PROGRAMA DE FORMACIÓN

Transformación digital e Industria 4.0

Fondo Social Europeo
Una manera de hacer Europa

EXTREMADURA EMPRESARIAL

Unión Europea

JUNTA DE EXTREMADURA

Taller 3.
Conectividad

Índice

Introducción del Programa Formativo

Objetivos, beneficiarios y Competencias asociadas

Contextualización de la Conectividad en la Industria 4.0

Temáticas específicas, Demostraciones, Actividades prácticas y Bibliografía:

- **Seguridad de la Información**
- **Ciberseguridad y Cloud**
- **Protección de Datos**
- **Seguridad de las Infraestructuras tecnológicas**
- **Internet de las cosas**

Introducción al Programa formativo

- Es un Programa formativo que pone en marcha la **Dirección General de Empresa y Competitividad de Consejería de Economía, Ciencia y Agenda Digital de la Junta Extremadura,** con el fin de fortalecer las competencias, habilidades y conocimientos de empresarios, directivos y mandos intermedios de empresas, para promover su crecimiento profesional y la adaptación a la industria conectada de sus organizaciones

- El programa está cofinanciado por el **Fondo Social Europeo (80%)** y la **Comunidad Autónoma de Extremadura (20%),** al estar enmarcado dentro de las actuaciones del **Programa Operativo FSE 2014-2020**

Introducción al Programa formativo

TALLER 1: AUTOMATIZACIÓN DE LA INDUSTRIA.

Sensorización, Monitorización, Sisitemas Ciberfisicos, Robotica, Fab. Aditiva, Impresión 3D…

Fechas: 21, 22, 23, 24 y 28 de octubre. Horario de 16 a 20h.

TALLER 2: DATOS DIGITALES.

Big Data. Analítica y Métricas de Infomación digital, Inteligencia Artificial…

Fechas: Del 29, 30 de octubre, 4, 5 y 6 de noviembre. Horario de 16 a 20h.

TALLER 3: CONECTIVIDAD.

Internet de las cosas, Cloud, Ciberseguridad, Infraestructuras tecnológicas, Protección de Datos…

Fechas: Del 11, 12, 13, 14 y 18 de noviembre. Horario de 16 a 20h.

TALLER 4: APLICACIONES Y SOLUCIONES DE CLIENTE.

Realidad virtual y aumentada, Wearables, Apps, Redes sociales y Softwares (ERP, CRM , MES…)

Fechas: Del 20, 21, 25, 26, y 27 de noviembre. Horario de 16 a 20h.

Introducción al Programa formativo

TALLER 3: CONECTIVIDAD: Contenidos por Jornada

11 de noviembre: Conceptos teóricos
Carlos G. Rodríguez: "Contextualización de la Conectividad en Industria 4.0"
David Romero: Seguridad de la Información

12 y 13 de noviembre: Conceptos teóricos
David Romero: Proteccion de Infraestructuras

14 de noviembre: Conceptos teóricos
Eleazar García – Protección de Datos

18 de noviembre: Conceptos teóricos
David Romero: Internet de las Cosas

Introducción al Programa formativo

A partir del minuto 1:30, hasta el minuto 2:20

https://www.youtube.com/watch?time_continue=220&v=9QEtcvVP4Mw&feature=emb_logo

Objetivos, Beneficiarios y Competencias asociadas

Objetivo General

- Presentar, de forma dinámica, los diferentes modelos de estrategia para la gestión de la empresa conectada y las tecnologías habilitadoras que intervienen en la industria 4.0 para poder incrementar el valor añadido industrial y el empleo cualificado del tejido empresarial de la región

¿Á quién va dirigido el programa?

- Empresarios, directivos, mandos intermedios y técnicos especialistas de todas las empresas extremeñas, especialmente las que desarrollen su actividad, directa o indirectamente, en el sector industrial
- Profesionales del ámbito de la consultoría que integren entre sus áreas de trabajo promover el desarrollo de la industria 4.0

Objetivos, Beneficiarios y Competencias asociadas

ESTE TALLER

TALLER 3: CONECTIVIDAD.

Contenidos: Tomaremos conciencia de la importancia de ciberseguridad y aprenderemos los conceptos básicos para la correcta gestión de protección de los datos. Conoceremos las posibilidades del Cloud computing, del Edge computing y el Almacenamiento de datos en la nube o en sistemas híbridos físico virtuales. Conoceremos las posibilidades del Internet de las Cosas (IoT) en sus aplicaciones a entornos empresariales e industriales.

Objetivos, Beneficiarios y Competencias asociadas

- Dominar el ecosistema del "**Cloud**" para la gestión empresarial, industrial y productiva, así como conocer las diferentes opciones y herramientas **del Almacenamiento de Datos en la nube,** y las consideraciones a tener en cuenta en su implantación

- Entender el concepto de **Ciberseguridad,** las claves esenciales para la seguridad de los datos en la empresa, y ver ejemplos prácticos. Igualmente entender la nueva Ley de **Protección de Datos**, y los condicionamientos a tener en cuenta en la gestión empresarial

- Conocer las **infraestructuras tecnológicas y digitales de las industrias**

- Introducirnos en el **Internet de las Cosas,** y las posibilidades que ofrece para los procesos industriales

Contextualización de la Conectividad en la Industria 4.0

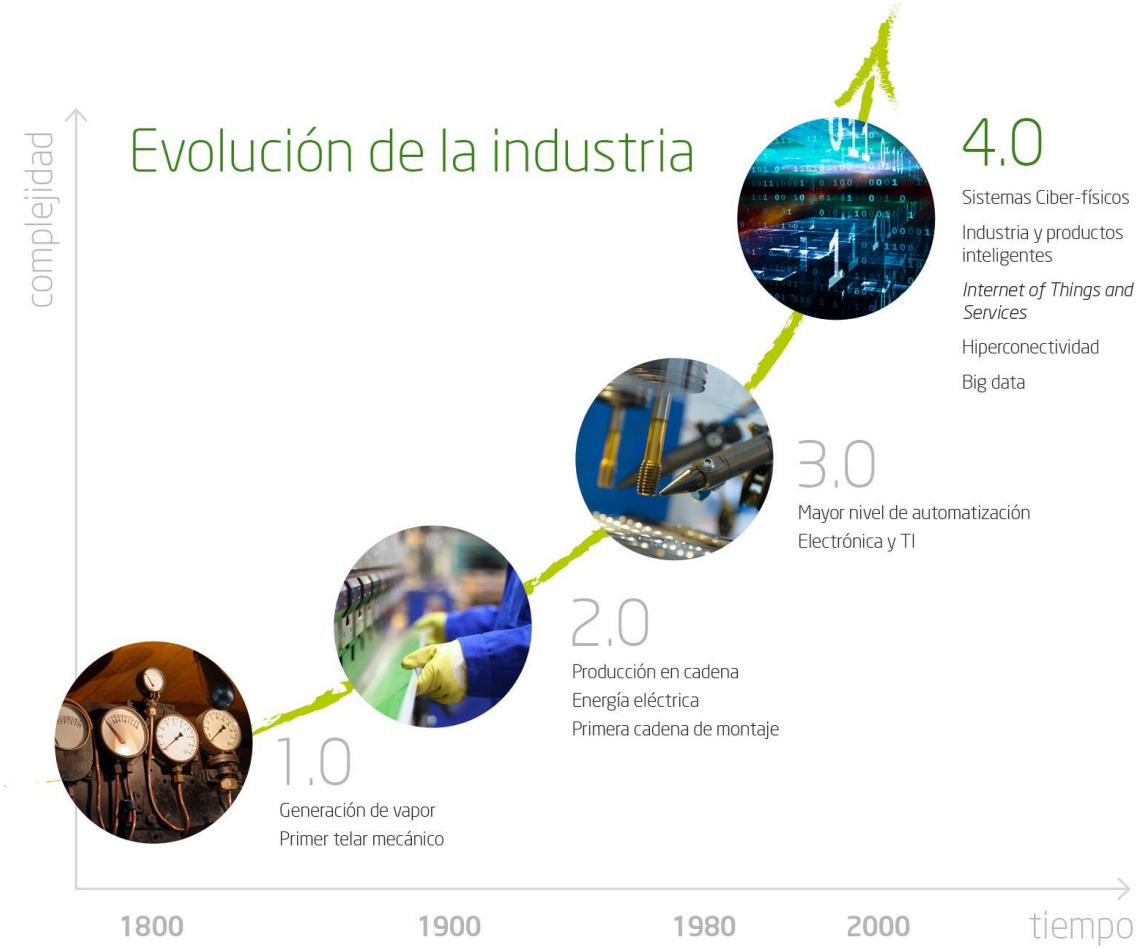
El concepto de **Industria 4.0** (también llamada industria inteligente o Ciberindustria del futuro) es relativamente reciente y se refiere a la **cuarta revolución industrial**, que consiste en la **introducción de las tecnologías digitales en la industria.**

Contextualización del taller

INTRODUCCIÓN

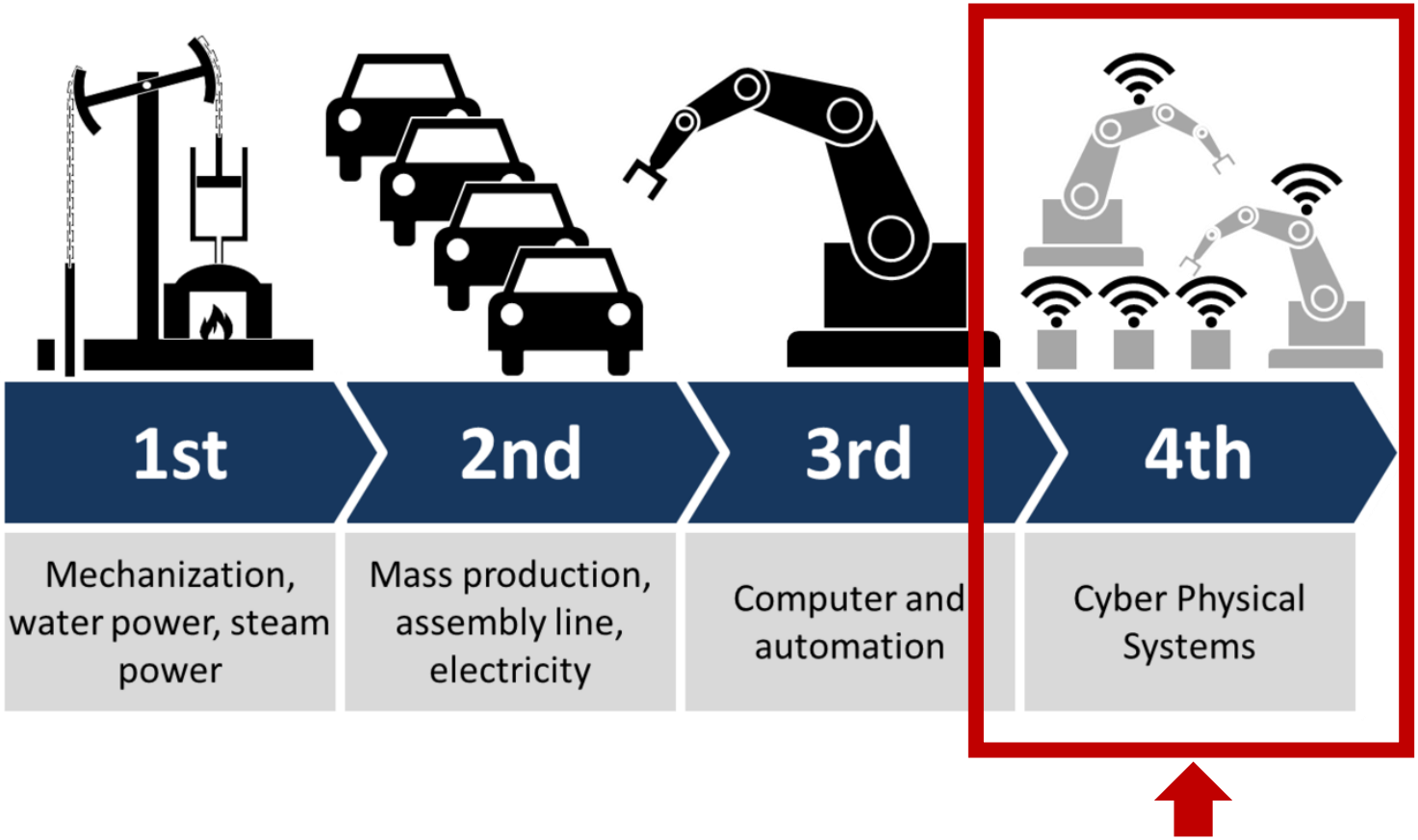
https://www.youtube.com/watch?v=IINsx1xsk2w&feature=emb_logo

Contextualización de la Conectividad en la Industria 4.0



Fuente: Elaboración propia en base a Zukunftsprojekt Industrie 4.0

Contextualización de la Conectividad en la Industria 4.0



Se multiplican la conectividad de todos los sistemas

Contextualización de la Conectividad en la Industria 4.0

Es una nueva manera de organizar los medios de producción que pretende alcanzarse el concepto de **"fábricas y empresas inteligentes" (smart factories),** con una mayor adaptabilidad a necesidades, procesos y una asignación más eficiente de los recursos, utilizando la **CONECTIVIDAD**

Contextualización de la Conectividad en la Industria 4.0

Fábrica inteligente: Caso de éxito

https://www.youtube.com/watch?v=GU4qux9zIeI&list=PLIaCHO19tFYbRYTItST_Fv7EpVEVQnYXU&index=4

Contextualización de la Conectividad en la Industria 4.0

Marco conceptual de la industria 4.0

Dimensiones claves de la empresa
(Núcleo central del esquema)

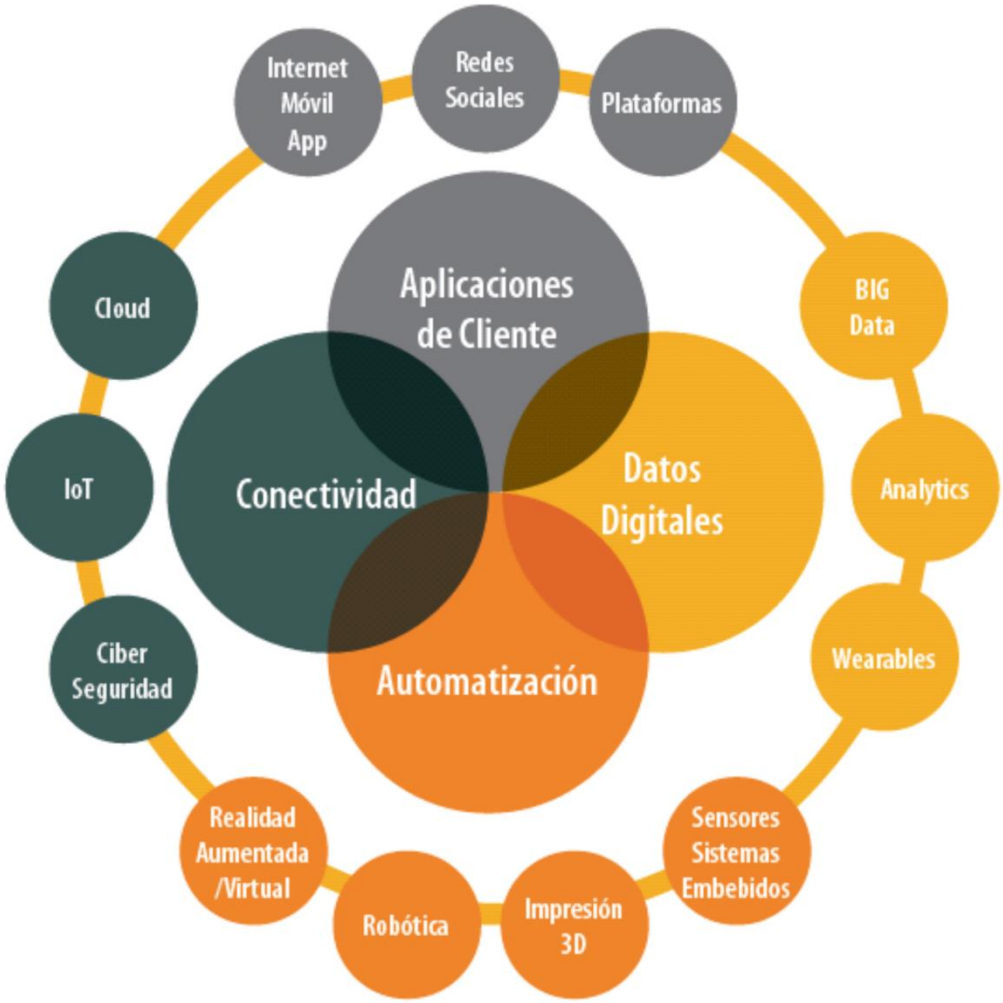
Palancas de impulso hacia la transformación digital y la industria 4.0
(Círculo externo del esquema)

Contextualización de la Conectividad en la Industria 4.0

Habilitadores digitales y tecnológicos de la industria 4.0:

Áreas tecnológicas claves en la empresa
(Núcleo central del esquema)

Habilitadores digitales de la industria 4.0
(Círculo externo del esquema)



Contextualización de la Conectividad en la Industria 4.0

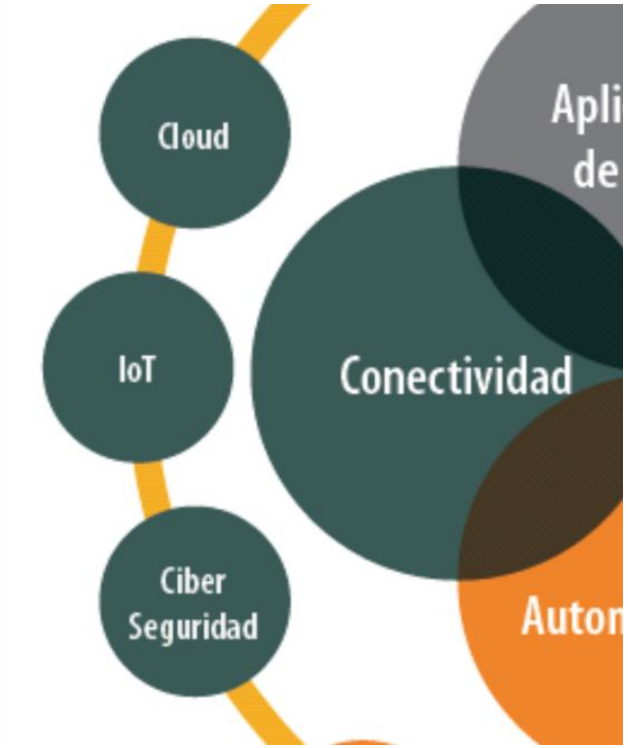
Habitadores y Tecnologías relacionados con la Conectividad

CLOUD

IoT

CIBERSEGURIDAD

Pero también tienen mucha importancia los **Sensores**, los **Productos interconectados**, las **Redes Sociales**, **Internet**, y las **Infraestructuras**



Contextualización de la Fábrica Inteligente

Ver: https://www.youtube.com/watch?time_continue=3&v=wVD39XT7Q-E&feature=emb_logo

Temáticas específicas, Demostraciones, Actividades prácticas y Bibliografía

Seguridad de la Información

David Romero Trejo

Protección de Infraestructuras

David Romero Trejo

Protección de Datos

Eleazar García

IoT

David Romero Trejo

Bibliografía. Documentos y Enlaces de interés:

- *Estrategia Nacional Industa 4.0 – Gobierno de España*
- *Estrategias regionales para el fomento de la Industria 4.0 en España*
- *Herramienta de Autodiagnóstico Digital Avanzado HADA*
- *Programa Activa Industria 4.0 - Convocatoria 2019*
- *Ayudas y Financiación nacional a la Iniciativa industria conectada 4.0*
- *Informe Nacional "La transformación digital de la industria española"*
- *Agenda para el Fortalecimiento del Sector Industrial en España*
- *Congreso Nacional de Industria Conectada 4.0 – CIC40*
- *Premios Nacionales Industria Conectada 4.0*
- *Portal de Recursos de Industria 4.0 – Junta de Extremadura*
- *Subvenciones para la transformación y adaptación a la industria 4.0 de la línea Incentivos Regionales de Extremadura*
- *Convocatoria "Ayudas a Empresas Industriales de Extremadura" – Activa industria 2019*
- *Programa Activa Industria 4.0 - Convocatoria 2019 - Extremadura*
- *Plan Coordinado Europeo sobre la Inteligencia Artificial*

