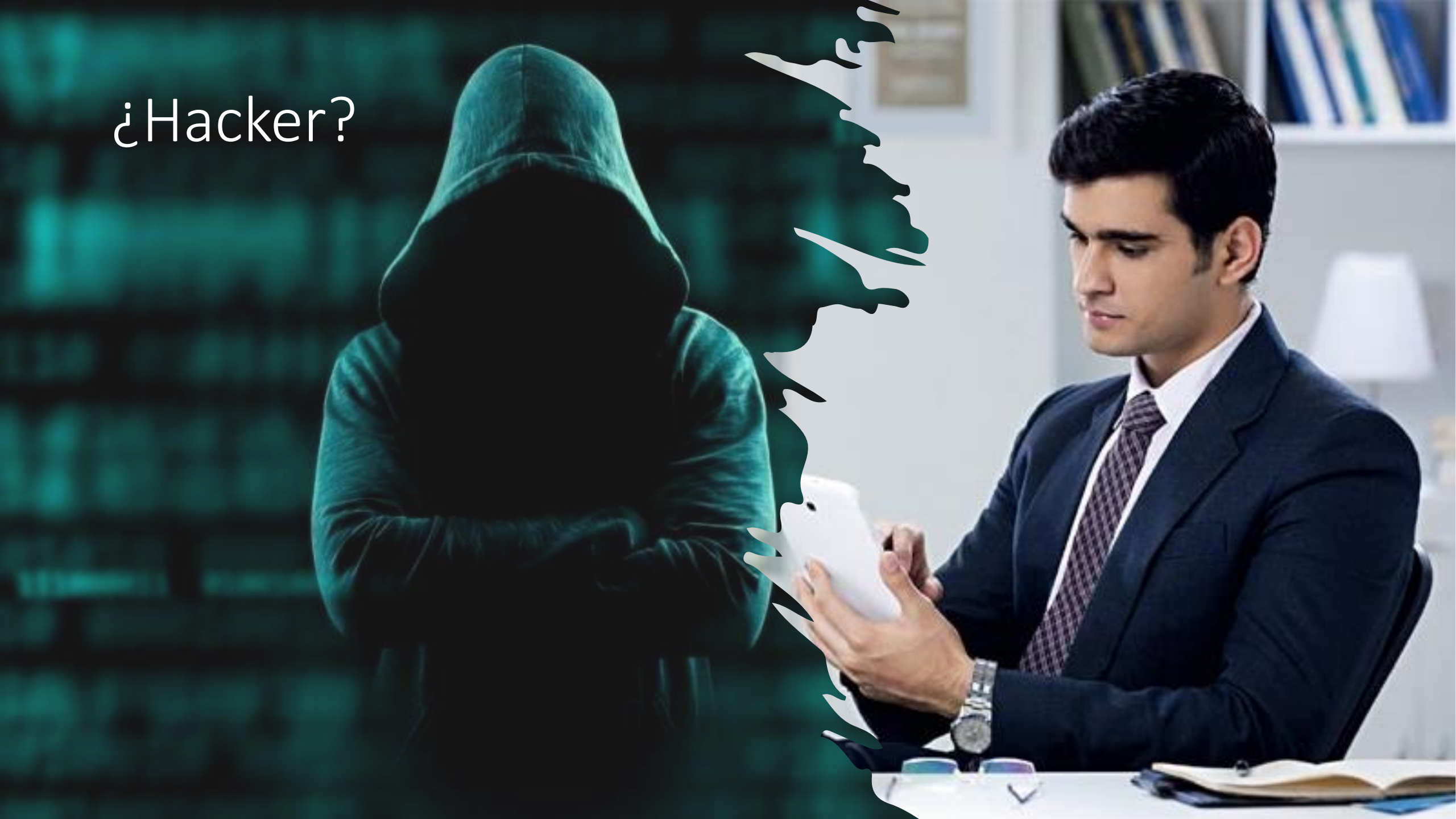
- ISO/IEC 27035-1:2016 Security techniques -- Information security incident management -- Part 1: Principles of incident management
- ISO/IEC 27035-2:2016 Security techniques -- Information security incident management -- Part 2: Guidelines to plan and prepare for incident response
- ISO/IEC 27037:2012 Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence
- ISO/IEC 27042:2015 Security techniques -- Guidelines for the analysis and interpretation of digital evidence
- ISO/IEC 27043:2015 Security techniques -- Incident investigation principles and processes

