bidaidea

CYBERSECURITY &
INTELLIGENCE

Jornadas:

La necesidad de la **Ciberseguridad Privada**

Retos y Oportunidades

Mikel Rufián Albarrán

18 de Diciembre de 2022

> La Ciberseguridad no es un estado, es un proceso continuo que involucra a toda la organización.

Mikel Rufián Albarrán

Managing Director – Head of Global Cybersecurity, Intelligence & Industry Lab

Mikel.rufian@bidaidea.com

Telf: (+34) 670 025 091

@mrufian

es.linkedin.com/in/mikelrufian

www.CiberseguridadBidaidea.com

Sólo hay dos tipos de empresas: las que han sido atacadas y las que no saben que han sido atacadas.

Bidaidea– Cybersecurity & Intelligence

Gracias a la creciente convergencia entre la seguridad física y la informática, el compromiso corporativo con la seguridad integral ha aumentado.

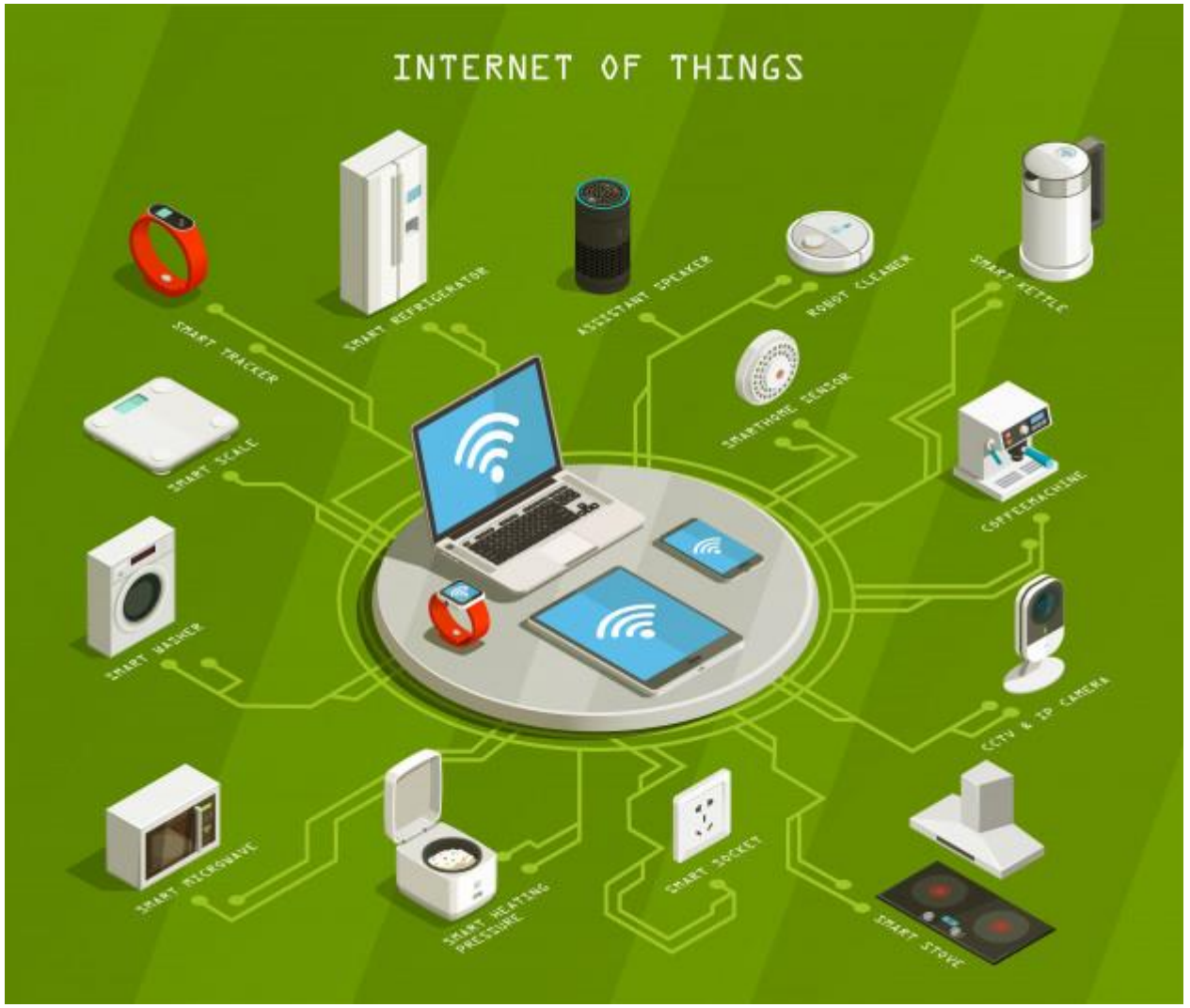
"…Seguridad Integral…"

Y en ese sentido, se han sumado a los organigramas corporativos las áreas de inteligencia y Ciberseguridad, que aplican de buena manera al campo de la seguridad.

Estado del Arte


mundos
VIRTUAL
+
FÍSICO
=
REAL
Seguridad Integral
Transformación Digital

Crecimiento exponencial del IoT – Internet de las Cosas



IoT ayudará y afectará a todos

Hoy en día los datos se convierten en nosotros mismos

¿Qué involucra el Ciberespacio?