Bibliografía. Documentos y Enlaces de interés:

- *Estrategia Nacional y Mapa de capacidades de tecnologías de Inteligencia Artificial*
- *Estandarización para la Industria 4.0 - Informes de Normalización*
- *Espec. UNE 0060: 2018 Industria 4.0. Sistema de gestión para la digitalización. Requisitos*
- *Espec. UNE 0061:2019 Industria 4.0. Sistema de gestión para la digitalización. Criterios*
- *Industria 4.0 – Wikipedia*
- *Transformación Digital – Wikipedia*
- *Blog CIC40 – Industria Conectada 4.0*
- *La Digitalización y la Industria 4.0 – CC.OO.*
- *Industria 4.0: 26 buenas prácticas en grandes empresas nacionales e internacionales*
- *Informe "Industria 4.0" – PWC*
- *"The Industry 4.0 paradox: Overcoming disconnects on the path to digital transformation" – Deloitte*
- *Estudio Smart Industry - Everis*
- *Manufacturers focused on operating efficiency are missing the point of i4.0 entirely: KPMG*

Bibliografía. Vídeos y Listas de reproducción de interés:

Lista de reproducción de Contenidos formativos Industria Conectada 4.0

1. *Industria Conectada 4.0. La industria del futuro ha llegado.*
2. *Retos y oportunidades de la cuarta revolución industrial*
3. *Procesos, productos y modelos de negocio. Triple impacto de la Industria 4.0*
4. *La fábrica inteligente*
5. *La importancia de los habilitadores digitales en la cadena de valor de la Industria*
6. La gestión del proceso productivo en la Industria 4.0
7. Innovación en el proceso de diseño industrial
8. Inteligencia de procesos basada en los datos
9. Fabricación flexible y a demanda
10. Logística 4.0: optimizando la cadena de suministro.
11. Los habilitadores digitales de la Industria 4.0
12. Automatización y colaboración hombre-máquina en la Industria 4.0
13. Internet de las cosas: sensores, sistemas embebidos y vestibles como fuente del dato
14. Fábrica inteligente en la nube: agilizando procesos y reduciendo costes con cloud computing

Bibliografía. Vídeos y Listas de reproducción de interés:

Lista de reproducción de Contenidos formativos Industria Conectada 4.0

15. Realidad aumentada y realidad virtual en la industria del futuro
16. Impresión 3D y la fabricación aditiva
17. Transformación digital: hacia la Industria 4.0
18. ¿Estamos preparados? Competencias profesionales para la Industria 4.0
19. Hoja de ruta para la transformación de la industria
20. Nuevos modelos de negocio de la Industria 4.0 en torno a la cadena de valor

Lista de reproducción de Casos de éxito y ejemplos empresariales de Activa industria 4.0

1. *EOI Industria 4.0 - TVITEC*
2. *EOI Industria 4.0 - KH7*
3. *EOI Industria 4.0 - ASTI*
4. *EOI Industria 4.0 - VICINAY*

Bibliografía. Vídeos y Listas de reproducción de interés:

Portales Nacionales

- Ministerio de Industria, Comercio y Turismo
- Portal Pyme
- Programas de la DGIPYME
- Escuela de Organización Industrial (EOI)
- Programa Crecimiento Empresarial
- Agrupaciones Empresariales Innovadoras (AEI)

Portales Europeos

- Estrategias Europeas
- Políticas Europeas para la Transformación Digital de la Industria

Bibliografía. Vídeos y Listas de reproducción de interés:

- https://extremaduraempresarial.juntaex.es/web/guest/actividades?idContenido=11158023&redirect=/agenda
- http://www.rtve.es/alacarta/videos/telediario/industria-40-automatizacion-digitalizacion-para-fabricas-del-futuro/4001819/
- https://es.wikipedia.org/wiki/Automatizaci%C3%B3n_industrial
- https://es.wikipedia.org/wiki/Sistema_embebido
- https://es.wikipedia.org/wiki/Sistema_ciberf%C3%ADsico
- https://es.wikipedia.org/wiki/Rob%C3%B3tica

ANEXOS

Contenidos de Experiencias, Colaboradores y Demostraciones

PROGRAMA DE FORMACIÓN

Transformación digital e Industria 4.0

Fondo Social Europeo
Una manera de hacer Europa

EXTREMADURA EMPRESARIAL

Unión Europea

JUNTA DE EXTREMADURA

Taller 3.

U1 – Seguridad de la Información

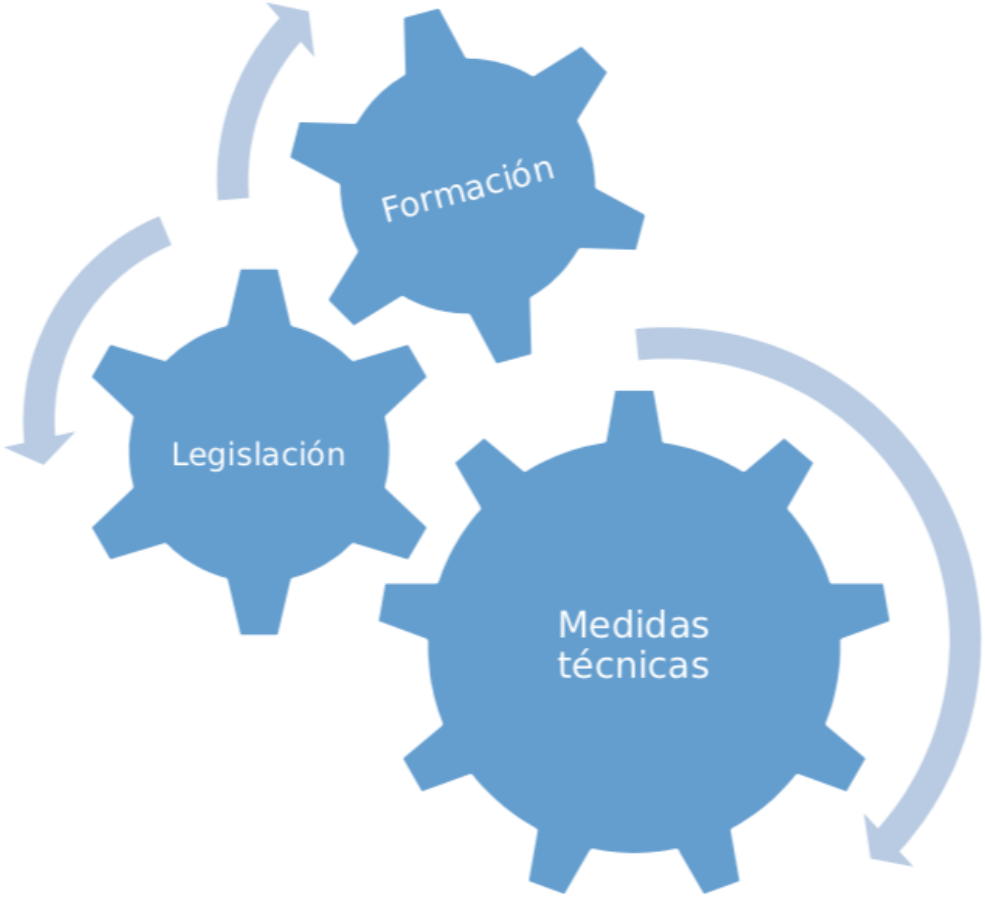
Taller 3. Conectividad

ÍNDICE

ÍNDICE

ÍNDICE

1.- INTRODUCCIÓN



1.- INTRODUCCIÓN

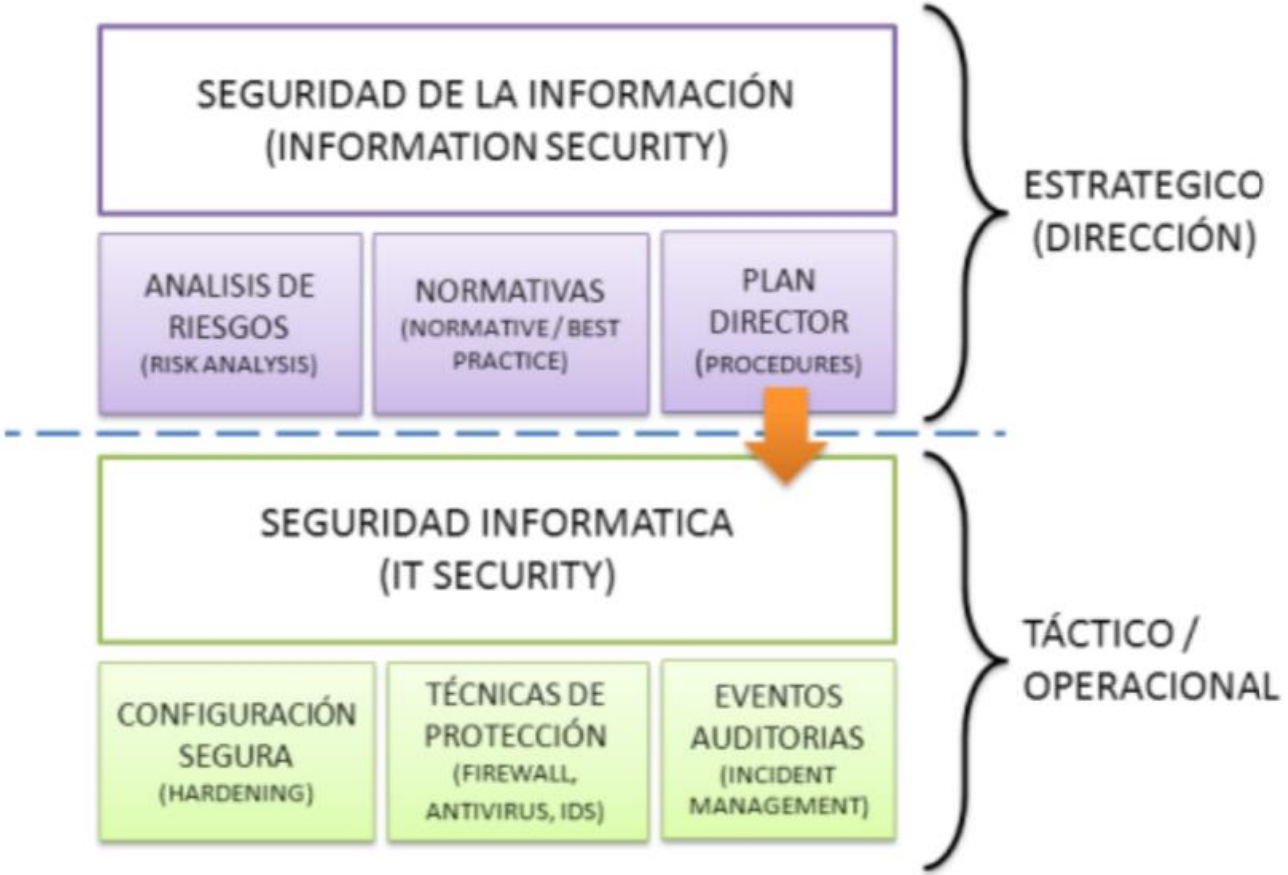
SEGURIDAD DE LA INFORMACIÓN: Se refiere a la protección de los activos de información fundamentales para el éxito de cualquier organización.

≠

SEGURIDAD INFORMÁTICA: Se refiere a la protección de las infraestructuras de las tecnologías de la información y comunicación que soportan nuestro negocio.

Taller 3. **Conectividad**

1.- INTRODUCCIÓN



Taller 3. **Conectividad**

1.- INTRODUCCIÓN

1.- INTRODUCCIÓN

NO EXISTE UN SISTEMA DE INFORMACIÓN QUE GARANTICE AL 100% LA SEGURIDAD DE LA INFORMACIÓN

1.- MITOS DE INTERNET

1. "Mi antivirus está al día, así que no puede entrar ningún virus."
2. "Mi PC no le interesa a nadie, no hay peligro."
3. “Utilizo Mac, que no tiene virus.”
4. "Tengo el cortafuegos de Windows habilitado, así que no corro peligro."
5. "Mi copia de seguridad está al día, así que si pasa algo, puedo restaurar el sistema."
6. "Nunca dejo mi correo en ningún sitio ni estoy registrado en páginas Web, así que es imposible que me roben la dirección."
7. "Después de que entró un virus, reinstalé Windows y listo."
8. "Tengo todas las actualizaciones de Windows instaladas, no puede pasar nada."
9. "No uso Outlook Express ni Internet Explorer, así que estoy a salvo."
10. "No abro ningún fichero adjunto, los virus no pueden entrar."

Taller 3. **Conectividad**

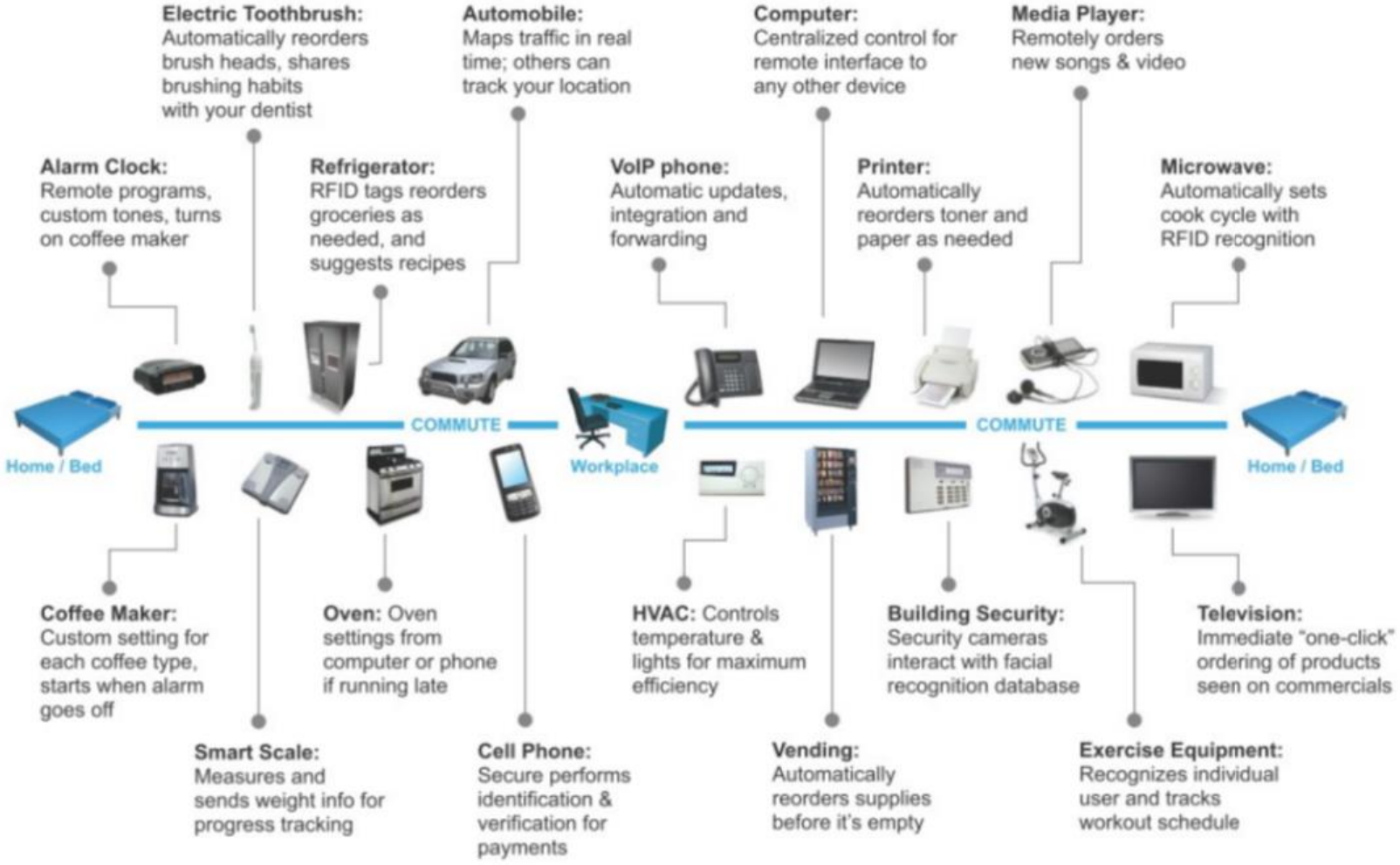
1.- REALIDADES DE INTERNET

Taller 3. **Conectividad**

1.- REALIDADES DE INTERNET

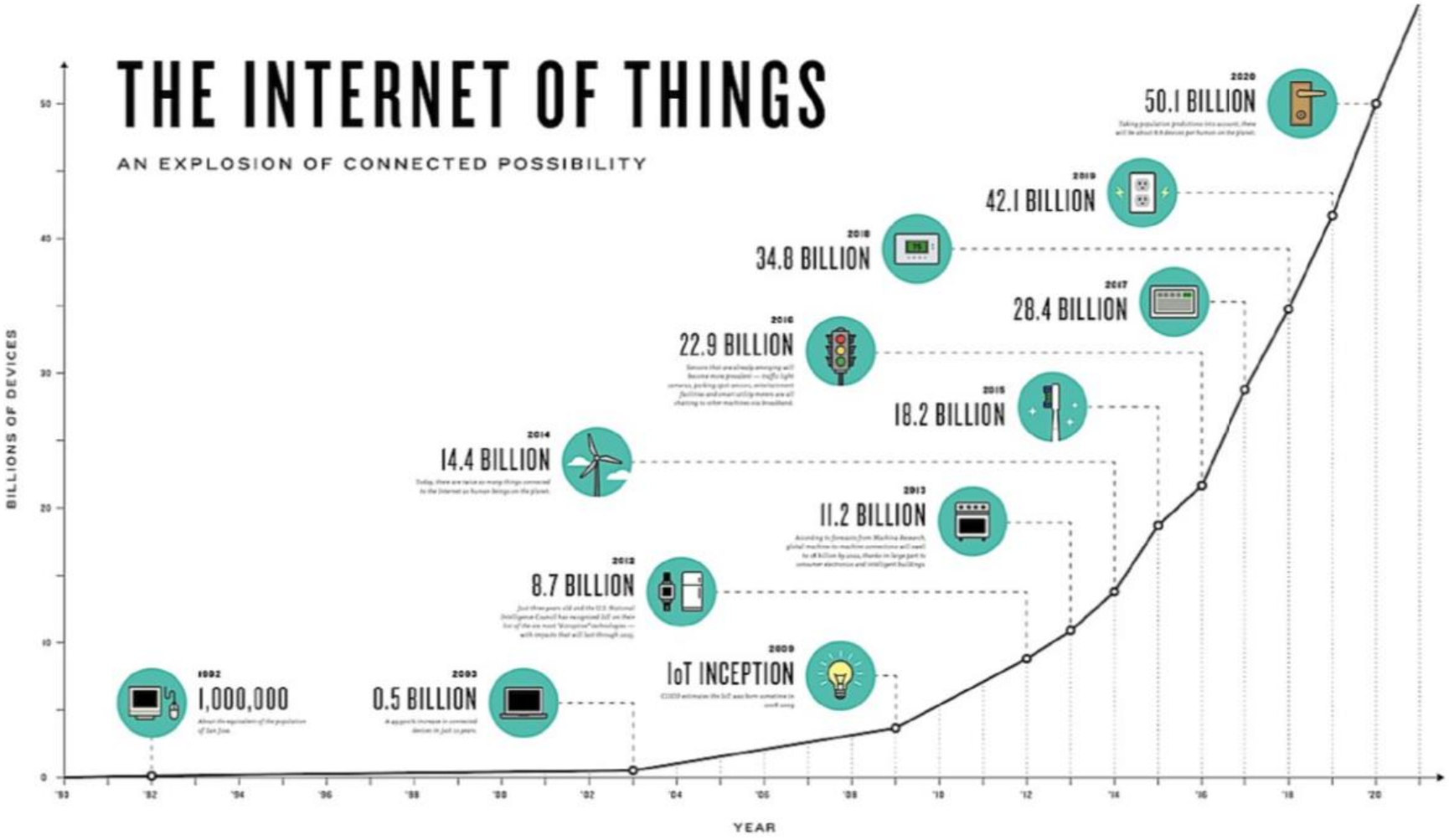
Taller 3. Conectividad

1.- REALIDADES DE INTERNET



Taller 3. **Conectividad**

1.- REALIDADES DE INTERNET



Taller 3. **Conectividad**

1.- INTRODUCCIÓN

Ciberloquesea

Ciberacoso	*Ciberactivismo*
Ciberarma	*Ciberataque*
Ciberbullying	*Cibercarterista*
Cibercrimen	*Ciberdefensa*
Ciberdelincuente	*Ciberdelito*
Ciberespacio	*Ciberespionaje*
Ciberguerra	*Ciberriesgos*
Ciberrobo	*Cibersexo*
Ciberterrorista	*Ciber...*

Una palabra Ciberdemoda

1.- INTRODUCCIÓN

Ciberpuerta de máxima seguridad y resistencia al taladro según UNE-EN 122009:2003 con sistema antirretroceso de cerrojo y bloqueo de cerradura

Taller 3. **Conectividad**

1.- INTRODUCCIÓN

La seguridad no es nada nuevo … ¿Cibercastillo?