Information security aspects of business continuity management

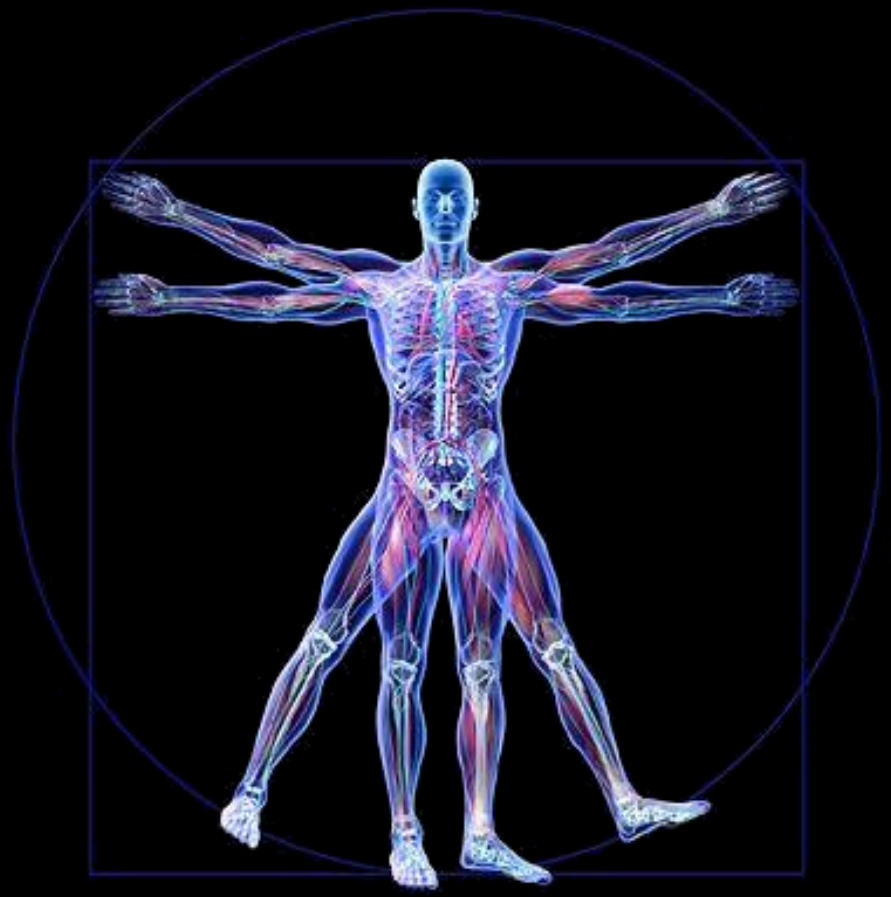
- ISO/IEC 27031:2011 Security techniques -- Guidelines for information and communication technology readiness for business continuity

This is not a comprehensive list, they are examples

¿Hacker?



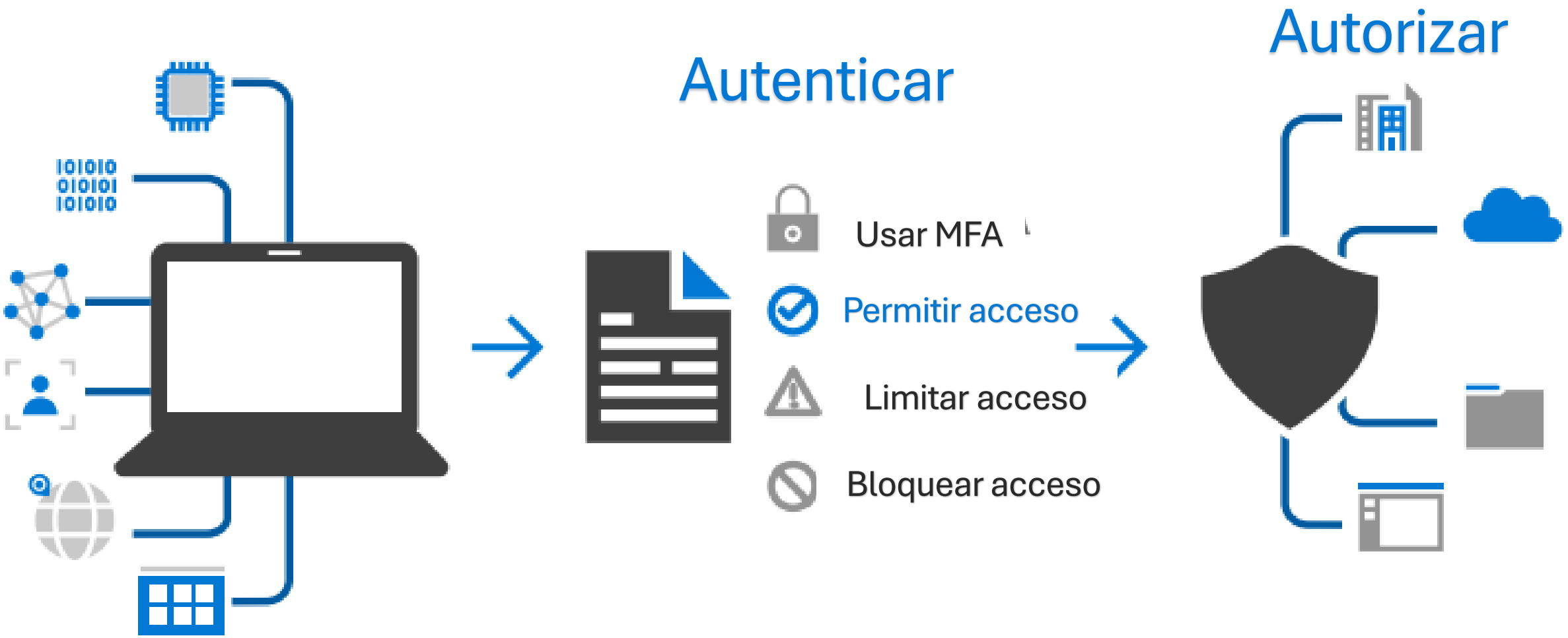
El cuerpo humano es el sistema más antiguo que hemos asegurado