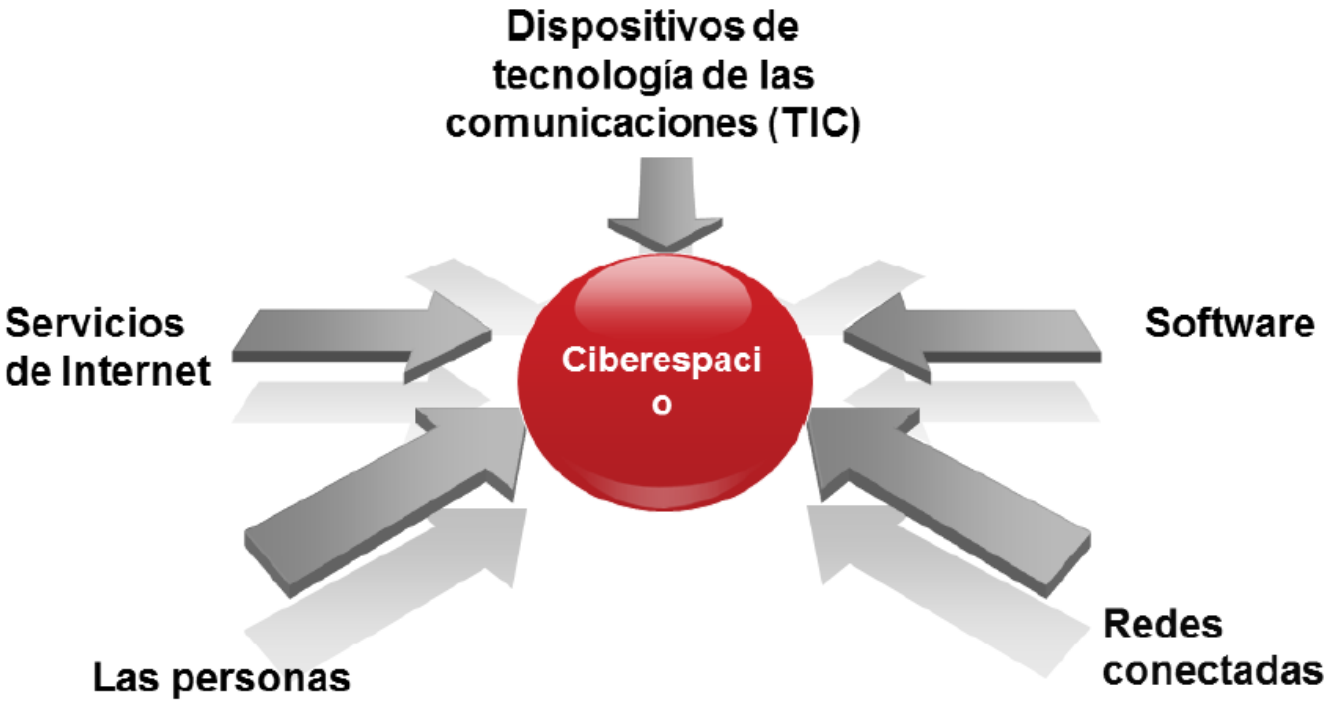
Ciberespacio

Entorno complejo resultante de la interacción entre las personas, el software y los servicios en Internet por medio de dispositivos tecnológicos conectados a redes, las cuales no existen en ningún tipo de forma física

Servicios de aplicaciones en el ciberespacio

Servicios de aplicación provistos a través del ciberespacio

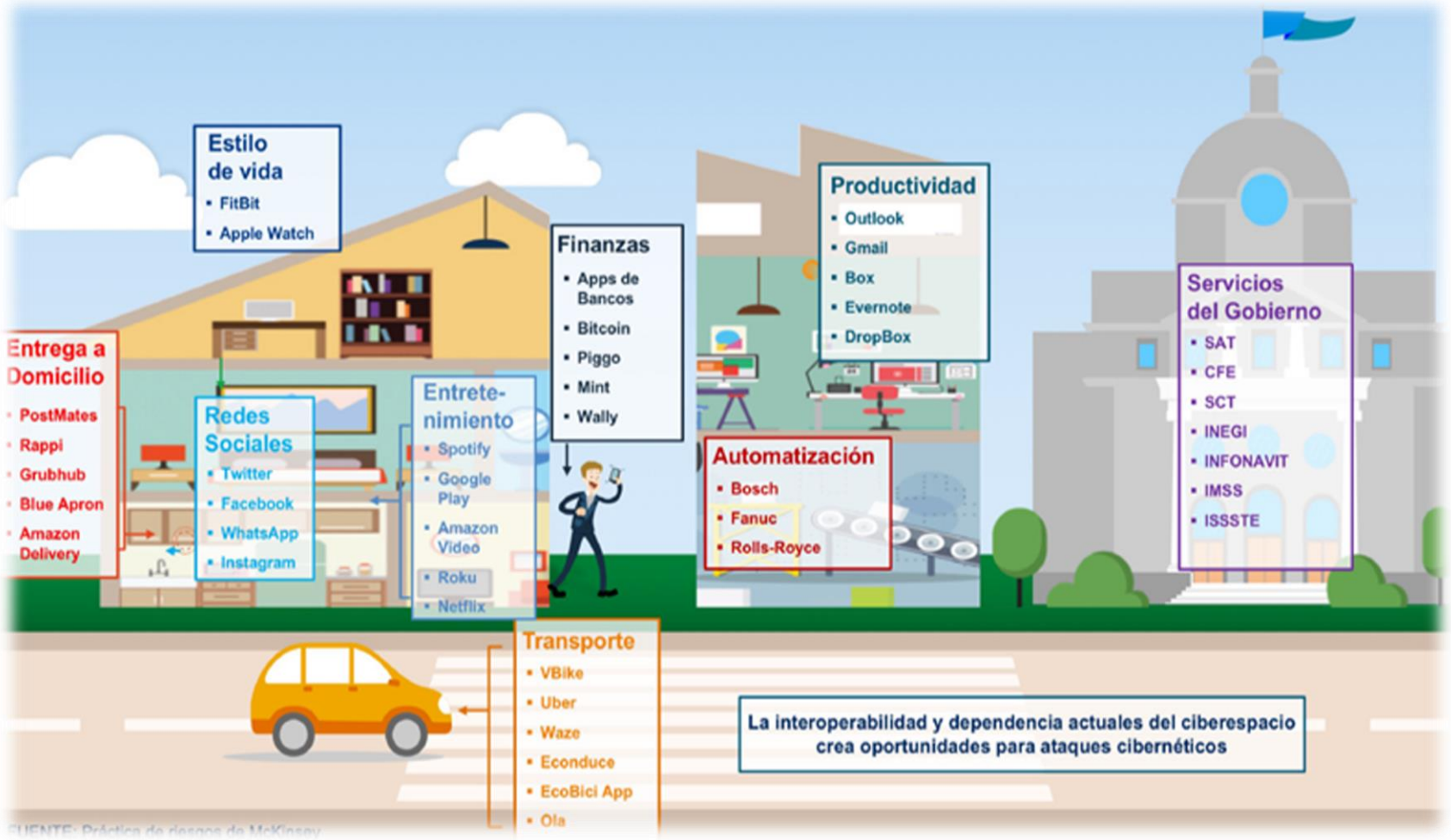
¿Qué involucra el Ciberespacio?



El Ciberespacio está creciendo

La cantidad de información y los dispositivos que la soportan están aumentando constantemente en cada sector de la vida cotidiana. Es el *Internet de Todo (IdT)*, lo que llamamos la inclusión de miles de millones de máquinas, comenzando con tabletas, teléfonos inteligentes, cajeros automáticos, instalaciones de seguridad, sistemas de controles, etc. Se estima que para el año 2020 habrá más de 200 mil millones de dispositivos que se integrarán a este grupo.

¿Qué involucra la Ciberseguridad?