2.- LEGISLACIÓN VIGENTE

1. **Reglamento General de Protección de Datos (RGPD)** es el reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. [Entró en vigor el 25/05/16 y fue de aplicación el 25/05/18]
2. Ley 59/2003, de 19 de diciembre, de **Firma Electrónica. [BOE 304 de 20-12-2003]**
3. Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** en el ámbito de la Administración Electrónica. [BOE 25 de 29-01-2010]
4. Real Decreto 4/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Interoperabilidad** en el ámbito de la Administración Electrónica.[BOE 25 de 29-01-2010]
5. Ley Orgánica 39/2015, de 1 de octubre, del **Procedimiento Administrativo Común de las Administraciones Públicas**. **[BOE 236 de 2-10-2015]**

2.- LEGISLACIÓN VIGENTE

1.¿Conoces la RGPD? +2 ptos.

2.¿Sabes que es un certificado digital? +1 pto.

3.¿Habéis utilizado un certificado digital? +2 ptos.

2.- LEGISLACIÓN VIGENTE

¿Cuánto valen sus datos personales en internet?

- **Tarjeta de crédito** se pueden comprar en internet por (si se compran en grandes cantidades,)
- Datos de acceso a una **cuenta bancaria en línea** asciende a unos
- Datos de **acceso a computadoras** personales por unos
- **Datos completos de una identidad robada**, con el número de la seguridad social y de la tarjeta de crédito incluidos, cuesta **me**

Informe anual sobre las amenazas en Internet realizado por la compañía de seguridad Symantec

2.- LEGISLACIÓN VIGENTE

¿Cuánto valen sus datos personales en internet?

- **Tarjeta de crédito** se pueden comprar en internet por **1,50€** (si se compran en grandes cantidades,)
- Datos de acceso a una **cuenta bancaria en línea** asciende a unos **225€**.
- Datos de **acceso a computadoras** personales por unos **5€**
- **Datos completos de una identidad robada**, con el número de la seguridad social y de la tarjeta de crédito incluidos, cuesta **menos de 15€**

Informe anual sobre las amenazas en Internet realizado por la compañía de seguridad Symantec

2.- LEGISLACIÓN VIGENTE

Un ejemplo de **ciberladrón** es el del británico **David Levy**, que **vendió artículos inexistentes por unos €300.000** con las identidades falsas de usuarios de eBay con buenos historiales de ventas por Internet, condición importante para vender productos en esa plataforma de subastas.

Levy, de 29 años, fue condenado a **tres años de cárcel** en noviembre del 2005.

PROGRAMA DE FORMACIÓN
Transformación digital e Industria 4.0

DIRECCIÓN ESTRATÉGICA · AUTOMATIZACIÓN DE LA INDUSTRIA · DATOS DIGITALES · CONECTIVIDAD · APLICACIONES PARA EL CLIENTE

Taller 3. Conectividad

2.- LEGISLACIÓN VIGENTE

Firma Electrónica

- **Objetivo principal:** lograr transmitir confianza y seguridad en las comunicaciones telemáticas.
- **Aspectos principales:**
  - **Permite detectar cualquier cambio ulterior de los datos firmados**.
  - Está **vinculada al firmante** de manera única y a los datos a que se refiere.
  - Ha sido **creada por medios que el firmante puede mantener bajo su exclusivo control.**

La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica **el mismo valor que la firma manuscrita en relación con los consignados en papel**.

6.- DEFINICIÓN DE VIRUS, TROYANOS Y SPYWARE

virustotal

PANDA SECURITY

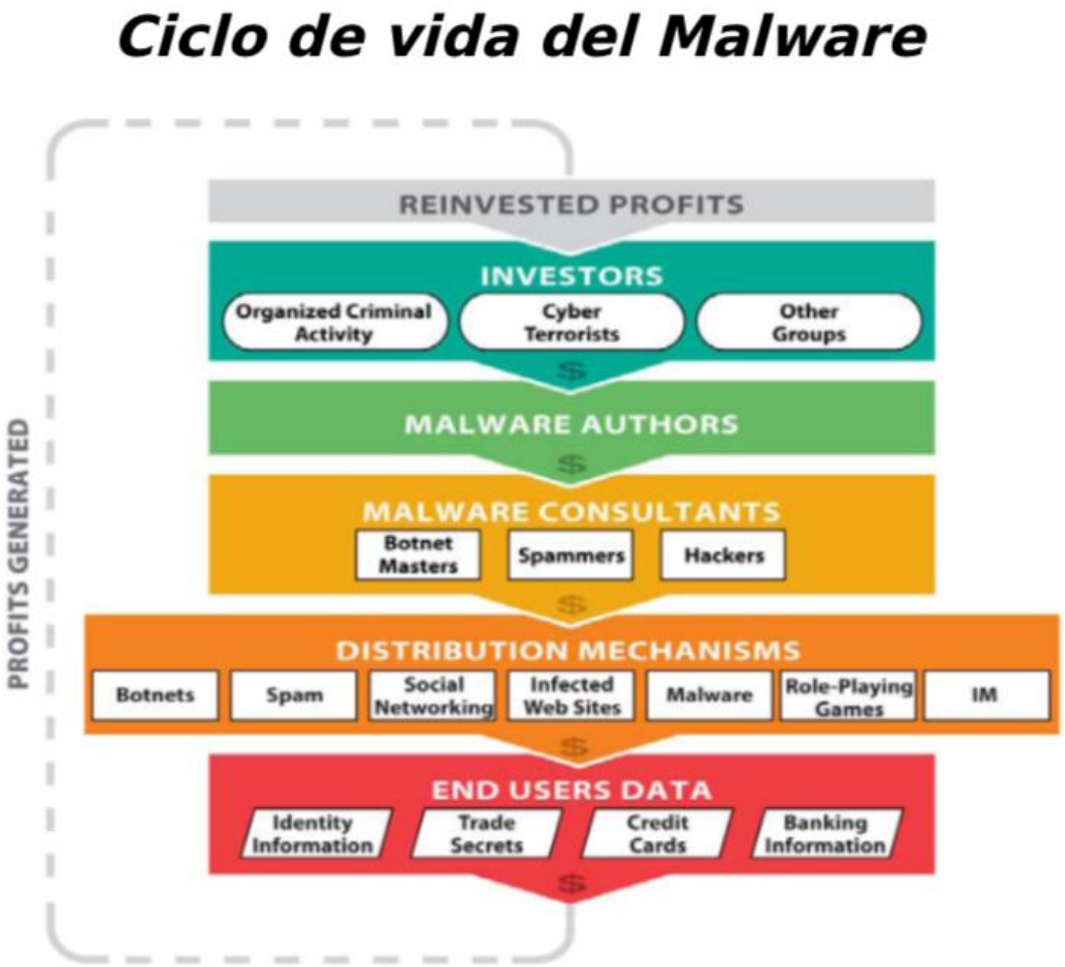
AVG. Free Anti-Virus

KASPERSKY

Microsoft Security Essentials

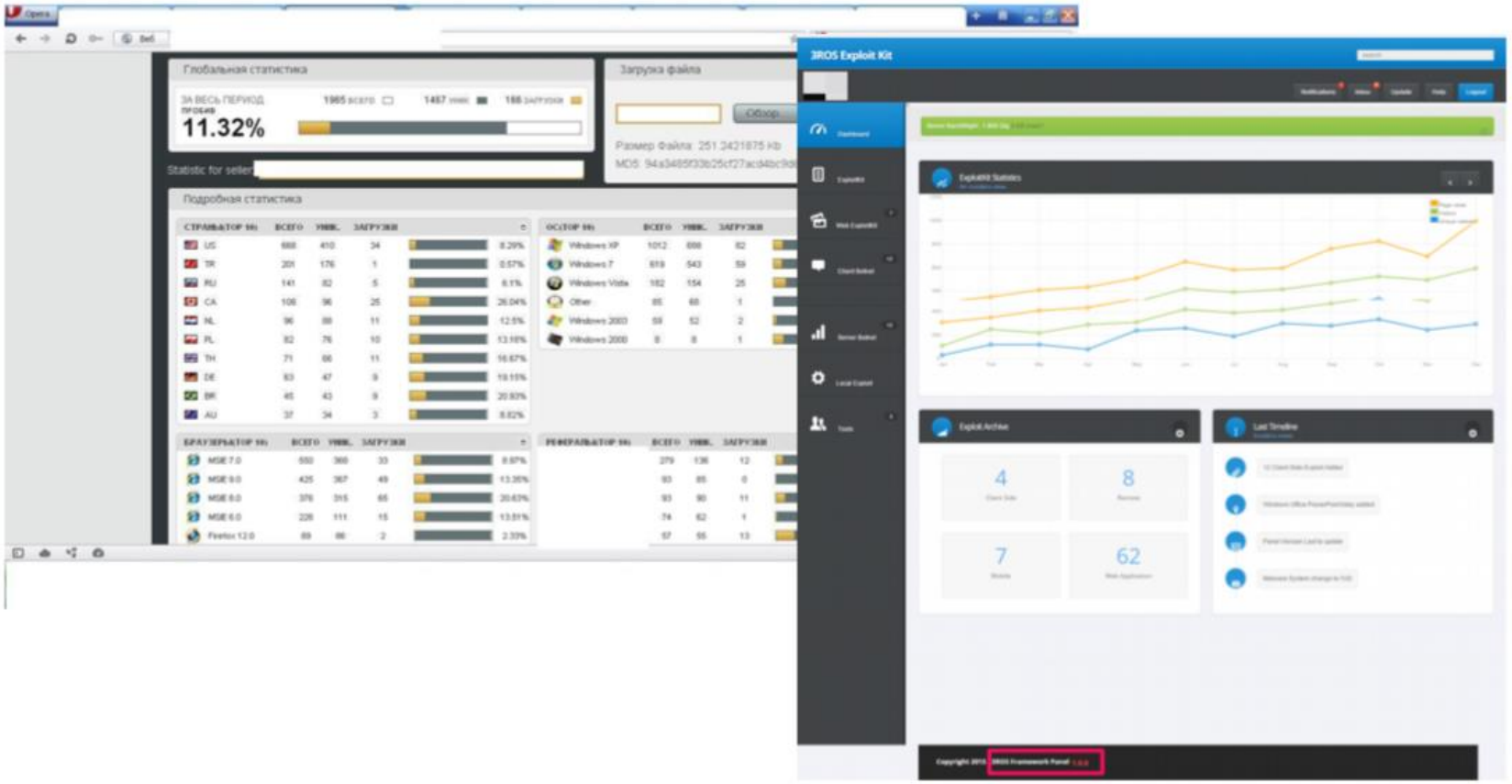
avast! be free

6.- DEFINICIÓN DE VIRUS, TROYANOS Y SPYWARE



6.- DEFINICIÓN DE VIRUS, TROYANOS Y SPYWARE

Cibercrimen como servicio



7.- PASOS CLAVES PARA PROTEGER LA INFORMACIÓN

1. **Mantén actualizado tu equipo,** tanto el Sistema Operativo como cualquier aplicación que tengas instalada.
2. Haz **copias de seguridad** con cierta frecuencia, para evitar la pérdida de datos importante.
3. Utiliza **software legal** que suele ofrecer garantía y soporte.
4. Utiliza **contraseñas fuertes** en todos los servicios, para dificultar la suplantación de tu usuario (evita nombres, fechas, datos conocidos o deducibles, etc.).
5. Utiliza **herramientas de seguridad** que te ayudan a proteger / reparar tu equipo frente a las amenazas de la Red.
6. **Crea diferentes usuarios**, cada uno de ellos con los permisos mínimos necesarios para poder realizar las acciones permitidas.

7.- PASOS CLAVES PARA PROTEGER LA INFORMACIÓN

1.Mantén actualizado tu equipo +2 Ptos
2.¿Haces copias de seguridad? +2 Ptos
3.¿Solo utilizas software legal? + 5 Ptos
4.¿Utilizas anitivirus? +5 Ptos

8.- MANEJO DE SPAM

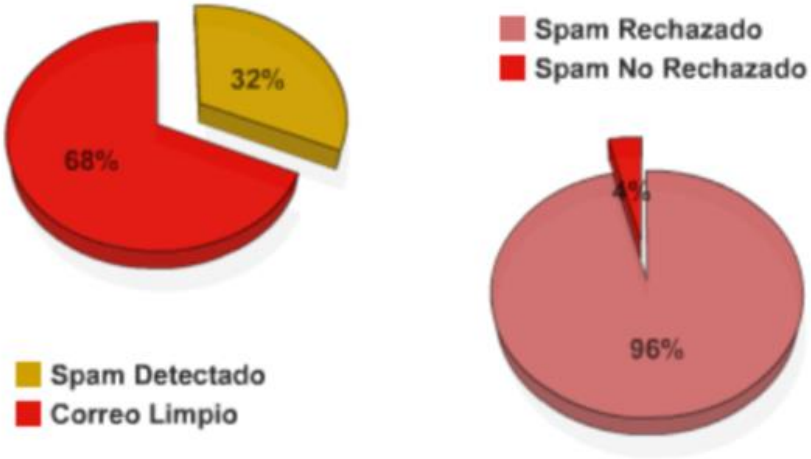
Monty Python's Flying Circus

https://www.youtube.com/watch?v=M_eYSuPKP3Y

8.- MANEJO DE SPAM

"En el mundo más del 80% del correo electrónico es SPAM"

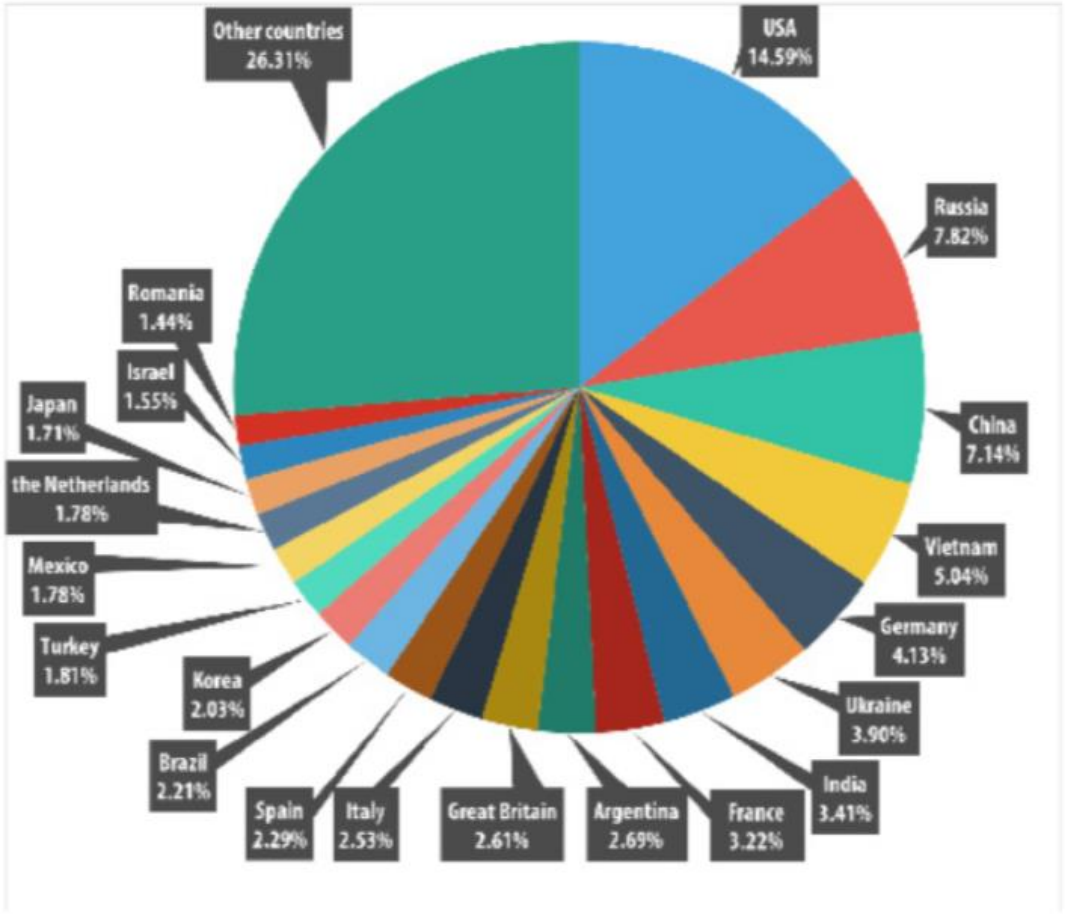
"En España el 32% del correo electrónico es SPAM"



Ninguna técnica de filtrado es 100% efectiva por sí misma

Taller 3. **Conectividad**

8.- MANEJO DE SPAM



Countries that were sources of spam, Q2 2015

8.- MANEJO DE SPAM

El Spam es **la obtención de información no solicitada**, habitualmente de tipo publicitario, que se envían aleatoriamente a grandes cantidades de usuarios. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva su gestión, representa un elemento molesto para los usuarios de Internet.

El spam conlleva:

- **Pérdida de tiempo.** La información que no es de interés o utilidad para el usuario y tiene que eliminarla.
- **Puede hacer perder información valiosa**. Algunos correos válidos son clasificados como spam por algunos filtros, lo que hace que se pierda información útil e incluso vital.

8.- MANEJO DE SPAM - PHISHING

Phishing es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta

Date: Mon, 27 May 2013 04:30:27 -0600
From: [redacted]@[redacted]d.gob.ni
To: [redacted]@[redacted].ni
Subject: NOTIFICACIÓN DE GANANCIA de mayo del 2013

Señor / Señora

Nos comunicaremos con usted para informarle que acaban de ganar la lotería organizada por la empresa MICROSOFT WINDOWS (250.000 euros).Para entrar en posesión de la ganancia, por favor envíe un correo electrónico para obtener el reconocimiento de agente judicial:
Maestro ANGE BATONNIER
[redacted]nier@e[redacted]ia.com

Obtenga todas las felicitaciones del grupo de Microsoft Windows.
La Sra. Veronique Carriere
Jefe de Campaña
MICROSOFT WINDOWS.