Tenemos que mantener nuestros sistemas y redes saludables

Identificar y Monitorear los Signos Vitales Seguir las Mejores Prácticas

Autenticación y Autorización




Zep
COMMERCIAL
Quick Clean
Disinfectant
32

Dirección de correo electrónico del remitente (en este caso el dominio del que salió el correo es hakoonalo·com no de sat·gob·mx)
Este dato aparece en algunas aplicaciones de correo solamente al pulsar sobre el nombre del remitente

DS **Servicio de Administración Tributaria**
Devoluciones SAT <devolucion@sat.gob.mx> <devolucion@sat.gob.mx.hakoonalo.com>

Nombre del remitente (este es un texto que cualquiera puede modificar, en este caso devolucion@sat·gob·mx es parte del nombre que el remitente usó para denominarse)

HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

SAT
SERVICIO DE ADMINISTRACIÓN TRIBUTARIA

Apreciable Contribuyente:

Adjunto puedes encontrar el archivo con los datos para su devolución correspondiente al ejercicio 2022

Atentamente

Devoluciones SAT

¡Gracias por cumplir!

Este mensaje de correo electrónico se ha enviado desde una dirección exclusivamente para envíos, no lo respondas.

En el SAT únicamente enviamos correos electrónicos con información y nunca solicitamos, por este medio, la instalación de software alguno.
Si requieres asesoría fiscal o más información, no devuelvas este mensaje y contáctanos por alguno de los siguientes medios:

sat.gob.mx SAT México SATMx SATMx MarcaSAT 55 627 22 728

Tienes derecho a ser informado y asistido por las autoridades fiscales con respeto y consideración.
Si requieres orientación o auxilio acerca de tus derechos y medios de defensa, acude a la Procuraduría de la Defensa del Contribuyente, prodecon.gob.mx, o llama al 800 61 10 190. La información de este correo no establece obligaciones ni crea derechos distintos de los contenidos en las disposiciones fiscales.

Para evitar caer en este tipo de engaños:
- ✓ **Asegúrate que el correo viene de la dirección legítima del remitente**
- ✓ **No abrir archivos adjuntos de personas desconocidas**
- ✓ **No habilitar macros a menos que estemos absolutamente seguros de que es un archivo legítimo**

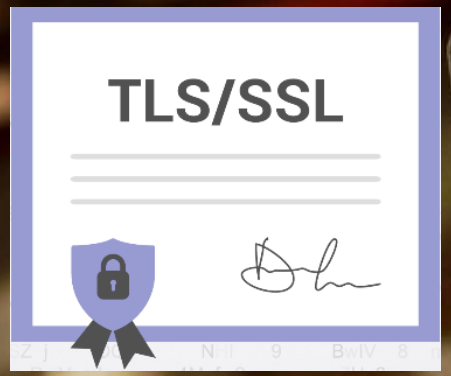
Adjuntan un archivo en formato ·doc
Este archivo está en un formato obsoleto (el vigente sería ·docx) y se considera inseguro ya que contenía macros, en este caso el archivo recibido contiene código malicioso que busca infectar el equipo del destinatario