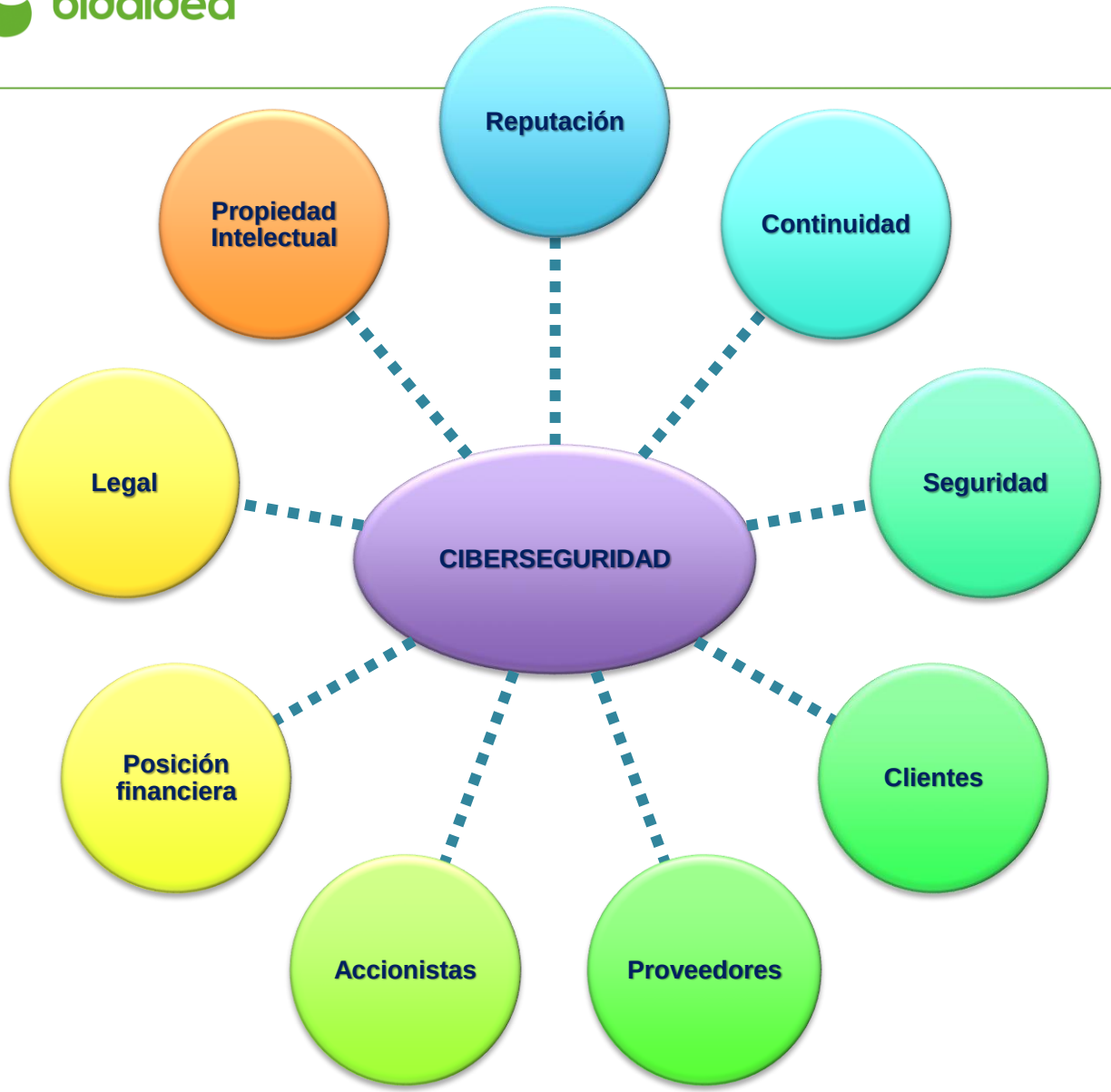


- Conexión de los PCs a internet (conexiones tipo web, FTP, SMTP)
- Conexión de la organización a Internet.
  - (conexiones tipo APIs, socket, puertos (80,8080,SSH,Telnet)
- Terminales Móviles con conexión (Webs, APP, RRSS) ¿Hay que protegerlos? ¿Como?
- Información en Internet

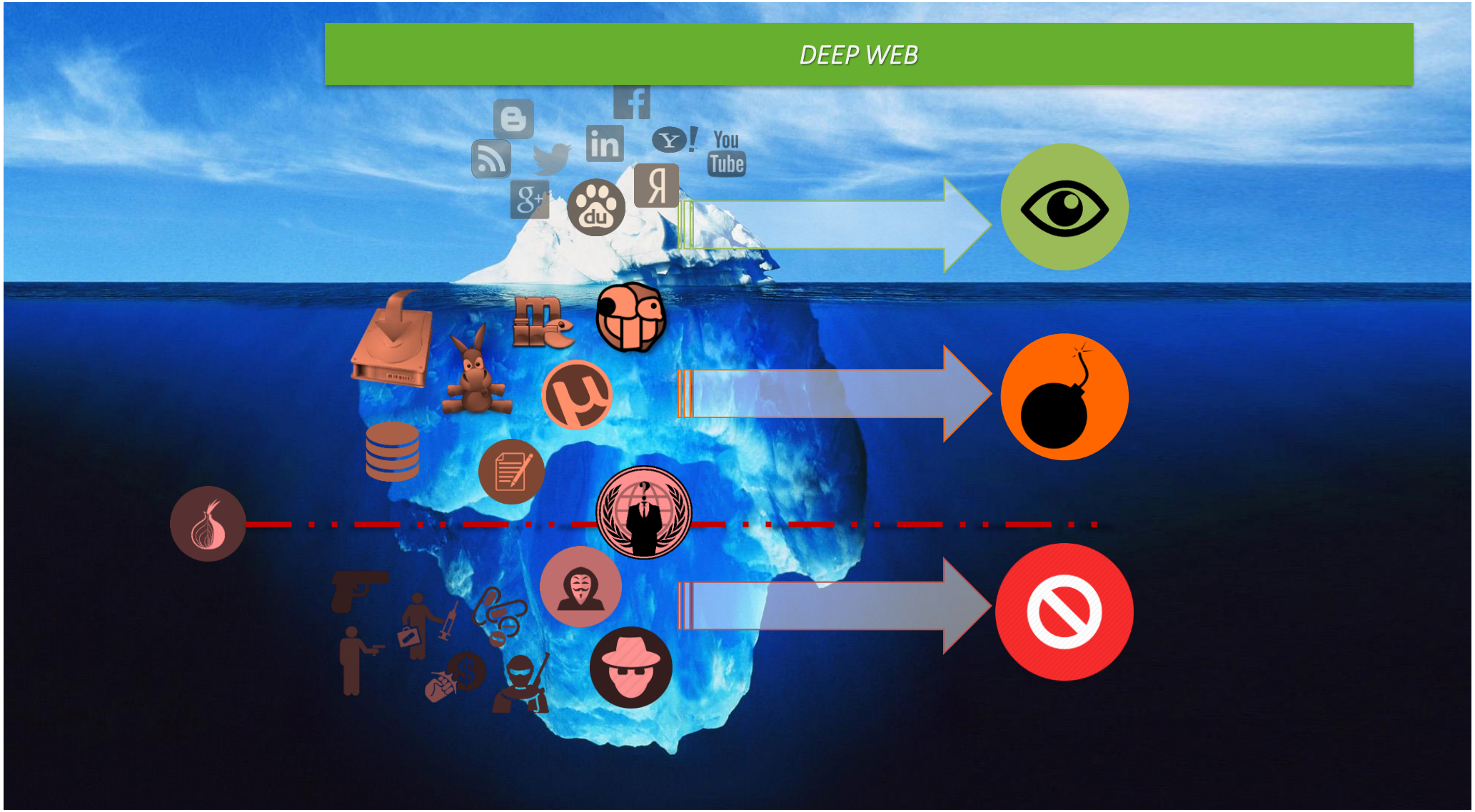
UIT-T X.1205 - Directrices para la ciberseguridad