De: "Loteria Nacional" <k[redacted]a@driv[redacted]n.ne.jp>
A:
Asunto: Notificacion de Premio 915,000.00Euros
Fecha: Fri, 28 Oct

Atencion,

ENHORABUENA
Buscar Adjunto de la notificacion de premio
Por favor, Rellenar este formulario para el proceso del pago y envirlo
Por la agente SARAPHINA SECURITY SERVICES por fax: 0044 208-082-5519

Antonio Williams
(director)

8.- MANEJO DE SPAM - PHISHING

BADAJOZ

La Policía recibe 172 denuncias por delitos informáticos desde enero

El 'phishing' es la estafa más común, ofrecen un gran sueldo a cambio de trabajar desde casa y vacían las cuentas del usuario de Internet

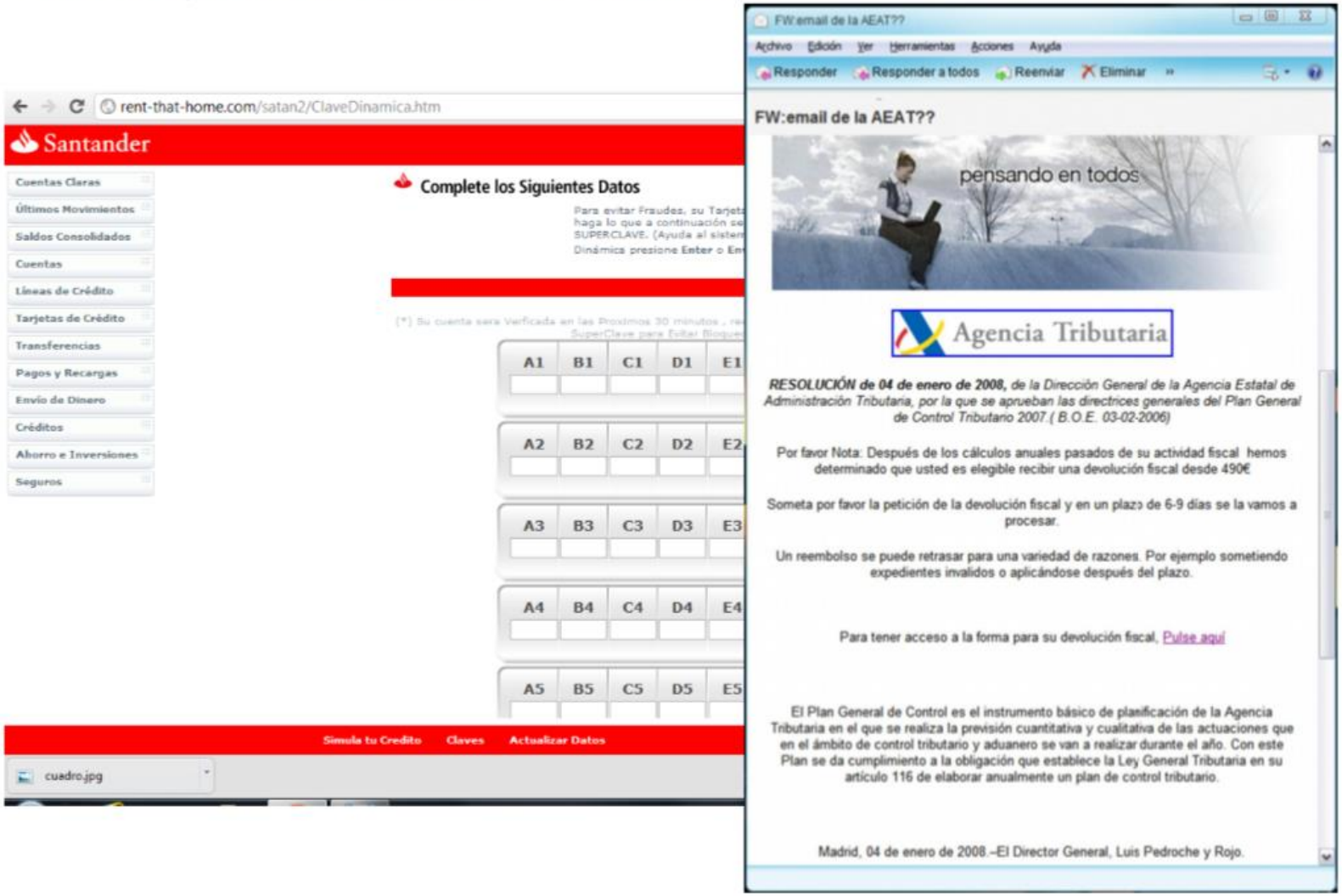
NATALIA REIGADAS | BADAJOZ

Reciben un correo electrónico de una mujer que se identifica como Elena, manager de una empresa internacional que busca empleados para el puesto de agentes en España. Ofrece un sueldo de 2.500 euros al mes y se puede trabajar desde casa con todas las comodidades.

El grupo de Delitos Tecnológicos detuvo recientemente a un 'mulero' en Badajoz. Era un hombre de 32 años de edad que ganó 3.320,4 euros en sólo unos días pero fue denunciado por las víctimas desde Santa Cruz de Tenerife. Su delito fue aceptar la oferta de trabajo de una empresa por Internet. Le pidieron que diese su número de cuenta, recibiría una transferencia y debía sacar el dinero e ingresarlo en otro lugar. Podía quedarse con el 5%.

Taller 3. **Conectividad**

8.- MANEJO DE SPAM - PHISHING



Taller 3. **Conectividad**

8.- MANEJO DE SPAM - PHISHING

8.- MANEJO DE SPAM - PHISHING

EJEMPLO REAL DE PHISHING

- La cantidad de visitas al sitio falso fue de **1.047 usuarios** únicos.
- Los usuarios que ingresaron su información personal y sus datos bancarios reales, **se obtienen 132 víctimas. (12,6%)**
- En el último caso un delincuente había creado **tres sitios falsos** de la misma entidad financiera **en 10 días** y había **logrado 1.325 clics** entre usuarios engañados.
- Si el 12% de los usuarios ingresó sus datos, el delincuente logró **al menos 159 cuentas válidas.**
- Suponiendo, en forma optimista, que el phisher sólo robó 30€ de cada cuenta obtenida, estaría logrando al menos **4.770 € en 10 días "de trabajo“.**

Autor Cristian Borghello www.segu-info.com

8.- MANEJO DE SPAM - PHISHING

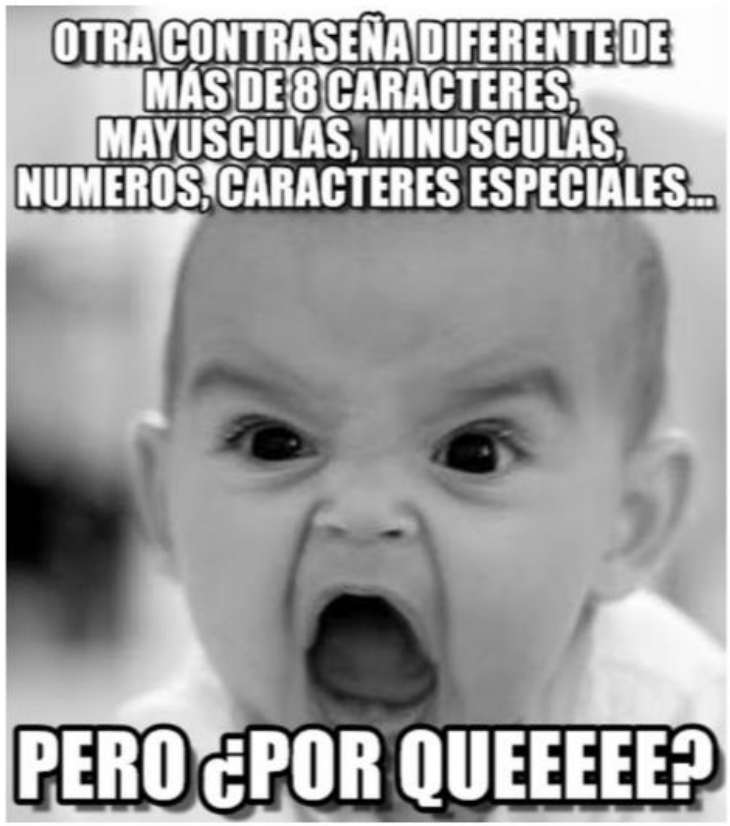
RECOMENDACIONES

- **No haga pública su dirección de correo** en foros, chats, grupos de noticias, etc.
- Publique su dirección en páginas web solo cuando sea necesario.
- Ignore el contenido de mensajes en los que se apela a su caridad, se le avisa de peligrosos virus o se le indica que los reenvíe a otras personas (correos encadenados).
- **No conteste a mensajes de correo basura** ni abra las páginas Web en las que invitan a conseguir más información o a borrarle de su lista de clientes; con esto sólo se consigue confirmar la existencia de la dirección.

8.- MANEJO DE SPAM

- Si no das tu dirección de correo por ahí libremente + 2 Ptos
- Si no hacemos caso de los correos basura SPAM +2 Ptos

9.- MANEJO DE CONTRASEÑAS



Taller 3. **Conectividad**

9.- MANEJO DE CONTRASEÑAS

NO	Top 1-100	Top 101–200	Top 201–300	Top 301–400	Top 401–500
1	123456	porsche	firebird	prince	rosebud
2	password	guitar	butter	beach	jaguar
3	12345678	chelsea	united	amateur	great
4	1234	black	turtle	7777777	cool
5	pussy	diamond	steelers	muffin	cooper
6	12345	nascar	tiffany	redsox	1313
7	dragon	jackson	zxcvbn	star	scorpio
8	qwerty	cameron	tomcat	testing	mountain
9	696969	654321	golf	shannon	madis
10	mustang	computer	bond007	murphy	987654
11	letmein	amanda	bear	frank	brazil
12	baseball	wizard	tiger	hannah	lauren
13	master	xxxxxxxx	doctor	dave	japan
14	michael	money	gateway	eagle1	naked
15	football	phoenix	gators	11111	squirt
16	shadow	mickey	angel	mother	stars
17	monkey	bailey	junior	nathan	apple
18	abc123	knight	thx1138	raiders	alexis
19	pass	iceman	porno	steve	aaaa
20	fuckme	tigers	badboy	forever	bonnie
21	6969	purple	debbie	angela	peaches

Cuanto mayor sea la longitud de su clave más seguridad añadirá a su información

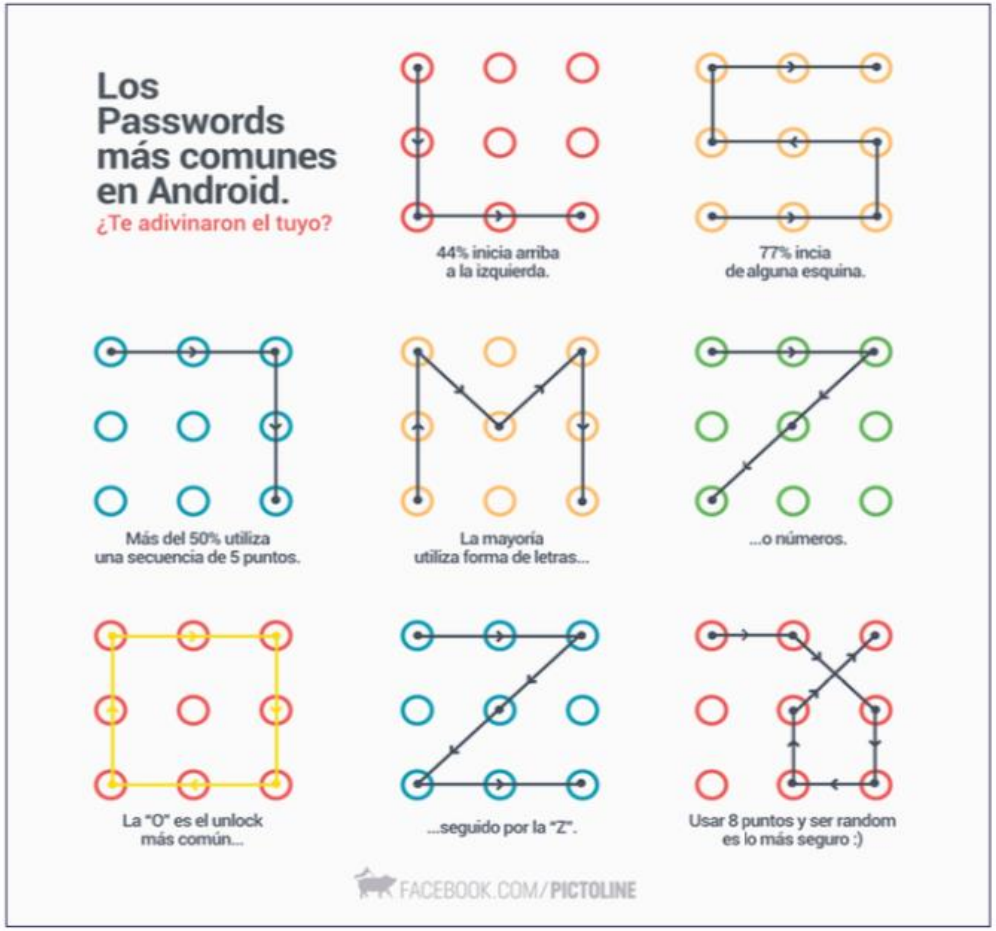
Incluye caracteres extraños como !-_#@!

No uses datos deducibles

Cambia tus claves con regularidad

9.- MANEJO DE CONTRASEÑAS

	PIN	Frecuencia
#1	1234	10,713%
#2	1111	6,016%
#3	0000	1,881%
#4	1212	1,197%
#5	7777	0,745%
#6	1004	0,616%
#7	2000	0,613%
#8	4444	0,526%
#9	2222	0,516%
#10	6969	0,512%
#11	9999	0,451%
#12	3333	0,419%
#13	5555	0,395%
#14	6666	0,391%
#15	1122	0,366%
#16	1313	0,304%
#17	8888	0,303%
#18	4321	0,293%
#19	2001	0,290%
#20	1010	0,285%



9.- MANEJO DE CONTRASEÑAS

¿Para qué recordar el PIN?
Tecnología Contactless

9.- MANEJO DE CONTRASEÑAS

Tecnología Contactless

¿Sabías que los datos de tu tarjeta de crédito/débito están al alcance de cualquier móvil?

Jakub Motyka el 19/04/2016 a las 11:03

ING, iPP310, V3, PIN Pad/Card Reader/SCR/Contactless, New INGENICO terminal

$192.00
or Best Offer

From United States

Customs services and international tracking provided

Ingenico IPP220 Pin Pad w/ Smart Card w/o Contactless *Refurb*

NON CONTACTLESS READER | MPN: IPP220-01P1841A

$49.00
Buy It Now

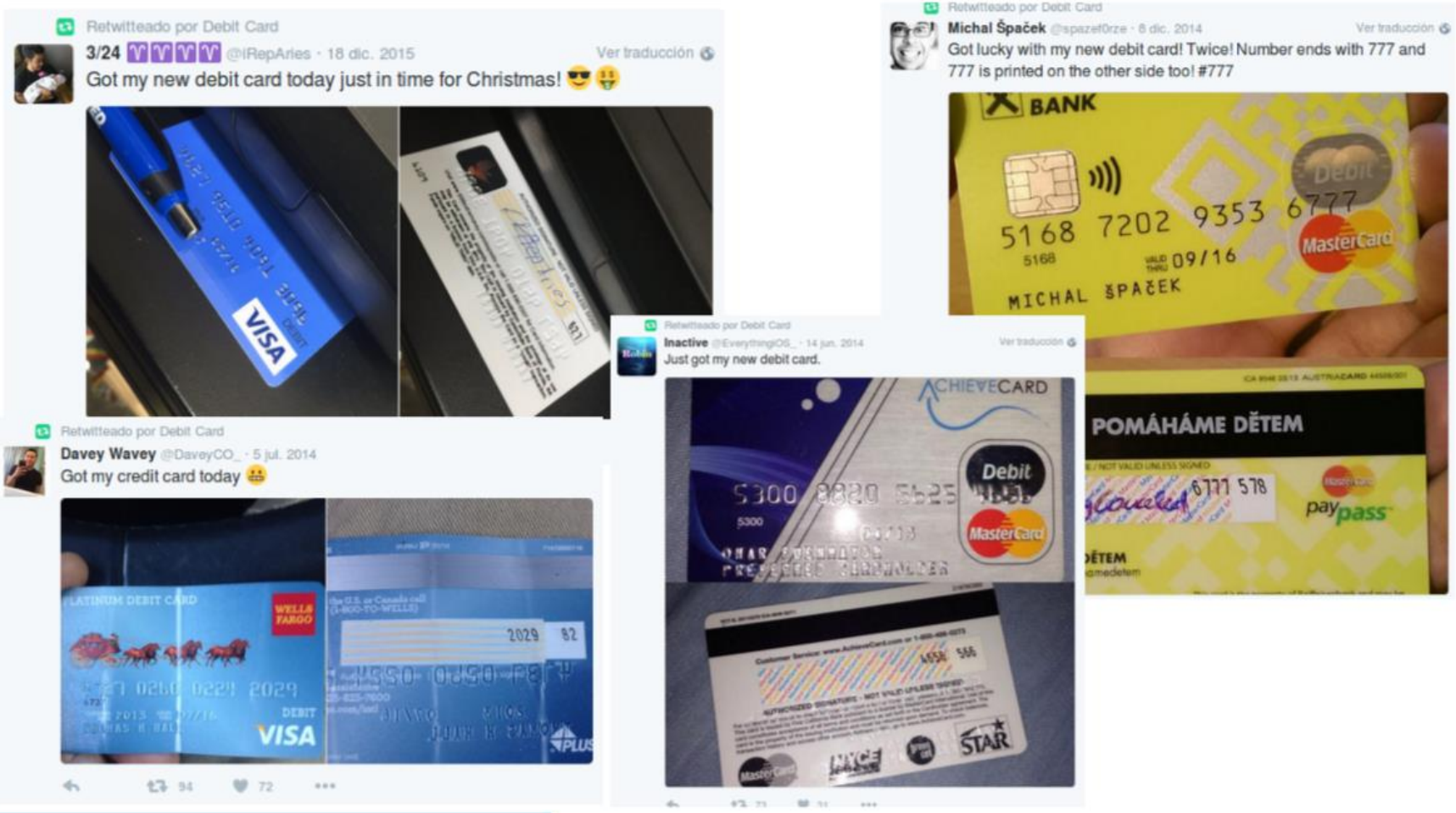
From United States

Customs services and international tracking provided

Taller 3. **Conectividad**

9.- MANEJO DE CONTRASEÑAS

La moda de publicar las tarjetas en redes sociales



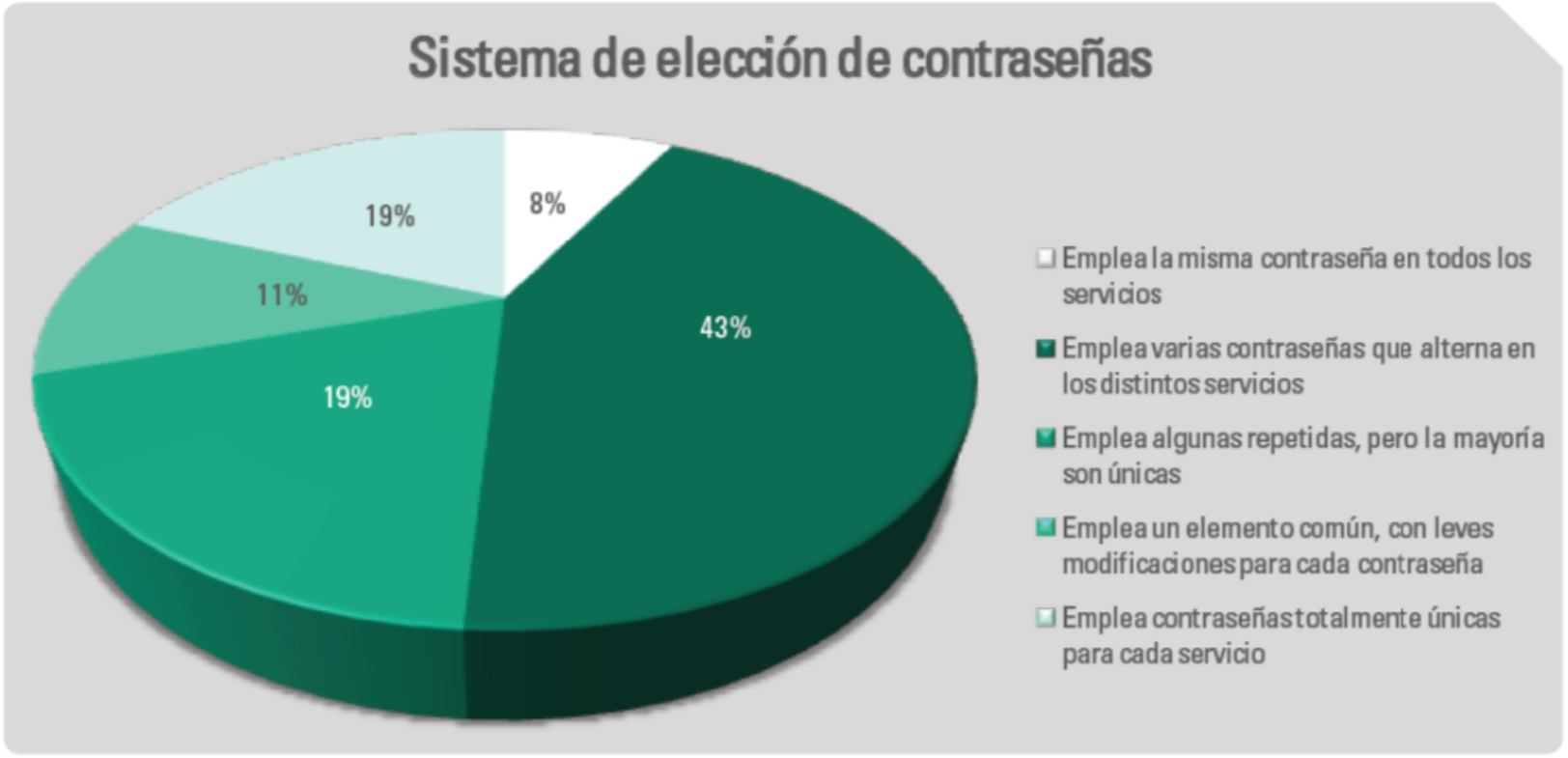
9.- MANEJO DE CONTRASEÑAS

Usar nemotécnicas:

1. "La seguridad es como una cadena, es tan fuerte como el eslabón más débil" podría convertirse en "Lsec1cetfceemd".