La firma e información al pie del correo, si bien tiene datos correctos, pueden solo haber sido copiados y pegados de alguna comunicación legítima

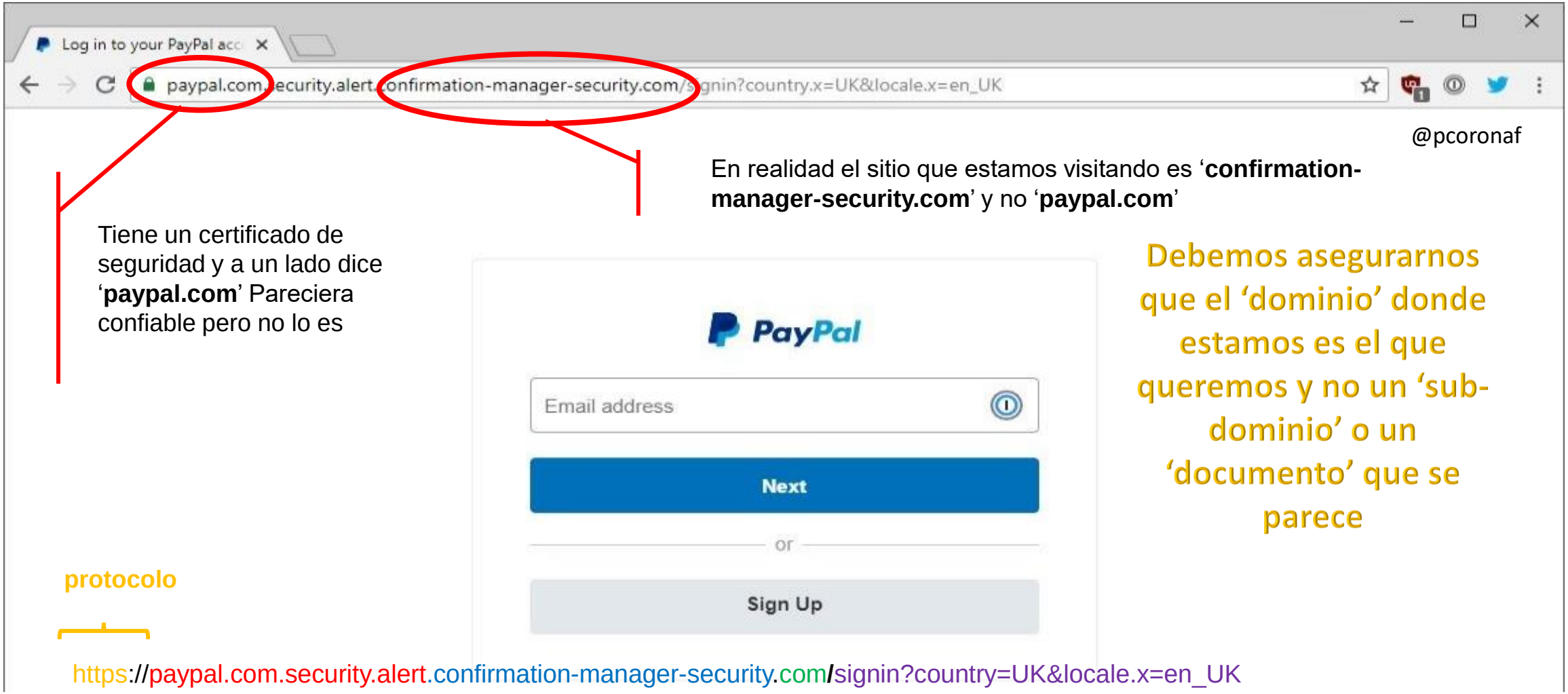
@pcoronaf

Complementar con Parches y Actualizaciones

Aislamiento ante las Amenazas Externas



¿Cómo Identificar una Dirección de Internet Segura?




Atención a las alertas

Trazabilidad

¿Qué?

¿Quién?

¿Dónde?

Correlación de actividades

Usar las herramientas adecudas

Realizar pruebas

Armas autónomas

Inteligencia Artificail

Algunos retos

Transparencia/ explicabilidad de los algoritmos

Cómputo cuántico

Gracias

Interacción
Preguntas
Llamado a acciones

Pablo Corona Fraga
pcoronaf@nyce.org.mx

Twitter: @pcoronaf