La Ciberseguridad es el conjunto de

- herramientas
- políticas
- conceptos de seguridad
- salvaguardas de seguridad
- directrices
- enfoques de gestión de riesgos
- acciones
- capacitación
- mejores prácticas
- garantía
- tecnologías que pueden utilizarse para proteger el medio ambiente, las organizaciones cibernéticas y los activos del usuario



RIESGOS DE CIBERSEGURIDAD Y SU IMPACTO


DEEP WEB
You
Tube

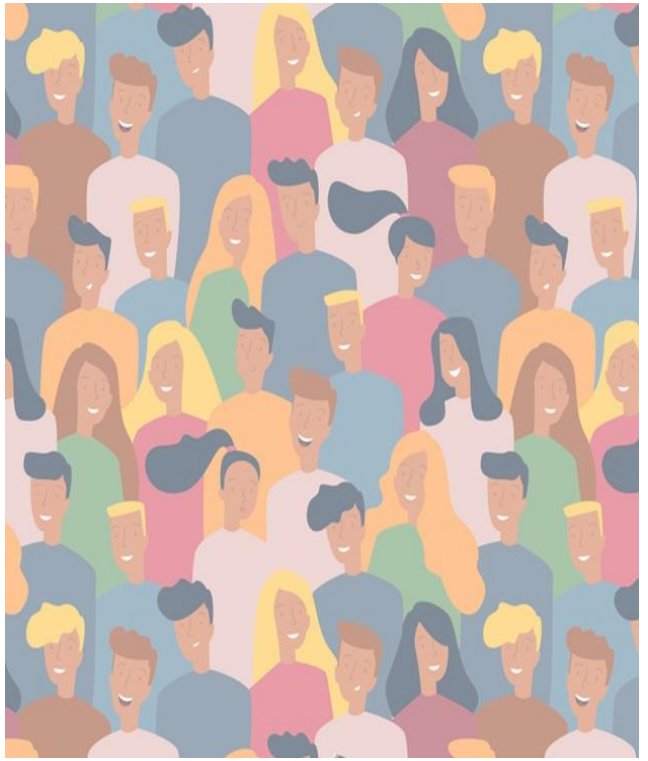
Origen de la Amenaza	Motivación
Estados	• Mejora de su posición Geopolítica o Estratégica. • Ciberterrorismo como falsa bandera. • Contraterrorismo o protección de la seguridad nacional.
Ciberdelincuentes	• Beneficio económico (Directo o indirecto)
Hacktivistas	• Acercarse a sus objetivos ideológicos.
Grupos Yihadistas	• Lograr la penetración de su ideología.
Grupos Terroristas	• Lograr cambios en la sociedad, mediante el uso del terror o influir en la toma de decisiones políticas. Objetivos de alto impacto.
Cibervándalos	• Picardía, Búsqueda de desafíos.
Actores internos	• Venganza o beneficios económicos o ideológicos (En ocasiones dirigida desde el exterior)
Ciberinvestigadores	• Revelación de debilidades y su propio perfil.
Organizaciones privadas	• Obtener y vender información valiosa.

TODOS SOMOS OBJETIVO

SECTOR PÚBLICO

SECTOR PRIVADO

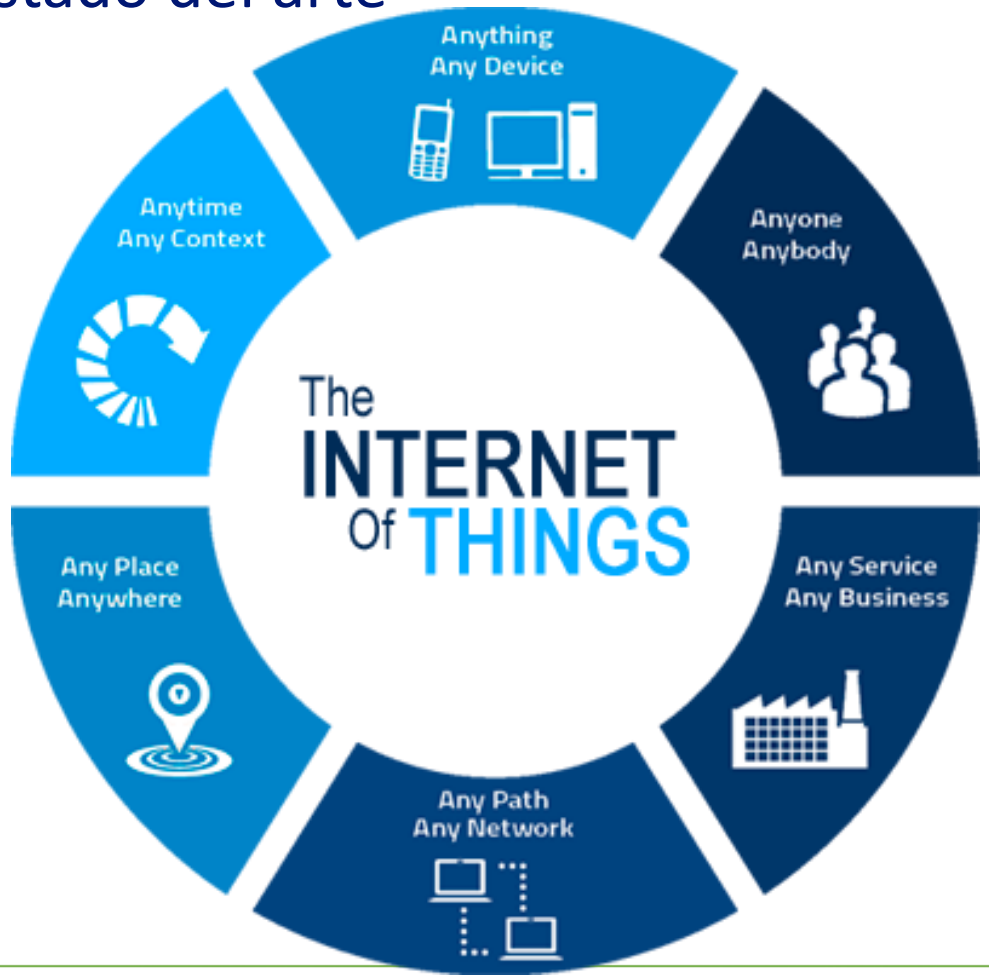
CIUDADANOS



Ciberseguridad

Estado del arte

IoT ayudará y afectará a todos



https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Todas las CIBERAMENAZAS no son iguales

	Amenazas molestas	Espionaje Económico	Crimen Organizado	Hacktivistas
Objetivo	Puntos de acceso	Ventaja Económica	Anímo de lucro	Difamación Prensa & Política
Ejemplo	Botnets & Spam	Advanced Persistent Threat (APT)	Robo de tarjetas de crédito	Anonymous & Lulzsec
Dirigida	✗	✓	✓	✓
Persistente	✗	✓	✓	✗

Tipo de Ataques

Distributed Denial of Service (DDoS) is an attack in which a master program sends data heavy traffic from multiple systems to few targeted servers and cripples them, usually mission critical servers

A vulnerability in the system that bypasses normal security authentications to enter a system

Malicious software that is used to disrupt operations, gather or modify sensitive information