Longitud de la contraseña	Todo tipo de caracteres	Sólo letras Minúsculas
3 caracteres	0.86 segundos	0.02 segundos
4 caracteres	1.36 minutos	0.46 segundos
5 caracteres	2.15 horas	11.9 segundos
6 caracteres	8.51 días	5.15 minutos
7 caracteres	2.21 años	2.23 horas
8 caracteres	2.10 siglos	2.42 días
9 caracteres	20 milenios	2.07 meses
10 caracteres	1,899 milenios	4.48 años
11 caracteres	180,365 milenios	1.16 siglos
12 caracteres	17,184,705 milenios	3.03 milenios
13 caracteres	1,627,797,068 milenios	78.7 milenios
14 caracteres	154,640,721,434 milenios	2,046 milenios

9.- MANEJO DE CONTRASEÑAS



¿Preguntas?

Gracias!!

David Romero Trejo
www.ariadnex.com
david@ariadnex.com

PROGRAMA DE FORMACIÓN

Transformación digital e Industria 4.0

Fondo Social Europeo
Una manera de hacer Europa

EXTREMADURA EMPRESARIAL

Unión Europea

JUNTA DE EXTREMADURA

Taller 3.

U2 – Protección de Infraestructuras

SEGURIDAD PERIMETRAL

- Introducción
- Política de seguridad
- Componentes de seguridad perimetral

INTRODUCCIÓN

"El único sistema verdaderamente seguro es aquel que está apagado, encerrado en un bloque de hormigón y sellado en una habitación recubierta de plomo con guardias armados.... y aún así tengo mis dudas"

Eugene Spafford

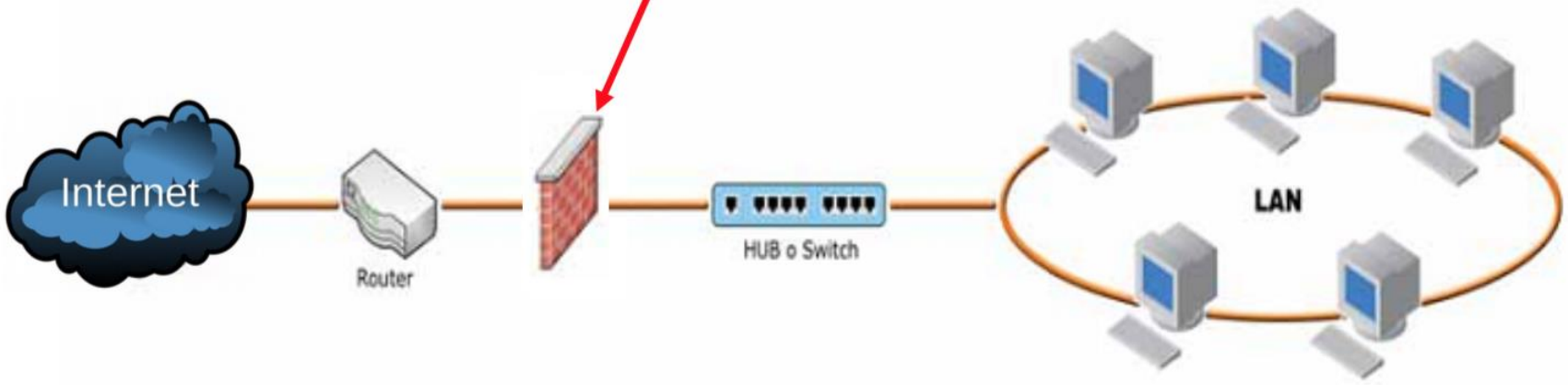
¿QUÉ ES UN CORTAFUEGOS?

Un cortafuegos o FW, es un dispositivo que ha sido diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Por lo tanto debe ser capaz de:

- "Escuchar" la totalidad del tráfico que deseemos analizar. Esto ya lo conocemos, y es la técnica que emplea todo "sniffer".
- Tener la capacidad de "desarmar" los encabezados de cada protocolo.
- Tener patrones estandarizados para comprender cada protocolo (para verificar su uso correcto).
- Capacidad de enrutamiento
- Control de sesión o control de estado.
- Dos tipos:
  - FWs de hosts (a veces asociados a FWs personales y/o a servidores).
  - FWs de red.

¿QUÉ ES UN CORTAFUEGOS?

FIREWALL = **“Cortafuegos”**



Controlar las comunicaciones, permitiéndolas o bloqueándolas según las políticas de seguridad.

CATEGORÍAS DE CORTAFUEGOS

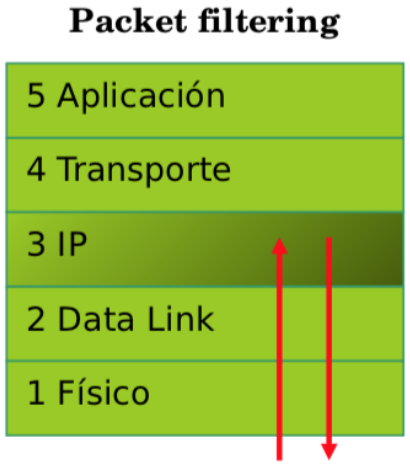
Esta clasificación depende del nivel o niveles dentro del modelo *TCP/IP* trabaje el sistema cortafuegos:

- Packet filtering
- Proxy servers
- Stateful multilayer inspection

CATEGORÍAS DE CORTAFUEGOS

Packet Filtering:

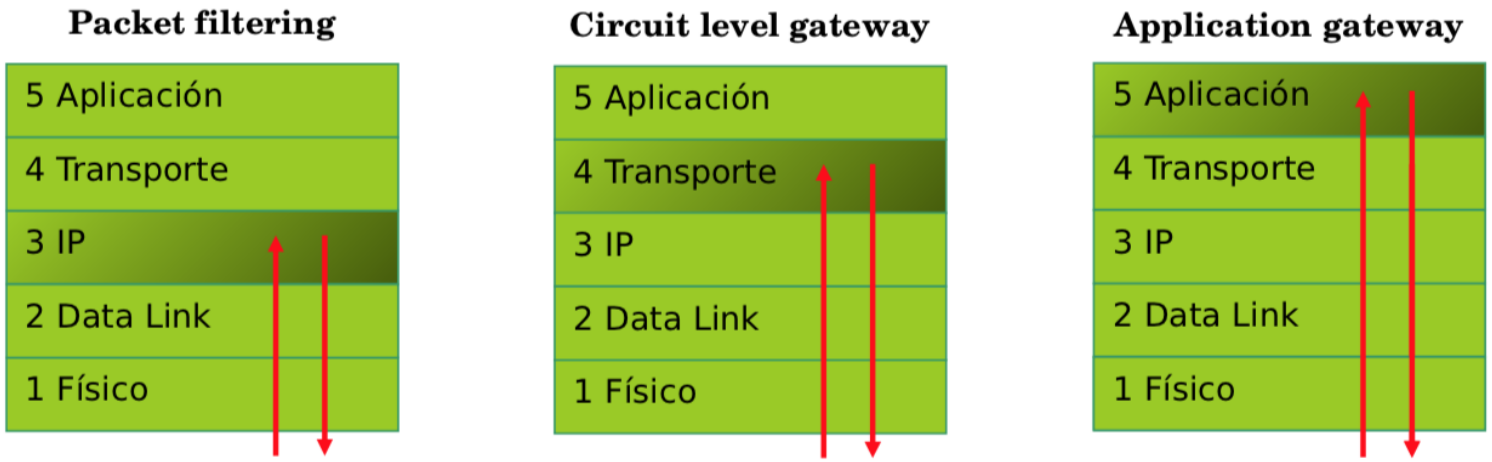
- Actúa dentro del *nivel IP* según el modelo *TCP/IP*
- Suele ser implementado utilizando *routers*
- Cada paquete puede ser analizado en función de:
  - @IP origen / destino
  - Puerto origen / destino
  - Protocolo usado: TCP / UDP / ICMP



CATEGORÍAS DE CORTAFUEGOS

Proxy Server

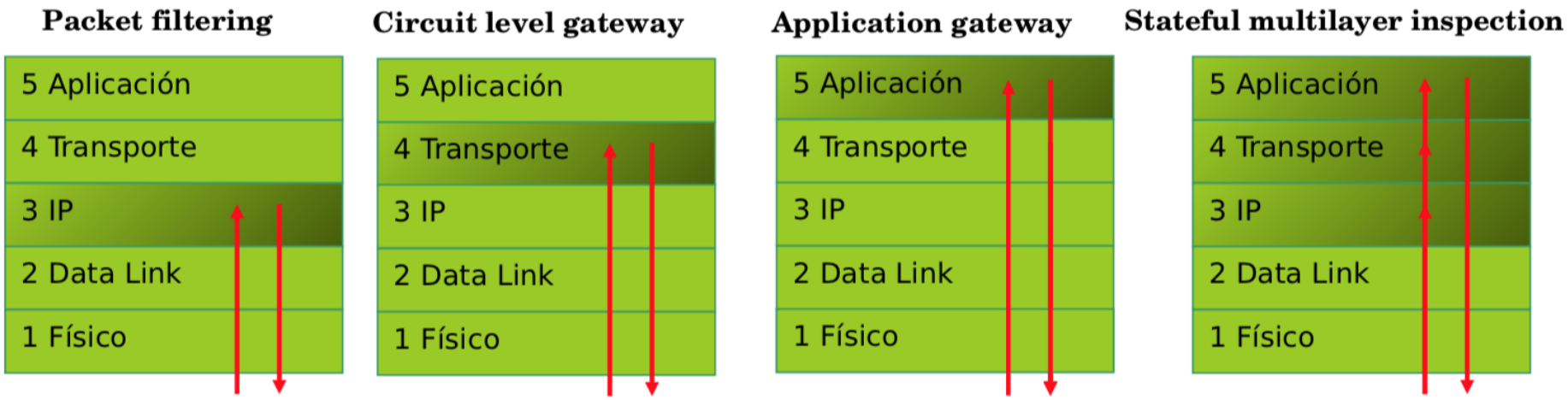
- Actúa dentro de los *niveles de transporte y aplicación* (*circuit level gateway* y *application gateway* respectivamente) según el modelo *TCP/IP*.
- Procesa, valida y regenera cada paquete recibido; impidiendo la conexión directa entre 2 redes diferentes.
- Para cada servicio (*telnet, ftp, http...*) se utiliza un proxy específico, pudiendo así prohibir el uso de determinadas órdenes de un servicio.



CATEGORÍAS DE CORTAFUEGOS

Stateful Multilayer Inspection

- Actúa dentro de los *niveles de IP, transporte y aplicación* según el modelo *TCP/IP*
- Comprueba (y no procesa, como en un Proxy server) los paquetes a distintos niveles verificando la validez de estos, basándose en un seguimiento del estado de la conexión en cada momento.
- Permite conexiones directas entre distintas redes, dando un servicio transparente a ambos lados.



UTM Y NGFW

- UTM es la evolución natural de un Firewall, donde además de las funcionalidades normales de un Cortafuegos también añade otros servicios.
  - Antivirus y AntiSpam
  - Detección y prevención de intrusos (IDS/IPS)
  - Anti-Spyware
  - Filtro de contenidos web y control de aplicaciones.
- Su diferencia fundamental es el análisis de una porción de los datos de paquete para determinar el tipo de tráfico.
- Un Firewall o NGFW (Next Generation FW) realiza inspección del estado de las cabeceras de los paquetes: **Stateful Packet Inspection** (SPI) frente a **Deep Packet Inspection** (DPI).
- Un UTM sin los servicios adicionales activos es un Firewall.
- Tiene capacidad de inspeccionar tráfico SSL

DIMENSIONAMIENTO DE UN CORTAFUEGOS

Para poder valorar un sistema firewall, debemos de analizar los siguientes aspectos:

- Performance (Rendimiento)
- Availability (Disponibilidad)
- Security (Seguridad)
- Flexibility (Flexibilidad)
- Ease of use (Facilidad de Uso)

DIMENSIONAMIENTO DE UN CORTAFUEGOS

Al activar todos los servicios de UTM el **rendimiento baja** muchísimo puesto que tiene que realizar análisis detallado y exhaustvo del tráfico.

- **No todos los servicios consumen lo mismo**: El Filtro web es más ligero, la prevención de intrusos y el anti-spyware tiene un impacto moderado, y sin embargo el antivirus que escanea y analiza los archivos es más intenso.
- El rendimiento de un UTM con todos los servicios activados es como cinco veces Inferior al rendimiento del equipo en sólo firewall.
- En la **inspección SSL** los protocolos que utilicen este cifrado se debe considerar que se reducirá en aprox. 50% el rendimiento.
- En el número de **conexiones concurrentes** de un usuario se deben considerar unas 100-200 aprox. para calcular el equipo.

Sizing Tool https://competitive.myfortinet.com/product_sizing

FABRICANTES

FortiGate

Service Provider

FortiGate-5000 Series Chassis
FortiGate-5000 Series Blades
FortiSwitch-5000 Series Blades
FortiGate-3950B
FortiGate-3810A
FortiGate-3240C
FortiGate-3140B

Large Enterprise

FortiGate-3950B
FortiGate-3810A
FortiGate-3240C
FortiGate-3140B
FortiGate-3040B
FortiGate-1240B
FortiGate-1000C

Medium Enterprise

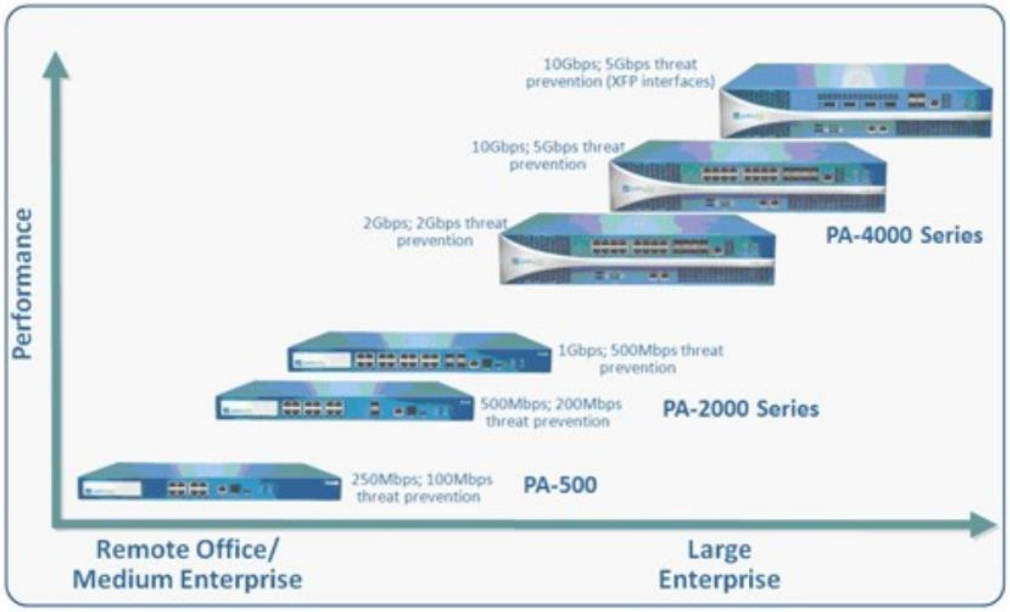
FortiGate-1240B
FortiGate-1000C
FortiGate-800C
FortiGate-600C
FortiGate-300C
FortiGate-200B/200B-POE

Small Business

FortiGate-100D
FortiGate Rugged-100C
FortiGate-80C/CM
FortiGate-60C
FortiGate-40C
FortiGate-20C

FABRICANTES

Palo Alto



FABRICANTES

Otros

Check Point SOFTWARE TECHNOLOGIES LTD.

CISCO

Cyberoam

WatchGuard

McAfee

STONESOFT

JUNIPER NETWORKS

DELL SonicWALL

Taller 1. **Automatización en la industria**

SEGURIDAD PERIMETRAL

- Introducción
- Política de seguridad
- Componentes de seguridad perimetral

POLÍTICA DE SEGURIDAD

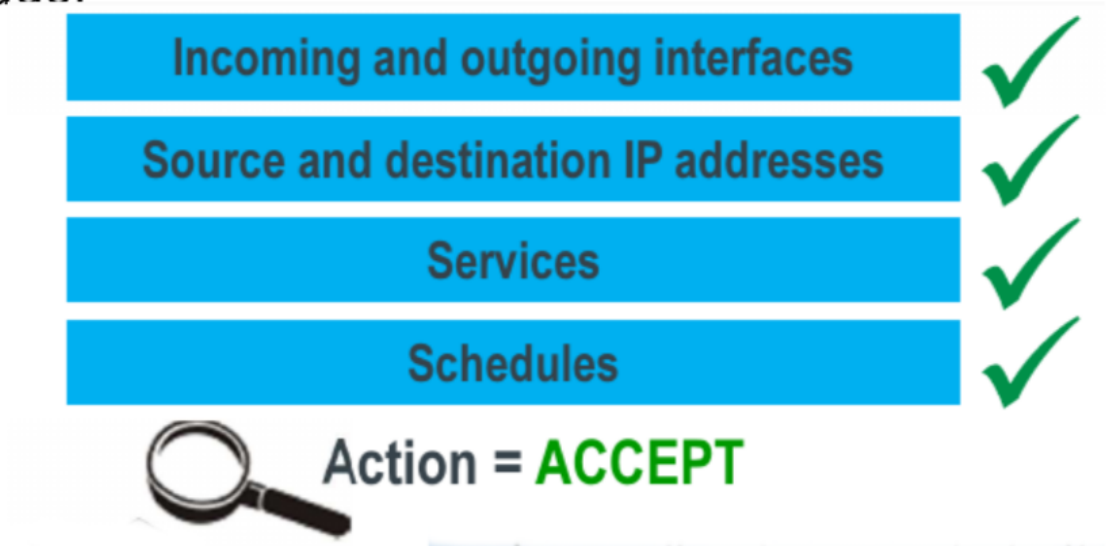
¿Qué busca un atacante/intruso?

- En general se debe tener en cuenta que un **INTRUSO** dedica todo o la mayor parte de su tiempo a nuestra red, pues es esta su actividad, y casi con seguridad está al tanto de las últimas novedades encontradas en Internet.
- Existen muchas personas que les **SOBRA TIEMPO** y que observan no lo global, sino el detalle fino, esas muy pequeñas cosas que se pueden llegar a pasar por alto, a esto le dedican todo su tiempo pues vulnerarlas es su desafío, y tarde o temprano **LO LOGRAN**.
- Por tanto, es de gran importancia cada acceso, por muy granular que sea, a la red.