DDoS

Backdoor

Malware

Man in the middle

Ransomware

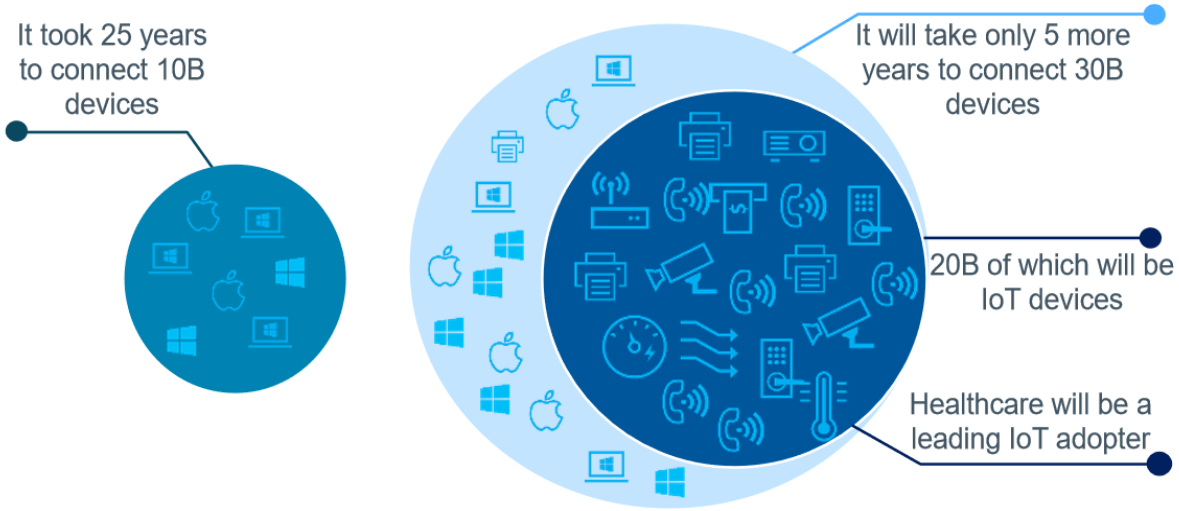
Software vulnerability

Attacker secretly relays/ alters the communication between two systems

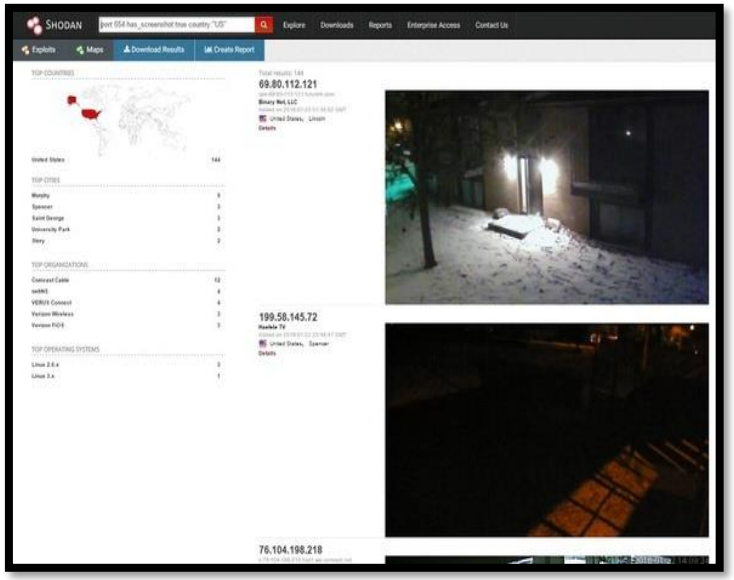
Some systems run on outdated or unsupported software that have vulnerabilities that are hard to patch

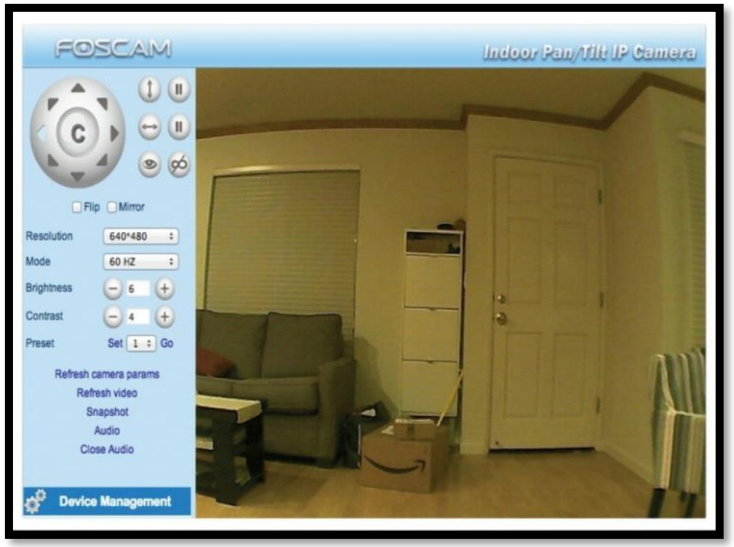
A type of malicious software designed to block access to a computer system until a sum of money is paid

Crecimiento Exponencial del IoT



Diversidad de Dispositivos IoT





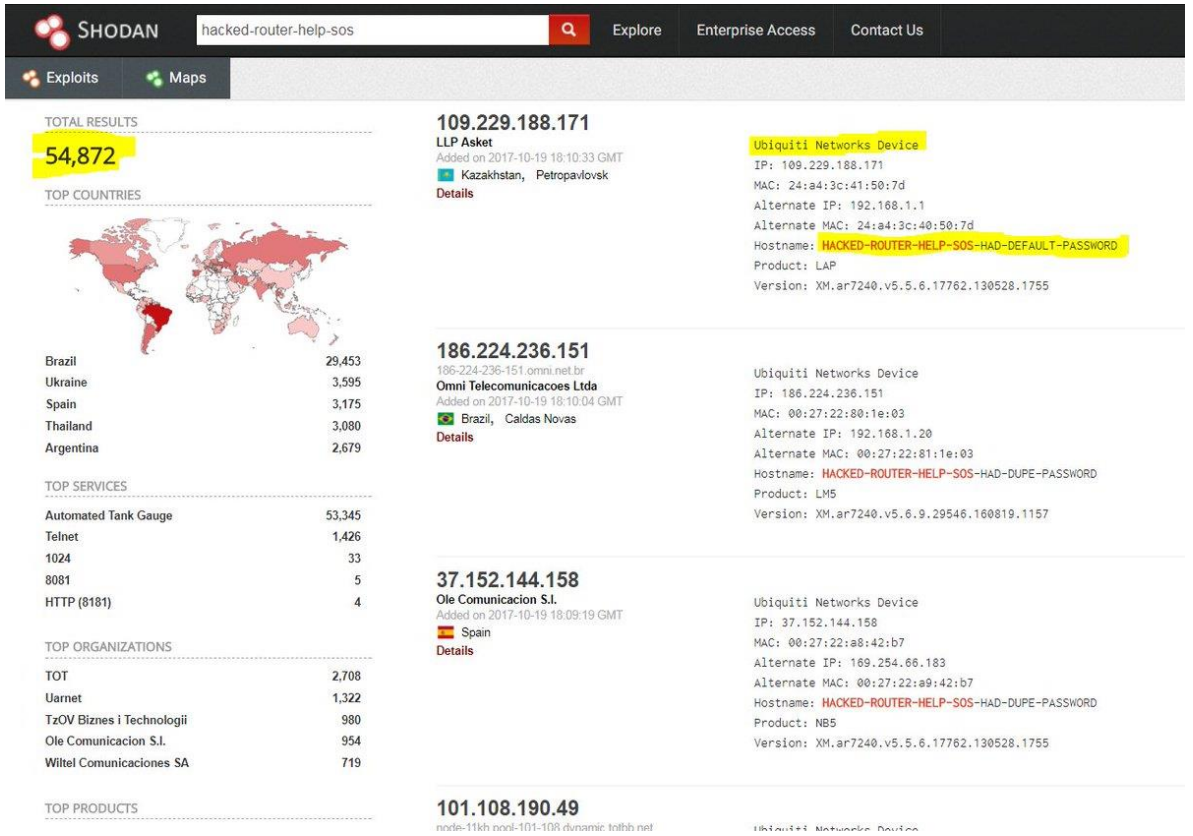
Qué es Shodan: Motor de Búsqueda IoT

Shodan es un motor de búsqueda en el que, a diferencia de Google y otros buscadores, no podemos buscar, por ejemplo, una imagen o un texto.

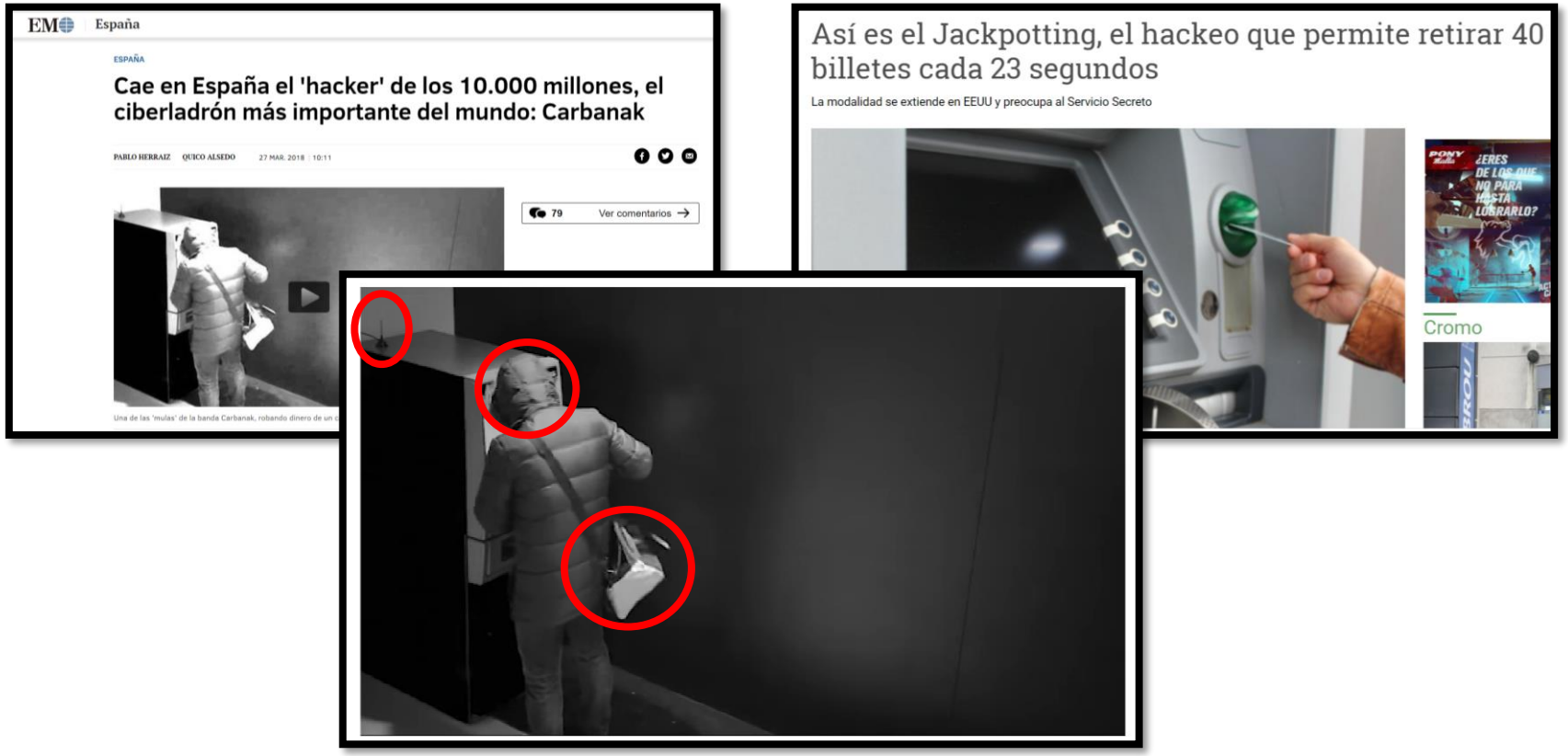
Este motor de búsqueda está enfocado únicamente a buscar sistemas y servicios conectados a internet .

Por este motivo, **Shodan** está clasificado como uno de los motores de búsquedas más peligrosos, por todo el contenido que tiene.

Podemos hacer todo tipo de búsquedas dentro de su ámbito, incluso podemos utilizar los dorks que incluye este motor de búsquedas, como por ejemplo el dork country:es , que nos permite buscar por países, en este caso España.



Algunos Ejemplos



https://www.youtube.com/watch?v=083s802WMw0

El reto: la incorporación constante de nueva tecnología en las organizaciones

DISASTROUS
Cause irreversible damage

DISRUPTIVE
Disrupt corporate and operational processes.

DAMAGING
Enable information stealing

Illegal remote monitorig

Tampering with temperature controls

Spying via video and microphone

Accessing classified information

Snooping on calls

Obtaining user credentials

Extracting Wi-Fi credentials to carry out further attacks

IP-Connected Security Systems

Many use proprietary radio frequency technology that lack authentication and encryption.

Disable camera to allow physical break in.