POLÍTICA DE CORTAFUEGOS

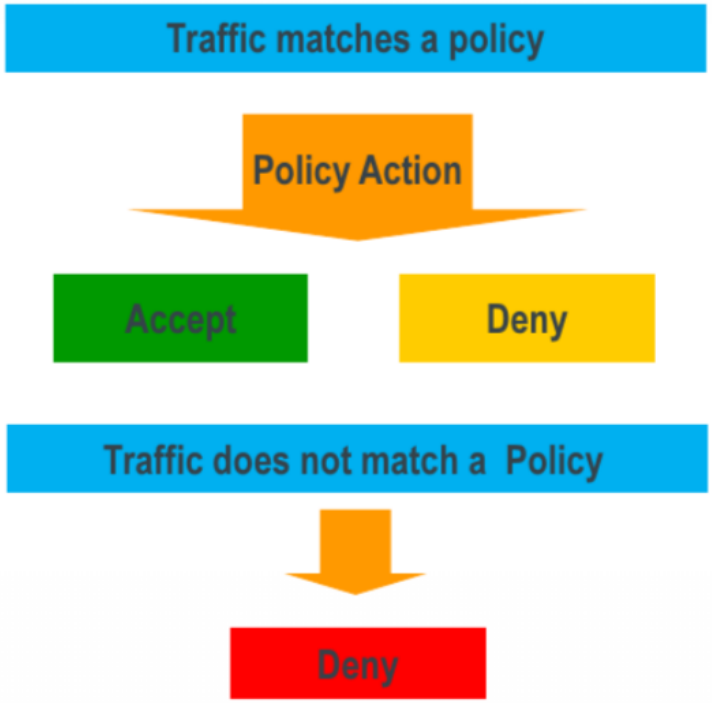
Las políticas de Firewalls incluyen las intrucciones usadas por los equipos de seguridad perimetral Firewallas para determinar que hay que hacer cuando se produce una petición de conexión.

Se analiza el tráfico de paquetes, se compara el contenido con la estructura de políticas y se realiza la acción que se ha determinado.

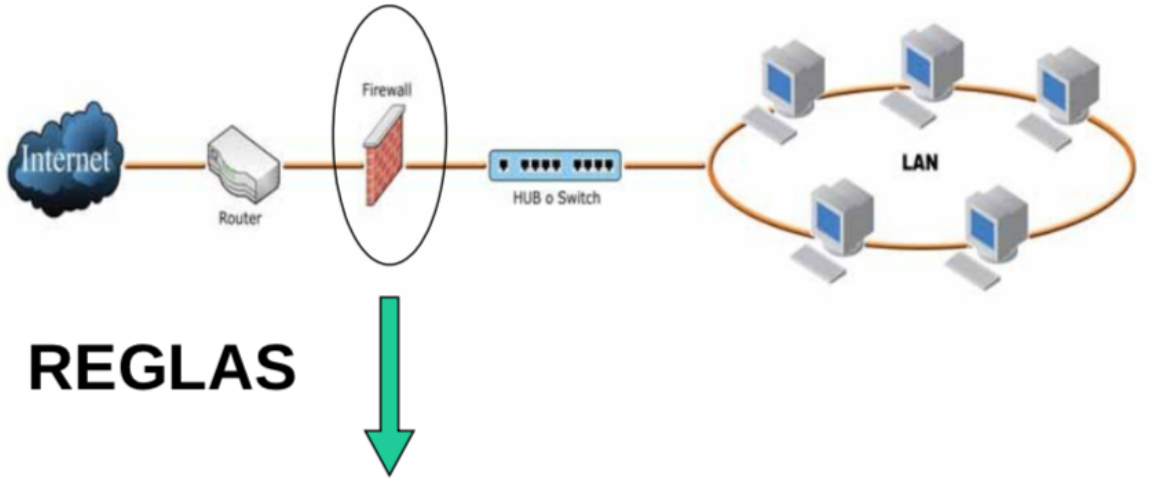


POLÍTICA DE CORTAFUEGOS

Las políticas de cortafuegos se aplican por una secuencia determinada y se establece en base a objetos que se definen dentro del equipo de seguridad perimetral que se esté utilizando.



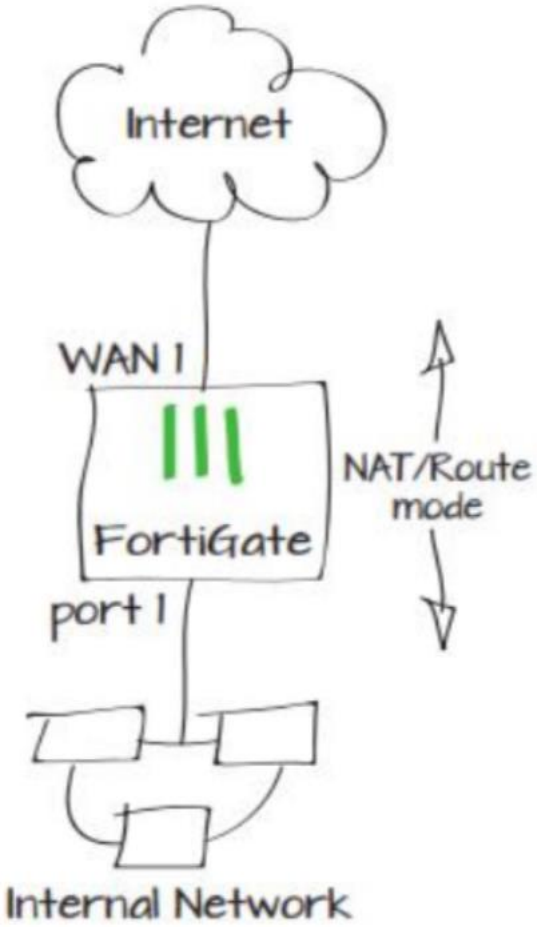
POLÍTICA DE CORTAFUEGOS

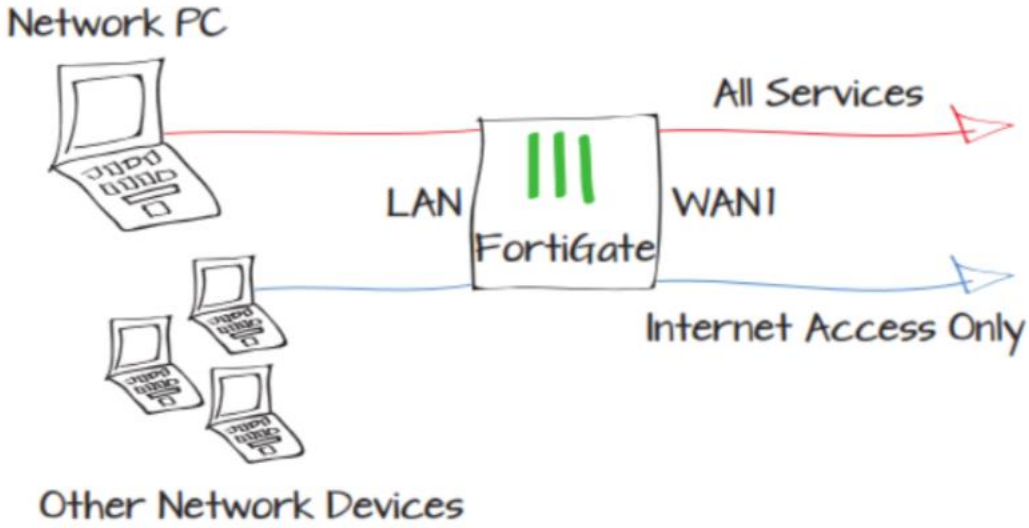


Todo lo que venga de la red local al Firewall : ACEPTAR
Todo lo que venga de una IP local al puerto TCP 22 = ACEPTAR
Todo lo que venga de la IP del Gerente al puerto TCP 1723 = ACEPTAR
Todo lo que venga de la red local al exterior = ENMASCARAR (NAT)
Política Implícita = DENEGAR

Taller 3. **Conectividad**

POLÍTICA DE SEGURIDAD BÁSICA





SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS (IDS/IPS)

IDS basados en host (HIDS):

Ventajas:

- Detectan mejor los ataques desde dentro de la red ya que detectan inicios de sesión, cambios en archivos, etc.
- Son capaces de asociar usuarios + programas = efectos
- Forman parte del propio blanco
- No se necesita monitorizar todo el tráfico de la red

Desventajas:

- Difícil implantación (SO diferentes)
- Al monitorizar los cambios en el sistema, se descubren los ataques una vez realizados.
- Si el equipo ha sido atacado no podemos confiar en sus informes.
- Si el equipo se apaga, o no está disponible, no puede enviar informes o alarmas.

SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS (IDS/IPS)

IDS basados en sensores Wireless (WIDS):

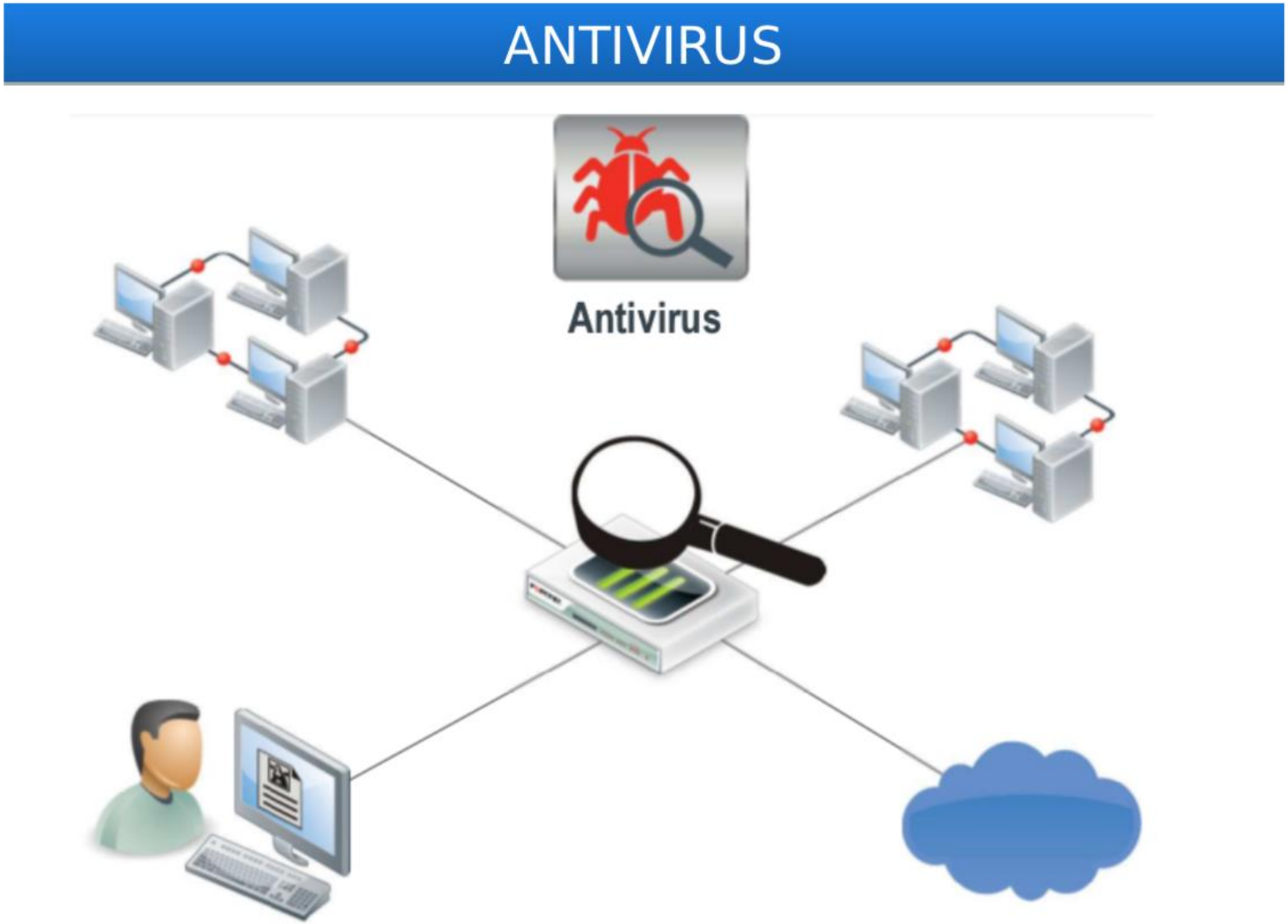
Ventajas:

- Detección de Roque AP
- Detección de ataques de acceso a la red inalámbrica

Desventajas:

- Difícil implantación de los sensores (situación geográfica)

Taller 3. Conectividad



ANTIVIRUS

¿Qué es un virus?

- Un virus informático es un malware que tiene por objetivo alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario.
- Existen distintos tipos de virus:
  - Troyano
  - Gusano
  - Bombas lógicas
  - Hoax
  - Virus cifrados
  - Virus Polimórficos
  - etc

ANTIVIRUS

¿Cómo funciona un troyano?

- Se ejecuta cuando se abre un programa vulnerable. No es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, pero es suficiente. El efecto más usual es el robo de información.

¿Cómo actúan los troyanos?

- Esperan que se introduzca una contraseña, clickar un link, o por transmisión de un disco extraíble.

Ejemplos

- Zeus, Cryptolocker, Atadommoc, Upatre, etc

ANTIVIRUS

¿Cómo funciona un spyware?

- Es un término que incluye una gama de software malicioso y no malicioso que en general extraen información del la máquina sin que el usuario tenga conocimiento de esto.

- Existen sin embargo algunos softwares que se conocen como Adware, que informan al usuario de sus intenciones, pero que esta “advertencia” esta normalmente escondida en cientos de líneas de texto legal.

ANTIVIRUS

Consecuencias por infección de Spyware

- **Robo de Información**
  - Programas de Monitoreo de Sistemas
  - Robo de passwords, números de tarjetas de crédito
  - Riesgo de problemas legales y reputacionales

- **Hacking**
  - Tomar el control del equipo
  - Usar el equipo para espiar a la organización
  - Una amenaza más grave que virus

ANTIVIRUS

Vectores de infección

- Pueden incluir diferentes modalidades de software:
  - Programas de bromas
  - Utilitarios “necesarios”
  - Troyanos
  - Cookies
  - Dialers
  - Programas de re-direccionamiento de páginas de inicio
  - Adware
  - Adjuntos de e-mail

ANTIVIRUS

Prevención

- La estrategia implantada contra los virus también funciona para el Spyware
  - Configuración de Software y Hardware
  - Actualizaciones de los sistemas operativos
  - Administración de medios magnéticos de almacenamiento
  - Escaneo
  - Políticas de correo electrónico
  - Políticas de usuario final
  - EDUCACION AL USUARIO FINAL

ANTIVIRUS

¿Qué es un Antivirus?

- Los Antivirus son programas utilizados para prevenir, detectar y eliminar virus y otras clases de malwares, utilizando todo tipo de estrategias para lograr este objetivo. Hay en total mas de 40 antivirus en el mundo, pero los mas importantes son:
  - AVG
  - Norton
  - Microsoft Security
  - Avira
  - Kaspersky
  - Panda
  - Avast!
  - Comodo

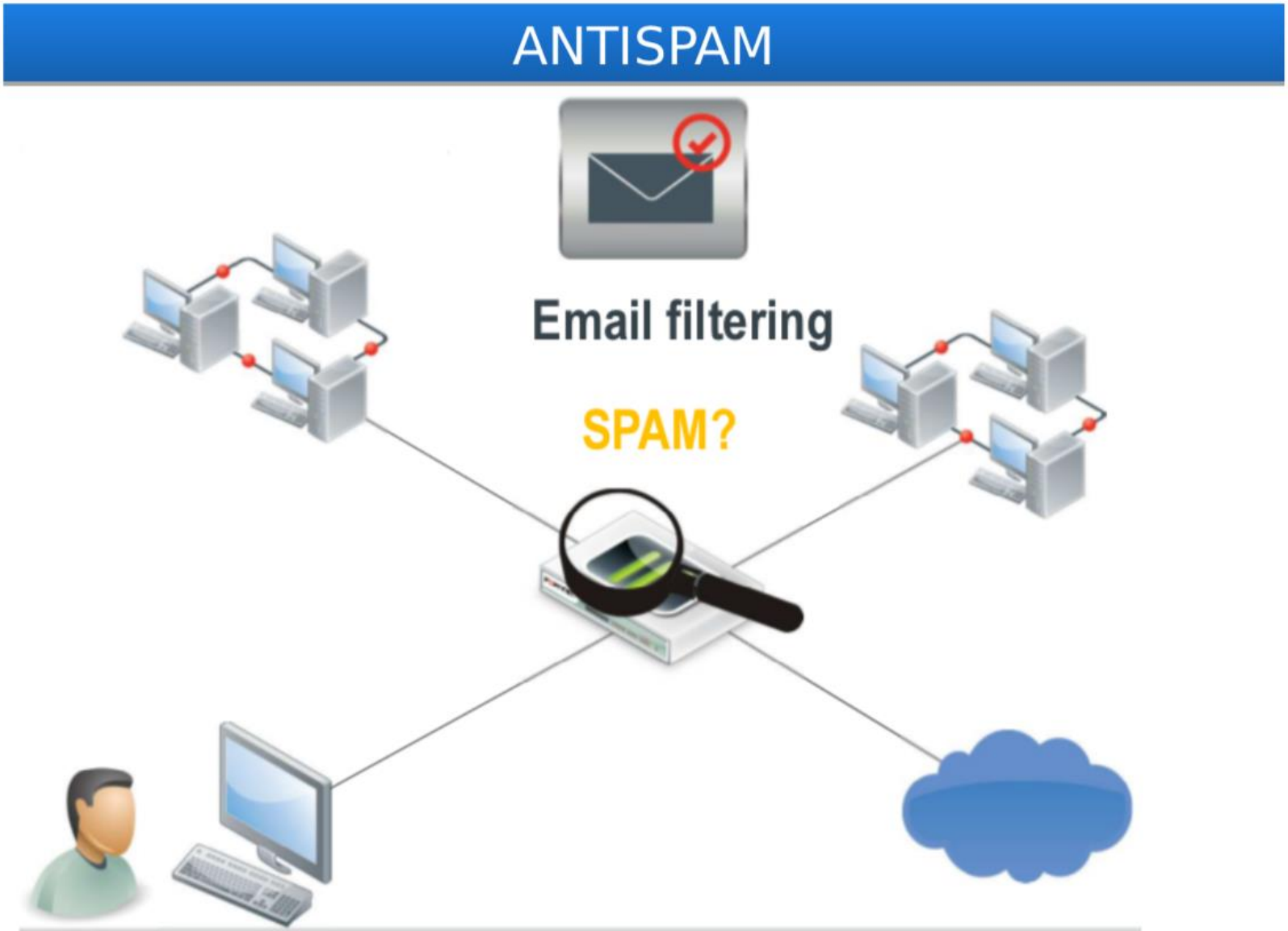
ANTIVIRUS

Spyware

- Han salido al mercado una serie de herramientas que prometen acabar con el Spyware.
- Entre las más conocidas están:
  - Ad-Aware
  - McAfee Anti-Spyware
  - HouseCall-TrendMicro (solo remueve)
  - Microsoft AntiSpyware (Beta)
  - SpyBot Search & Destroy

Sin embargo, hay que tener cuidado con todo lo que se ofrece al respecto, ya que muchas ofrecen funcionalidades que no tienen.
Muchas veces una sola herramienta no es suficiente.

Taller 3. Conectividad



ANTISPAM

¿Qué es el Spam?

- El spam es el correo electrónico, normalmente con contenido publicitario, que se envía en forma masiva.

ANTISPAM

¿Tipos de Spam?