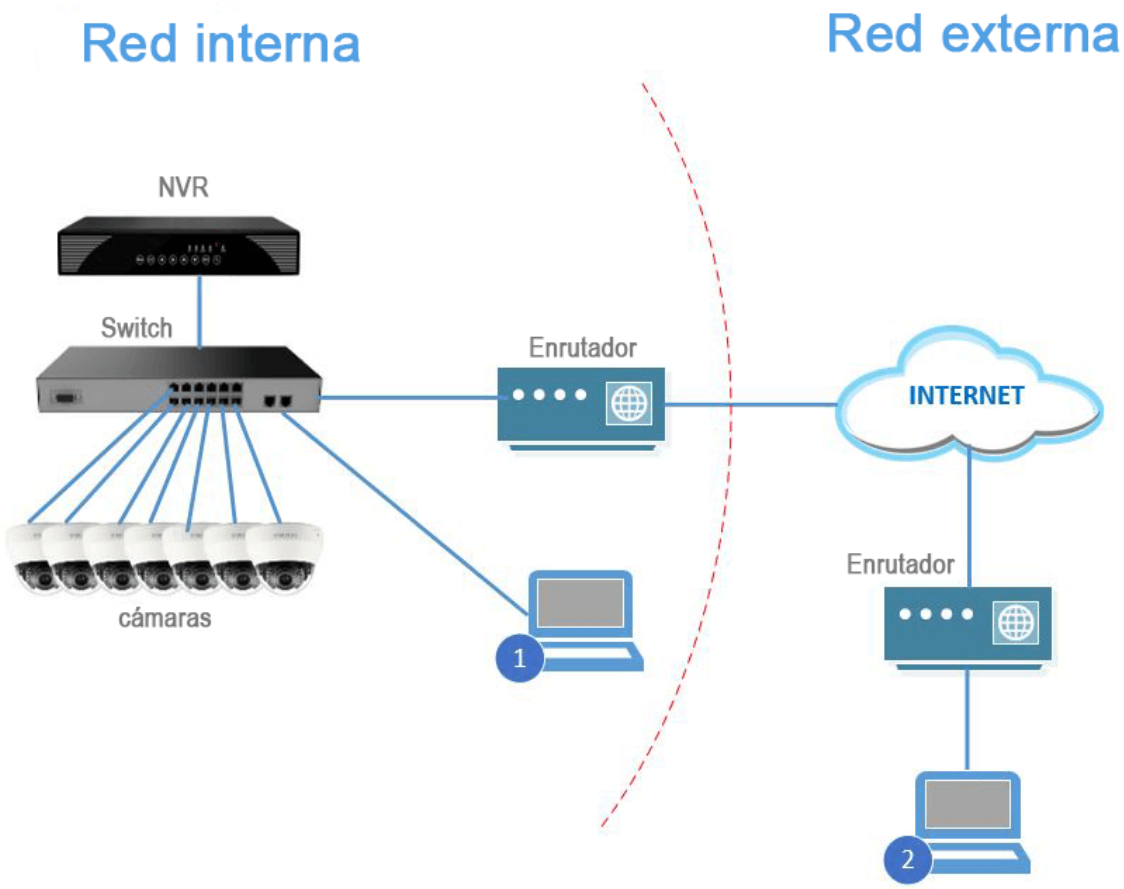
Hijack camera to spy on employees usage of computers, passwords, applications, designs.

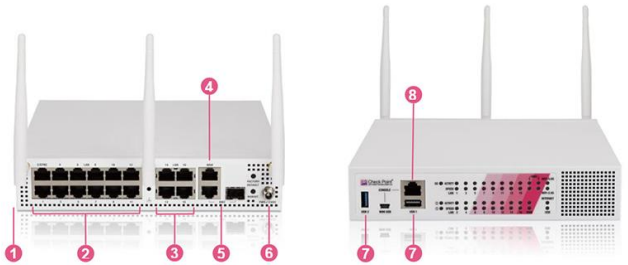
Attackers can form radio signals to send false triggers and access system controls.

Use as launching point for DDoS attacks.

User compute capability to ex-filtrate large amounts of datas.

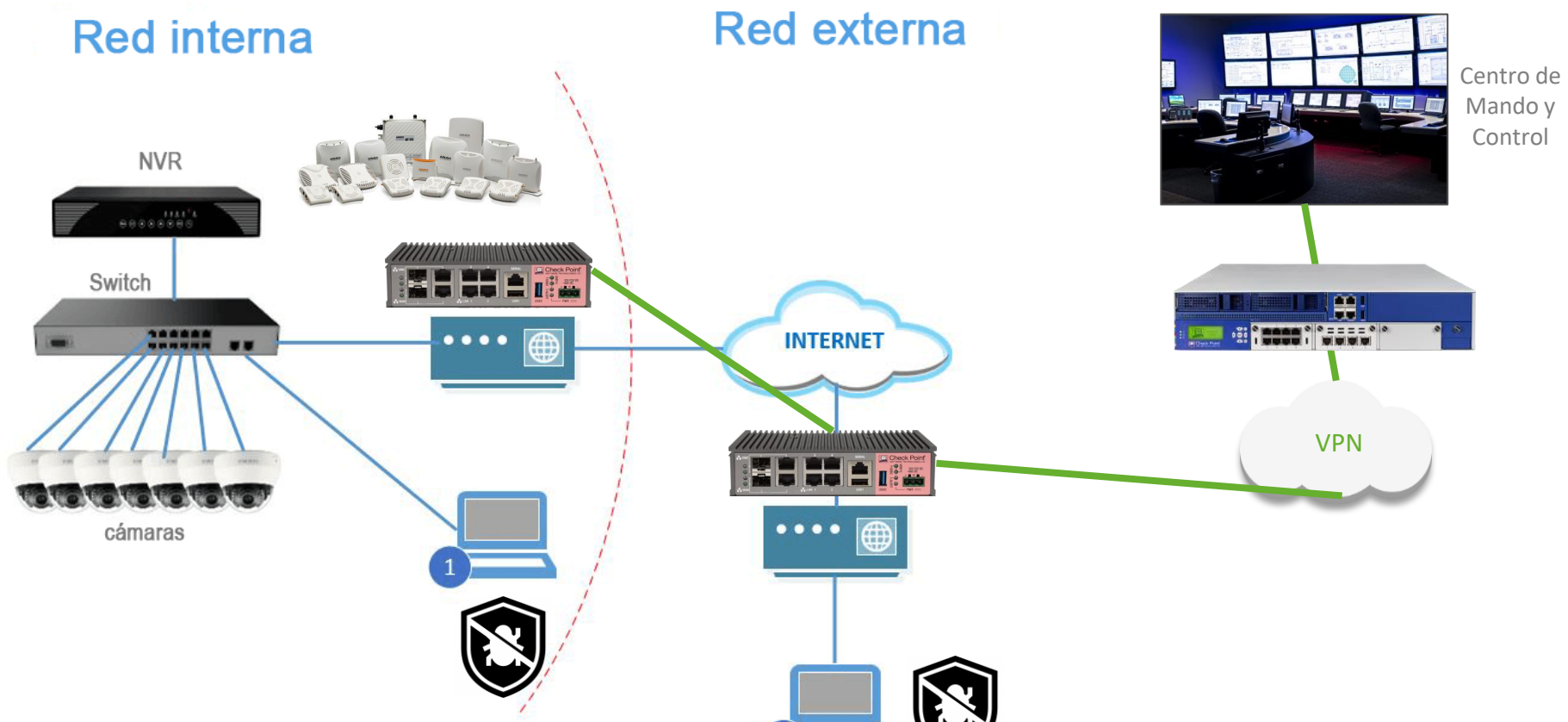
La Solución: Seguridad Integral


Red interna
Red externa
NVR
Switch
Enrutador
INTERNET
Enrutador
cámaras
1
2



PROTECCIÓN DE RED DOMÓTICA / IoT / CCTV

Los appliances de Bidaidea aportan Ciberseguridad de nivel empresarial y doméstica en una solución completa (all-in-one), sencilla y asequible para proteger a empleados y familia, redes y datos de los cibercriminales. Un dispositivo único que ofrece **seguridad multicapa integrada**, Firewall, VPN, IPS, antivirus, anti-Bot, visibilidad y control de aplicaciones, filtrado URL y seguridad de correo electrónico, todo ello en un formato desktop ligero y compacto. Bidaidea ofrece el mismo paquete de seguridad líder que el utilizado para las compañías Fortune 100 / IBEX 35.


Red interna
Red externa
NVR
Switch
cámaras
INTERNET
VPN
Centro de Mando y Control
1
2

OT / IoT

IT

Bidaidea Integral Security Center.

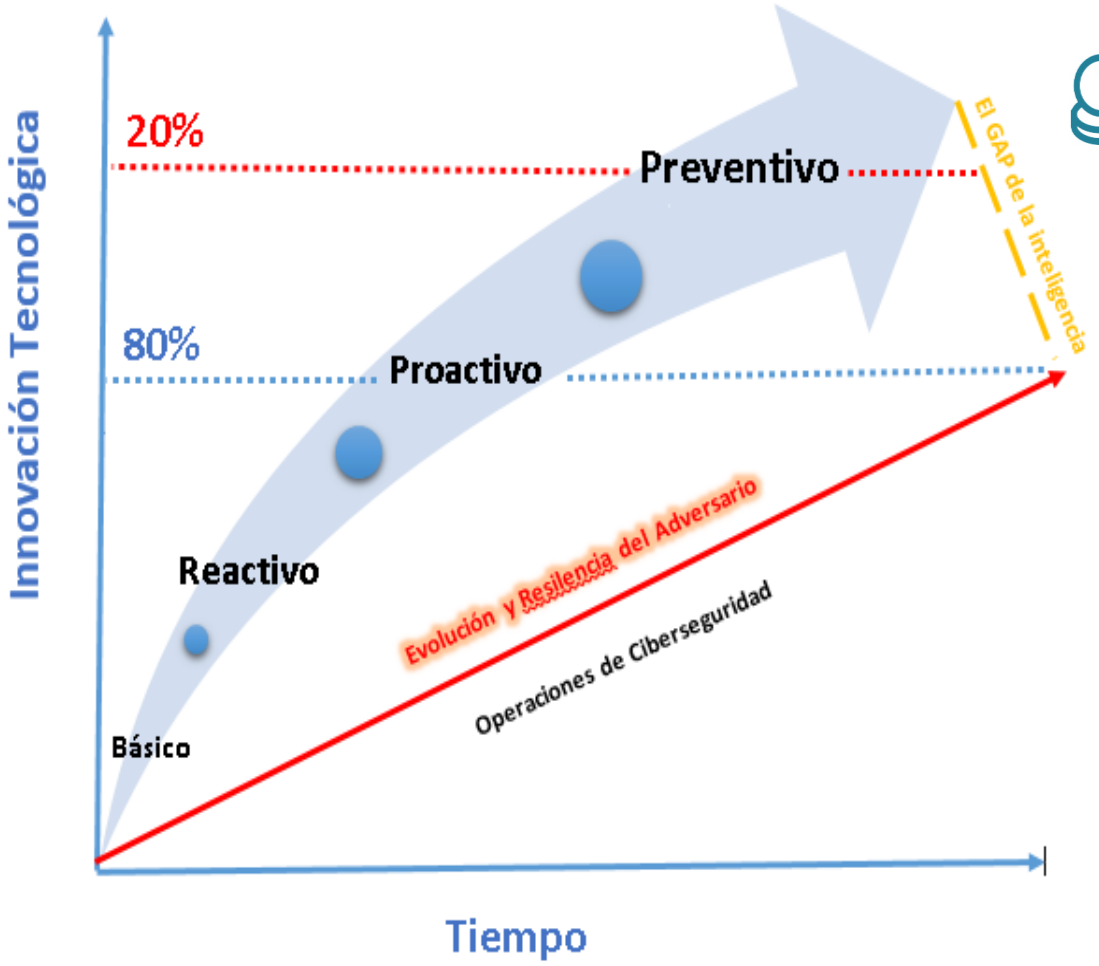
Proveedor Unificado de Seguridad.

Aumente su seguridad integral y eficiencia a través de la administración y monitorización unificada de todas sus operaciones de seguridad.

Mejor toma de decisiones.
Visión 360º, Administración integral de amenazas y riesgos

24x7

NUEVO MODELO DE CIBERSEGURIDAD



FUTURO	TRADICIONAL
Capacidad de Respuesta en tiempo real	Reacción
Evitar daños -> **Prevenir**	Minimizar daños
	Retomar control
PREVENTIVO	**REACTIVO**
FOCO EN LOS NUEVOS CANALES	OBSOLETO
ANTICIPACIÓN	COSTOSO E INEFICIENTE
REDUCCIÓN DE INCERTIDUMBRE	SIEMPRE POR DETRÁS
RESILENCIA	SIN CONTEXTO
SUPERANDO LÍMITES	FRACASO
INTELIGENCIA DE CONTEXTO	LIMITADO
Percepción global	Percepción parcial

Conclusiones

Conclusiones

Seguridad integral, ese desafío “Unificación”

- La mayoría de las empresas utilizan diferentes proveedores de seguridad y diferentes tecnologías de seguridad en su entorno.

Ataques Híbridos “Enemigo invisible”

- Combinan medios convencionales y no convencionales, ya sea por parte de países o actores no estatales para obtener objetivos específicos y están por debajo del nivel para declararse como guerra.

Creciente amenaza “Ciberinteligencia”

- La ingente cantidad de nuevas amenazas a todos los dispositivos electrónicos que usamos a diario ha hecho que los fabricantes de hardware hayan descuidado la seguridad del **Internet de las Cosas** (por sus siglas en inglés IoT).

La Seguridad es una inversión, no un gasto…

> La Ciberseguridad no es un estado, es un proceso continuo que involucra a toda la organización.

Mikel Rufián Albarrán

Managing Director – Head of Global Cybersecurity, Intelligence & Industry Lab

Mikel.rufian@bidaidea.com

Telf: (+34) 670 025 091

@mrufian

es.linkedin.com/in/mikelrufian

www.mikelrufian.com

Consultoria y Auditoria Tecnica

Gobierno, Riesgo y Cumplimiento

Productos Especializados

Alianzas estratégicas con los mejores fabricantes

Centro de Servicios 24x7 (iSOC)

Soluciones especializadas en Ciberseguridad & Inteligencia

Outsourcing

Externalización de personal especialista

Formación y Concienciación

Campus Bidaidea

I+D+i

Investigación, desarrollo e innovación

www.Ciberseguridadbidaidea.com

bidaidea

CYBERSECURITY &
INTELLIGENCE

BASQUE CYBERSECURITY CENTRE

EMPRESA REGISTRADA incibe

España – EEUU - Brasil – Colombia – México – Perú - Portugal