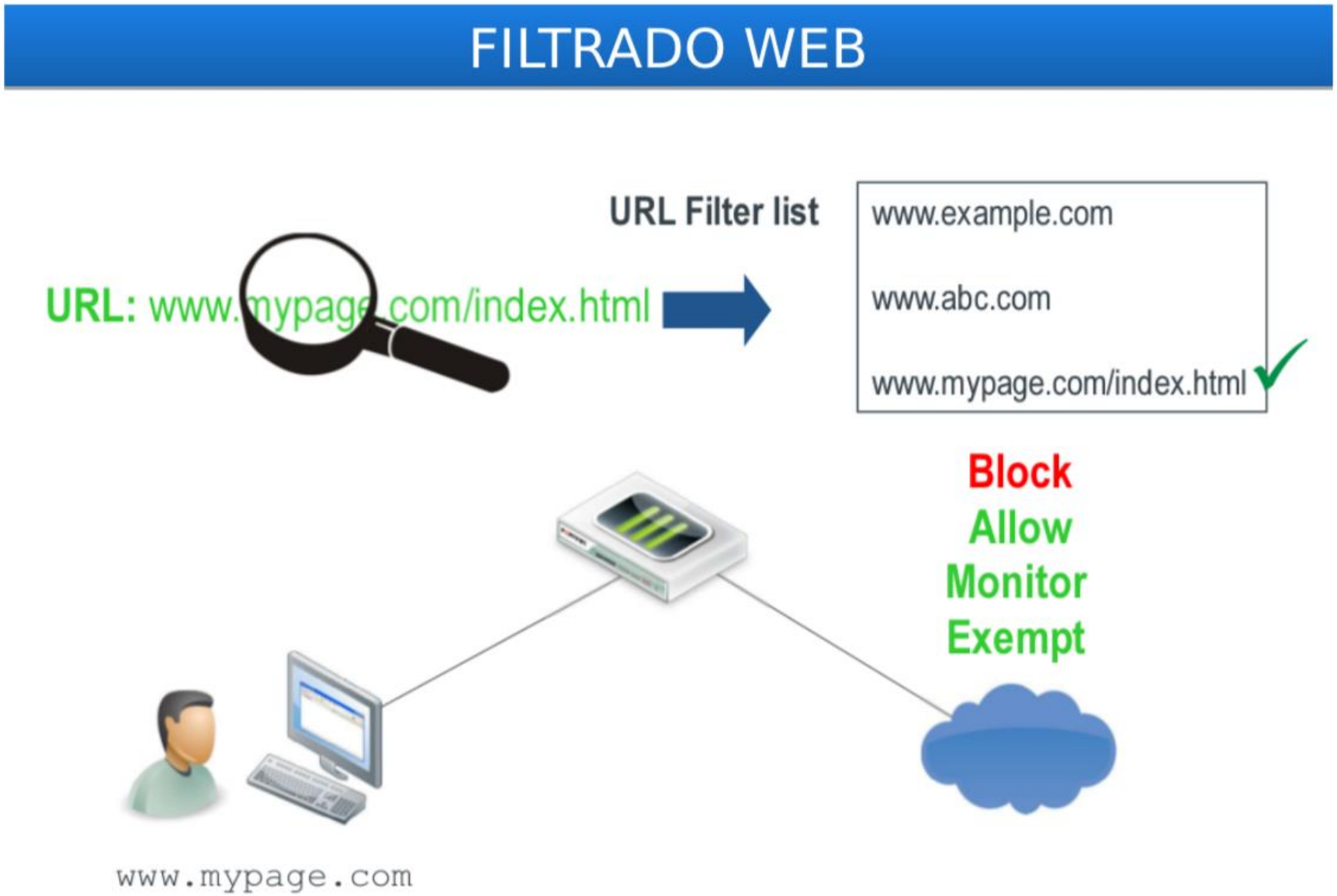
- **Spam:** Enviado a través del correo electrónico.
- **Spim:** Específico para aplicaciones de tipo Mensajería Instantánea.
- **Spit:** Spam sobre telefonía IP. La telefonía IP consiste en la utilización de Internet como medio de transmisión para realizar llamadas telefónicas.
- **Spam SMS**: Spam destinado a enviarse a dispositivos móviles mediante SMS.

ANTISPAM

¿Cómo se combate el Spam?

- **Antispam a nivel del servidor**: Son bases de datos que contienen direcciones IP o nombres de Dominio de sitios de los cuales no se quiere recibir correos.
- **Antispam a nivel del cliente de correo:** Es recomendable usar software *antispyware* y también *antispam* locales. Cabe recordar que muchos de ellos pueden eliminar, por confusión, correo que no es *spam*, con lo que sería conveniente verificar los correos que estos programas marcan como *spam*.

Taller 3. Conectividad



FILTRADO WEB

- Bloqueo de contenido web basado en categoría de URL y palabras clave.
- Filtrado web basado en la listas de reputación.

Security Risk
- Malicious Websites
- Phishing
- Spam URLs

General Interest - Business
- Finance and Banking
- Search Engines and Portals
- General Organizations
- Business
- Information and Computer Security
- Government and Legal Organizations
- Information Technology
- Armed Forces
- Web Hosting
- Secure Websites
- Web-based Applications

Adult/Mature Content
- Alternative Beliefs
- Abortion
- Other Adult Materials
- Advocacy Organizations
- Gambling
- Nudity and Risque
- Pornography
- Dating
- Weapons (Sales)
- Marijuana
- Sex Education
- Alcohol
- Tobacco
- Lingerie and Swimsuit
- Sports Hunting and War Games

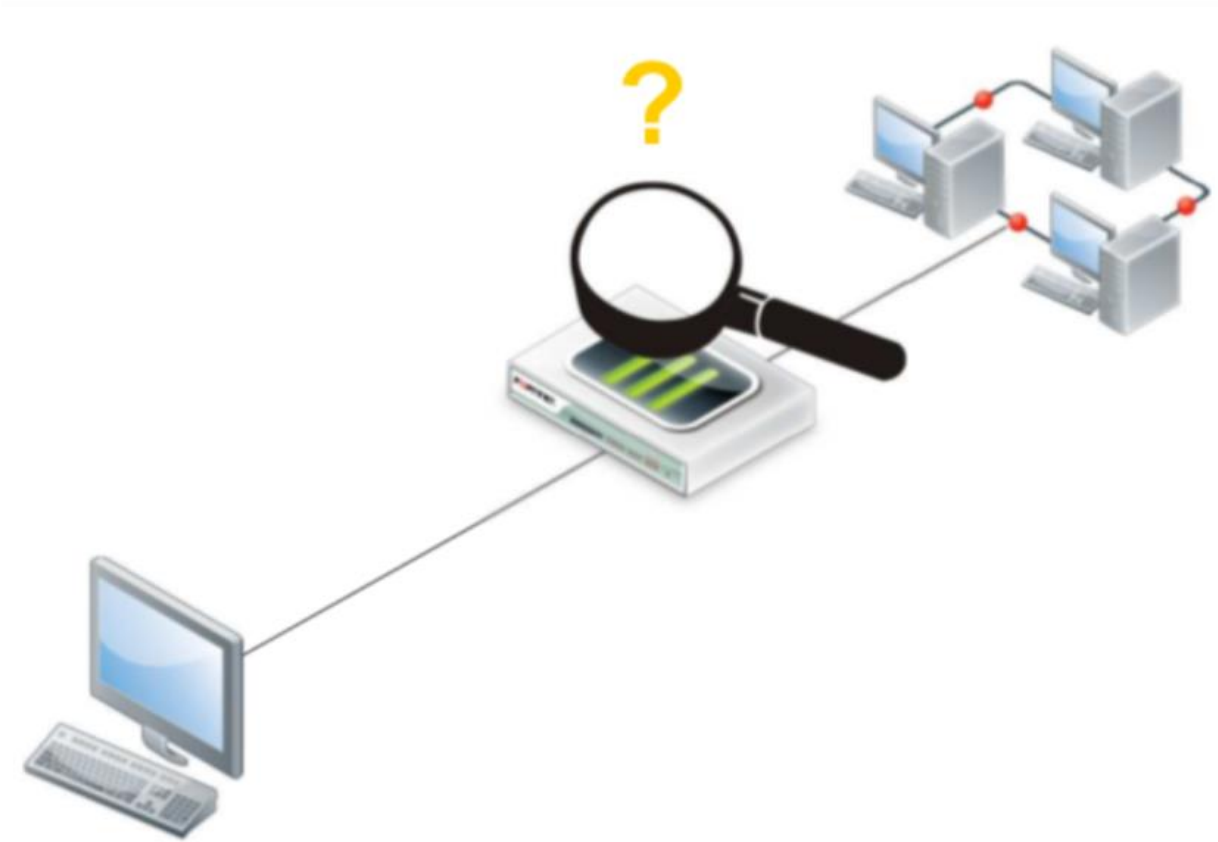
Bandwidth Consuming
- Freeware and Software Downloads
- File Sharing and Storage
- Streaming Media and Download
- Peer-to-peer File Sharing
- Internet Radio and TV
- Internet Telephony

Potentially Liable
- Drug Abuse
- Hacking
- Illegal or Unethical
- Discrimination
- Explicit Violence
- Extremist Groups
- Proxy Avoidance
- Plagiarism
- Child Abuse

http://www.fortiguard.com/static/webfiltering.html

Taller 3. Conectividad

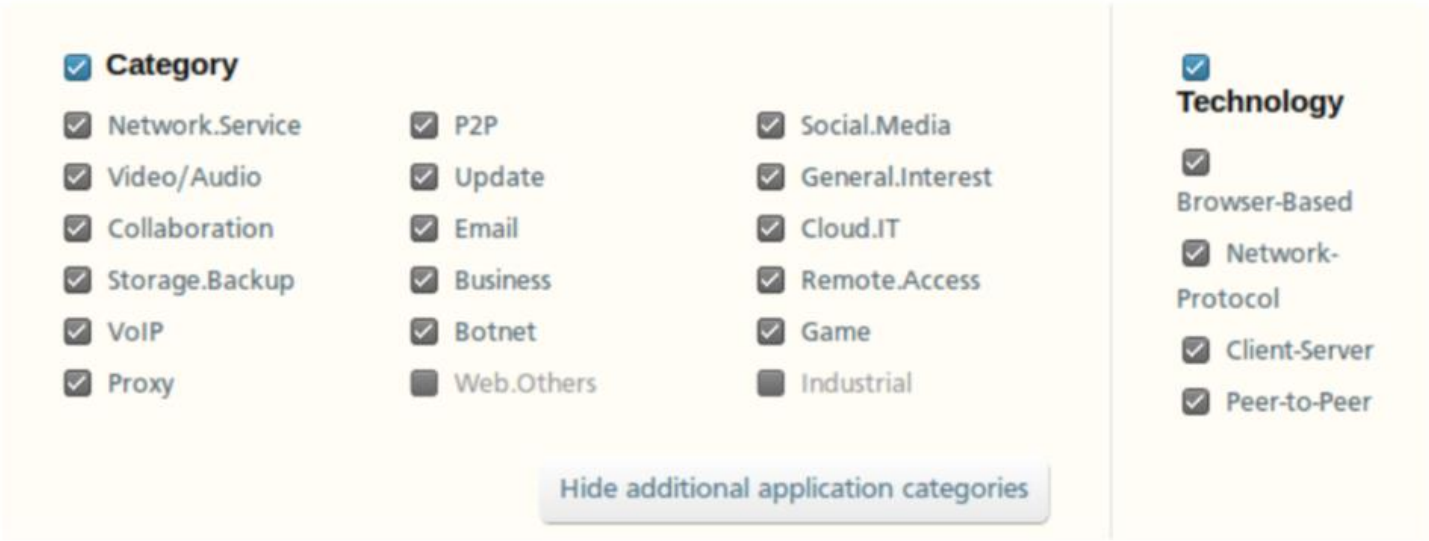
CONTROL DE APLICACIONES



Taller 3. Conectividad

CONTROL DE APLICACIONES

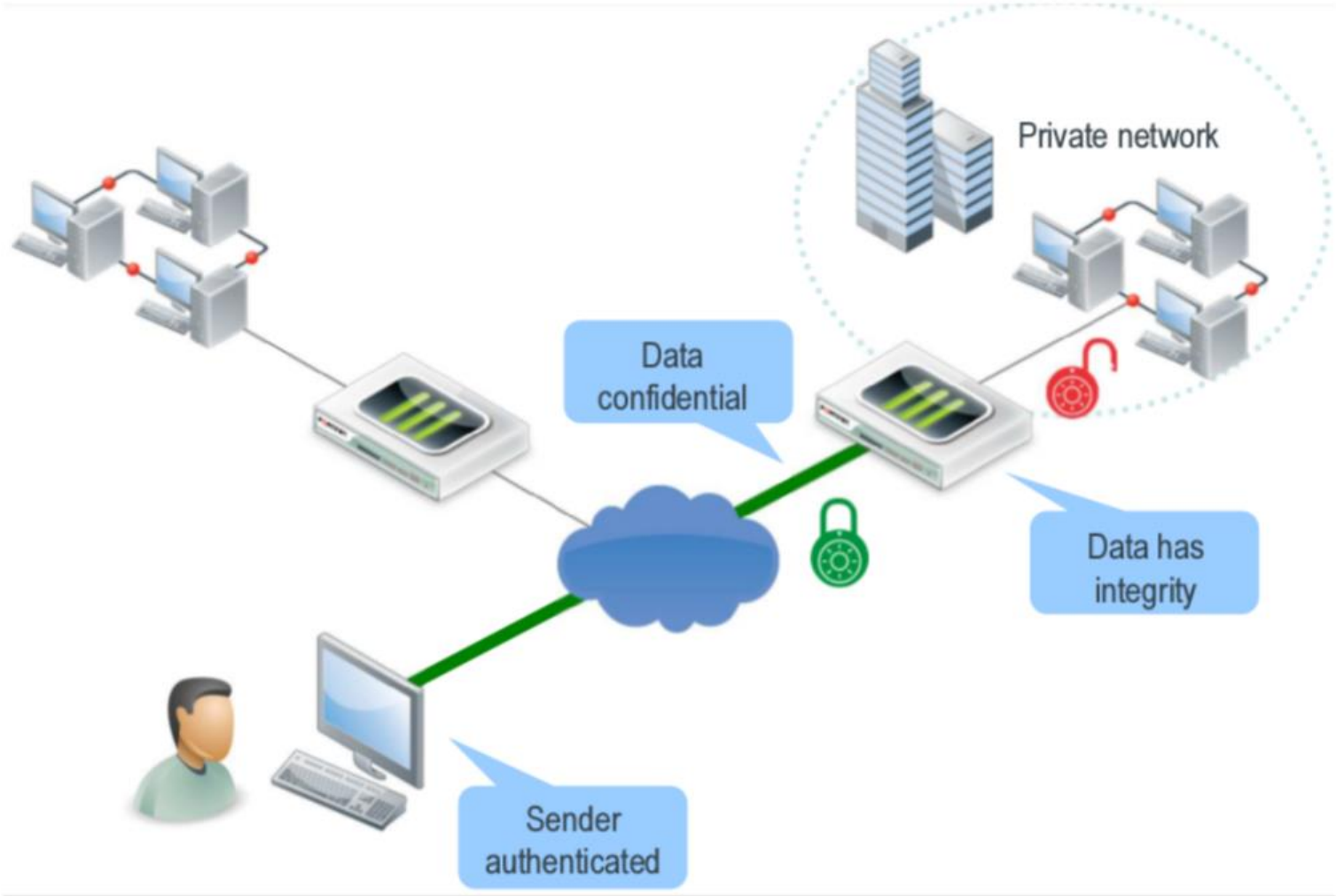
- Bloqueo de aplicaciones basado en tipos de aplicaciones



http://www.fortiguard.com/encyclopedia/applications/

Taller 3. Conectividad

REDES PRIVADAS VIRTUALES



REDES PRIVADAS VIRTUALES

VPN

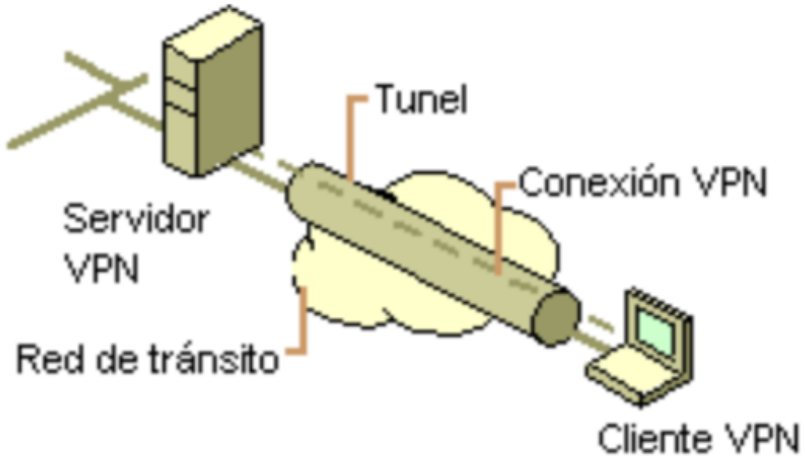
- Red privada y segura sobre red pública y no segura.
- Proporciona un túnel IP cifrado y/o encapsulado a través de internet.

REDES PRIVADAS VIRTUALES

Tipos de VPN

VPN de Cliente:

- El cliente se conecta remotamente a una LAN.
- Se usa PPP para establecer una conexión entre el cliente y la LAN.

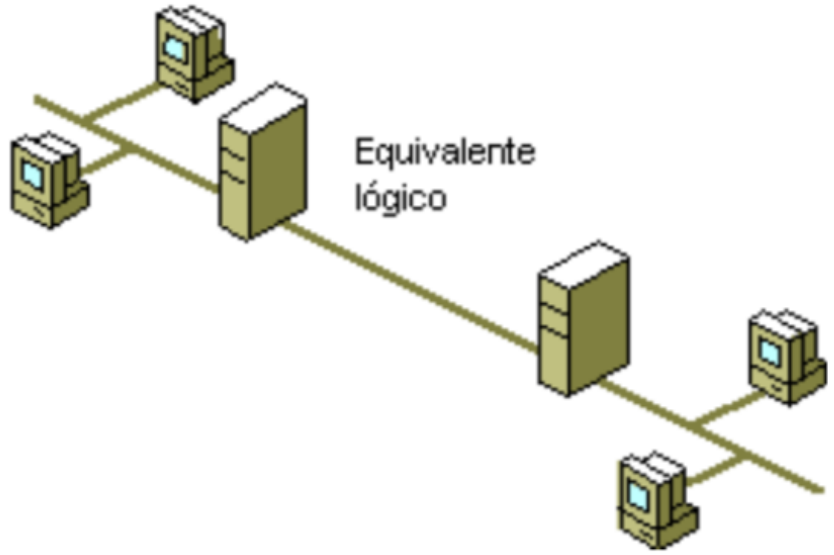


REDES PRIVADAS VIRTUALES

Tipos de VPN

VPN de LAN a LAN:

- Se encapsula el tráfico de una red local.
- Nos ahorramos el paso PPP (las tramas se encapsulan directamente).



MUCHAS GRACIAS

¿Preguntas?

Gracias!!

David Romero Trejo
www.davidromerotrejo.com
drt@davidromerotrejo.com

PROGRAMA DE FORMACIÓN

Transformación digital e Industria 4.0

Fondo Social Europeo
Una manera de hacer Europa

EXTREMADURA EMPRESARIAL

Unión Europea

JUNTA DE EXTREMADURA

Taller 3.
Conectividad
Protección de datos personales

Índice

Introducción al Programa formativo

- Es un Programa formativo que pone en marcha la **Dirección General de Empresa y Competitividad de Consejería de Economía, Ciencia y Agenda Digital de la Junta Extremadura,** con el fin de fortalecer las competencias, habilidades y conocimientos de empresarios, directivos y mandos intermedios de empresas, para promover su crecimiento profesional y la adaptación a la industria conectada de sus organizaciones

- El programa está cofinanciado por el **Fondo Social Europeo (80%)** y la **Comunidad Autónoma de Extremadura (20%),** al estar enmarcado dentro de las actuaciones del **Programa Operativo FSE 2014-2020**

Introducción al Programa formativo

TALLER 1: AUTOMATIZACIÓN DE LA INDUSTRIA.

Sensorización, Monitorización, Sisitemas Ciberfisicos, Robotica, Fab. Aditiva, Impresión 3D…

Fechas: 21, 22, 23, 24 y 28 de octubre. Horario de 16 a 20h.

TALLER 2: DATOS DIGITALES.

Big Data. Analítica y Métricas de Infomación digital, Inteligencia Artificial…

Fechas: Del 29, 30 de octubre, 4, 5 y 6 de noviembre. Horario de 16 a 20h.

TALLER 3: CONECTIVIDAD.

Internet de las cosas, Cloud, Ciberseguridad, Infraestructuras tecnológicas, Protección de Datos…

Fechas: Del 11, 12, 13, 14 y 18 de noviembre. Horario de 16 a 20h.

TALLER 4: APLICACIONES Y SOLUCIONES DE CLIENTE.

Realidad virtual y aumentada, Wearables, Apps, Redes sociales y Softwares (ERP, CRM , MES…)

Fechas: Del 20, 21, 25, 26, y 27 de noviembre. Horario de 16 a 20h.

Objetivos, Beneficiarios y Competencias asociadas

Objetivo General

- Presentar, de forma dinámica, los diferentes modelos de estrategia para la gestión de la empresa conectada y las tecnologías habilitadoras que intervienen en la industria 4.0 para poder incrementar el valor añadido industrial y el empleo cualificado del tejido empresarial de la región

¿Á quién va dirigido el programa?

- Empresarios, directivos, mandos intermedios y técnicos especialistas de todas las empresas extremeñas, especialmente las que desarrollen su actividad, directa o indirectamente, en el sector industrial
- Profesionales del ámbito de la consultoría que integren entre sus áreas de trabajo promover el desarrollo de la industria 4.0

Objetivos, Beneficiarios y Competencias asociadas

ESTE TALLER

TALLER 3: CONECTIVIDAD.

Contenidos: Conoceremos y aprenderemos los usos y funcionalidades de tecnologías, herramientas y equipamiento que permiten el flujo de la información y los datos en una sociedad e industrias hiperconectadas, y entenderemos el nuevo paso y los nuevos retos que nos ofrecen la industria 4.0 a través de sistemas ciberfísicos donde todo está conectado.

Introducción a la protección de datos personales

Disposiciones generales

Objeto

Protección de las personas físicas en el tratamiento de sus datos personales y normas libre circulación de tales datos.

Protege derechos y libertades fundamentales de las personas físicas (Dª protección datos personales)

Disposiciones generales

Ámbito de aplicación material

Normativa aplica al tratamiento total o parcial automatizado o no, de datos personales incluidos en un fichero.

No se aplica en actividades exclusivamente personales o domésticas.

Disposiciones generales

Ámbito de aplicación territorial

Normativa aplica actividades de un RT o ET de la UE

Normativa aplica al tratamiento de datos de personas residentes en UE (oferta de bienes y servicios; control de su comportamiento)

Disposiciones generales

Definiciones

Datos personales

Tratamiento

Limitación del tratamiento

Elaboración de perfiles

Seudonimización

Disposiciones generales

Definiciones

Fichero

Responsable del tratamiento

Encargado del tratamiento

Destinatario

Consentimiento del interesado (manifestación libre, especifica, informada e inequívoca)

Disposiciones generales

Definiciones

Violación de la seguridad de los datos personales

Datos genéticos

Datos biométricos

Datos relativos a salud

Establecimiento principal (RT o ET)

Principios jurídicos

Principios relativos al tratamiento

Lícito, leal, transparente

Fines determinados, explícitos y legítimos (tratamiento ulterior)

Adecuados, pertinentes y limitados en relación con los fines (minimización)

Exactos y actualizados

Mantenidos no más tiempo del necesario para los fines establecidos

Principios jurídicos

Principios relativos al tratamiento

Mantenidos no más tiempo del necesario para los fines establecidos

Tratados garantizando una seguridad adecuada

El RT será responsable del cumplimiento de todo lo anterior y capaz de demostrarlo (Responsabilidad proactiva)

Principios jurídicos

Licitud del tratamiento

Sólo será lícito si:

Consentimiento, Contrato, Obligación legal del RT, Intereses vitales, Interés público, Intereses legítimos

Principios jurídicos

Condiciones para el consentimiento

RT tiene que demostrar en todo momento el consentimiento del interesado

Inteligible, granulado, separado de otras finalidades, claro, sencillo

Se podrá retirar en cualquier momento no afectando al prestado hasta el momento

Ojo con consentimiento en contratos (libertad)

Principios jurídicos

Tratamiento de categorías especiales de datos personales

Están prohibidos (étnico, racial, política, religión, filosóficas, sindical, genéticos, biométricos, salud, sexual)

Excepto: consentimiento explícito; obligaciones del RT (laboral, seguridad social, convenio colectivo, etc.); intereses vitales, fundación o asociación con esas finalidades; sean públicos; interés público; reclamaciones, ttribunales, etc.

Principios jurídicos

Tratamiento de datos personales relativos a condenas e infracciones penales

Derechos del interesado

Información y acceso a los datos personales

Información a facilitar cuando los datos personales se obtengan del interesado:

(identidad; contacto RT; DPO; Fines; Base jurídica; IL; Destinatarios; TID; plazo conservación; derechos; oposición; reclamación ante autoridad; decisiones automatizadas; tratamiento ulterior).

Derechos del interesado

Información y acceso a los datos personales

Información a facilitar cuando no se obtengan del interesado: (identidad contacto RT; DPO; Fines; Base jurídica; Destinatarios; TID; plazo conservación; IL; derechos; oposición; reclamación ante autoridad; decisiones automatizadas; tratamiento ulterior).

Comunicar en el plazo de 1 mes desde que se recogen.

Derechos del interesado

Derecho de acceso del interesado

Derechos del interesado

Derecho de rectificación

Derechos del interesado

Derecho de supresión (derecho al olvido)

Derechos del interesado

Derecho a la limitación del tratamiento

Derechos del interesado

Derecho a la portabilidad de los datos

Derechos del interesado

Derecho de oposición

Derechos del interesado

Decisiones individuales automatizadas, incluida la elaboración de perfiles

Derechos del interesado

Limitaciones al tratamiento

Responsable y encargado del tratamiento

Obligaciones generales

Aplicar medidas técnicas y organizativas apropiadas en base a los datos tratados, fines, contexto, etc. (se revisarán y actualizarán)

Políticas de protección de datos

Códigos de conducta, mecanismos de certificación

Responsable y encargado del tratamiento

Obligaciones generales

Protección de datos desde el diseño y por defecto

Corresponsabilidad

Encargado de tratamiento (Contrato)(Outsourcing)

Registro de actividades de tratamiento

Responsable y encargado del tratamiento

Obligaciones generales

Seguridad del tratamiento (tener en cuenta factores)

Medidas: seudonimización, cifrado, anonimización…

Garantizar confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicio de tratamiento

Responsable y encargado del tratamiento

Obligaciones generales

Capacidad de restaurar la disponibilidad y acceso a datos personales rápidamente en caso de incidente

Procesos de verificación, evaluación y valoración regulares

Notificación violaciones de seguridad a la autoridad de control

Comunicación de violación de seguridad a interesados

Responsable y encargado del tratamiento

Obligaciones generales

Evaluación de Impacto relativa a la protección de datos personales

Consulta previa

Delegado de protección de datos: figura, designación, posición, funciones.

Códigos de conducta y certificación

Transferencias de datos personales a terceros países

Principio general

Prohibidas, salvo que se ajusten a la normativa:

- Basada en una decisión de adecuación (Comisión)
- Transferencias mediante garantías adecuadas (Instrumentos: PrivacySH)
- Normas corporativas vinculantes

Autoridades de control

Agencia Española de Protección de Datos

Agencia Vasca

Agencia Catalana

Oficina de Transparencia Andalucía

Sanciones

Hasta 10 millones o 2% volumen negocio
(Obligaciones de seguridad)

Hasta 20 millones o 4% volumen negocio
(Obligaciones jurídicas)

En resumen...

Elementos clave

- Análisis de tratamientos
- Registros de tratamientos
- EIP
- Modelos de datos
- Política de protección de datos
- Política de seguridad
- Revisión sitios web
- Control de proveedores
- Transferencias internacionales
- Formación
- Medidas de seguridad
- Evidencias

Resumen del Taller: ¿Qué hemos aprendido?

- Hemos conocido aspectos básicos e introductores en materia de protección de datos personales, así como las principales obligaciones de responsables y encargados de tratamiento

- Hemos entendido la importancia de detectar correctamente los tratamientos en las organizaciones y de garantizar el cumplimiento normativo, teniendo además la capacidad de poder demostrarlo

- Nos hemos introducido en las principales figuras de la materia así como los derechos que corresponden a interesados y las posibles sanciones por el incumplimiento de la normativa afectada

PROGRAMA DE FORMACIÓN

Transformación digital e Industria 4.0

Fondo Social Europeo
Una manera de hacer Europa

EXTREMADURA EMPRESARIAL

Unión Europea

JUNTA DE EXTREMADURA

Taller 3.
Conectividad

Taller 3. Conectividad

ÍNDICE

Taller 3. Conectividad

ÍNDICE

Taller 3. Conectividad

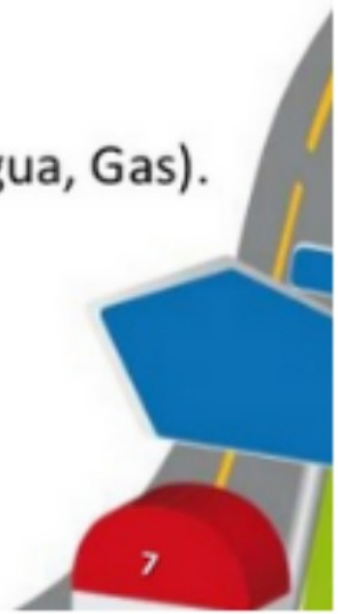
1.- Introducción

Taller 3. Conectividad

1.- Introducción

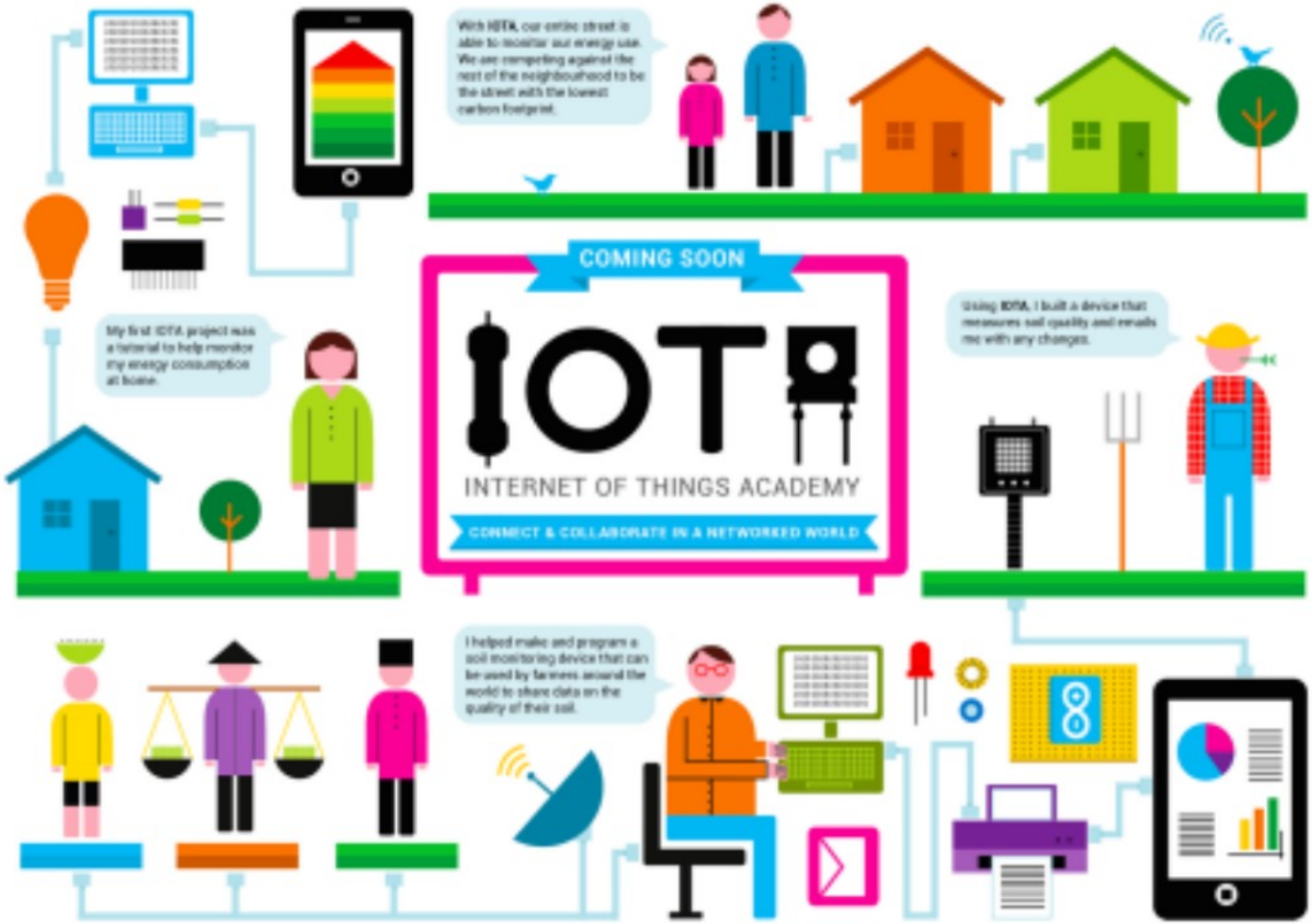
Qué deseamos conectar a Internet?

- Vehículos.
- Lugares.
- Sistemas de Señalización Vial.
- Alumbrado Publico.
- Aspersores.
- Contadores (Electricidad, Agua, Gas).
- Sombrillas.
- Los Baños.
- La cocina.
- Hasta las paredes!!!



Taller 3. Conectividad

1.- Introducción



Taller 3. Conectividad

1.- Introducción

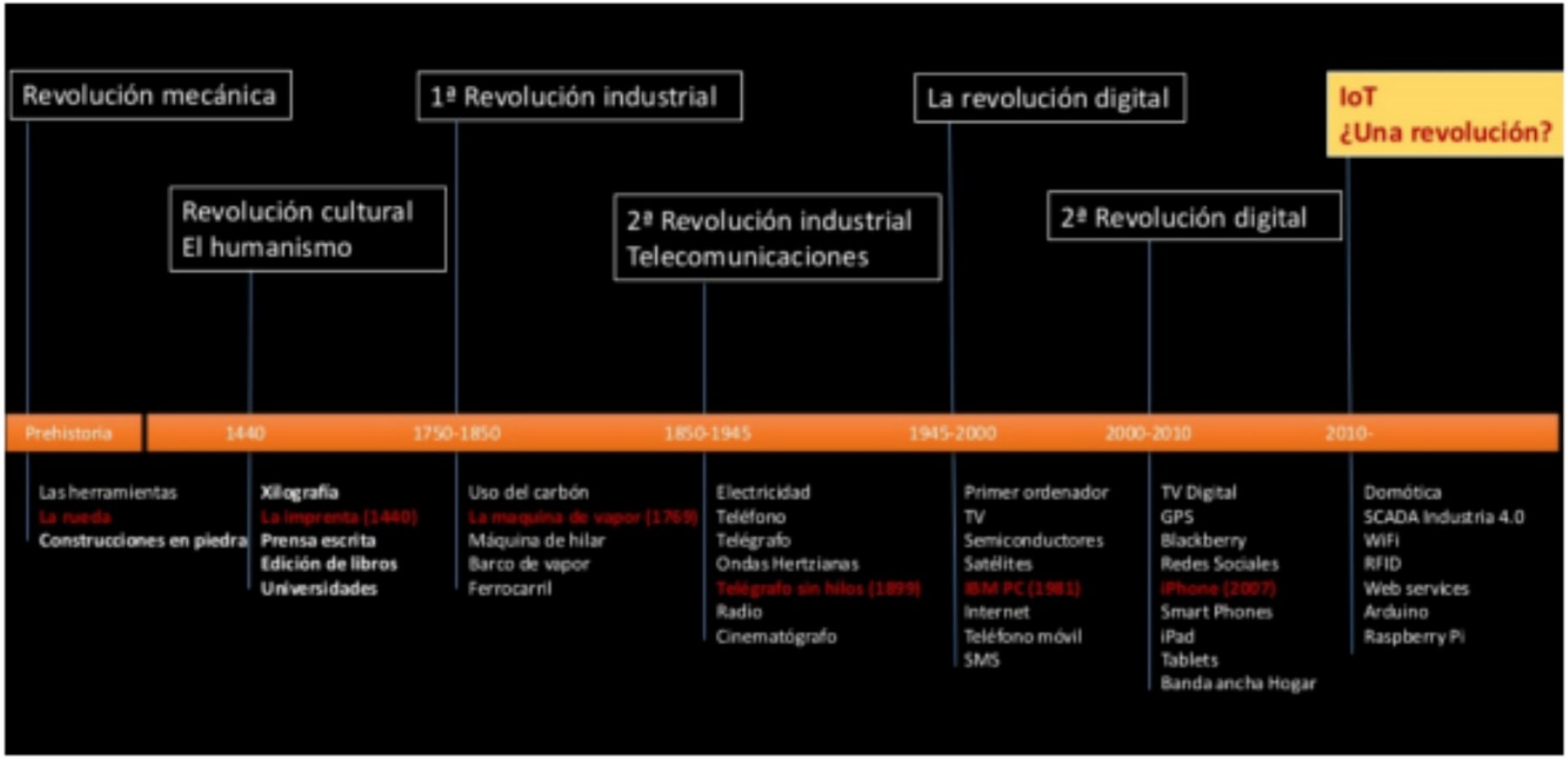
El concepto de "Internet of Things" fue acuñado por Kevin Ashton en 1999:

"If we had computers that knew everything there was to know about things — using data they gathered without any help from us — we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. ***The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so."***

Kevin Ashton, That 'Internet of Things' Thing, RFID Journal, July 22, 1999

Taller 3. Conectividad

1.- Introducción



Taller 3. Conectividad

1.- Introducción

Taller 3. Conectividad

2.- Concepto

Internet de las cosas (IoT) es algo conectado a una red, como puede ser internet, o a otras máquinas para que éstas trabajen con autonomía, sin necesitar la intervención humana

- **Se puede conectar…**
  - una vivienda
  - un coche
  - uno mismo
  - …el perro
- El término "nació" en algún punto entre 2008 y 2009, cuando habían más dispositivos conectados a Internet que personas en el mundo.
- En 2010, habían 6,8 mil millones de habitantes y 12,5 mil millones de artefactos con conexión web
- Se calcula que en 2020 al menos 50 mil millones de aparatos tendrán conexión a Internet, correspondiendo a 7,6 mil millones de habitantes

«Si una persona se conecta a la red, le cambia la vida. Pero si todas las cosas y objetos se conectan, es el mundo el que cambia»
(Hans Vestberg, CEO de Ericsson)

Taller 3. Conectividad

2.- Concepto

IEEE

"Una red de dispositivos – cada uno embebido con sensores – que se conectan a Internet"

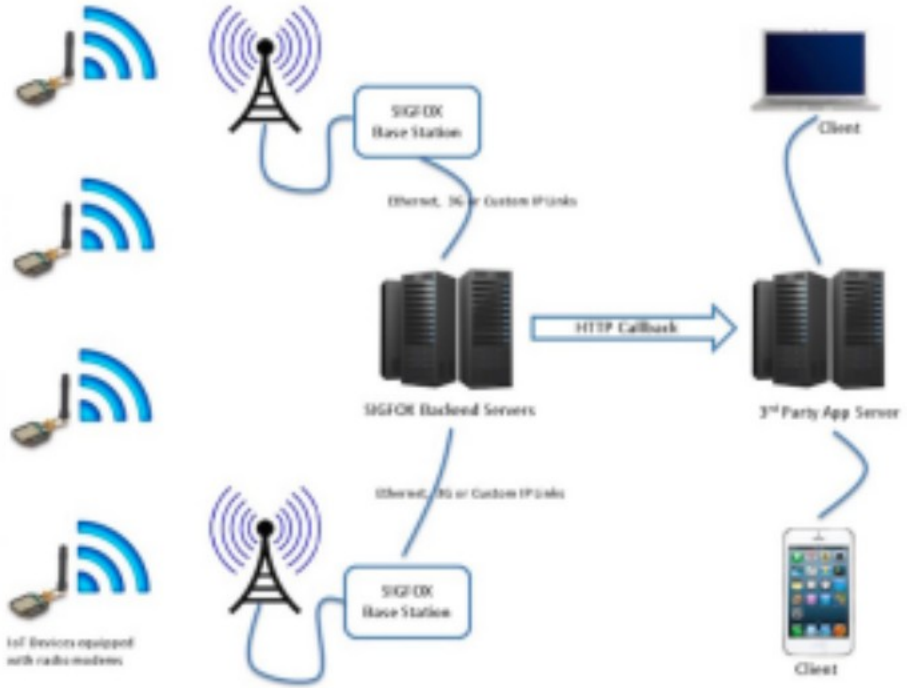
ITU

"Infraestructura mundial al servicio de la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión (física y virtual) de las cosas gracias al interfuncionamiento de tecnologías de la información y la comunicación (existentes y en evolución)".

Taller 3. Conectividad

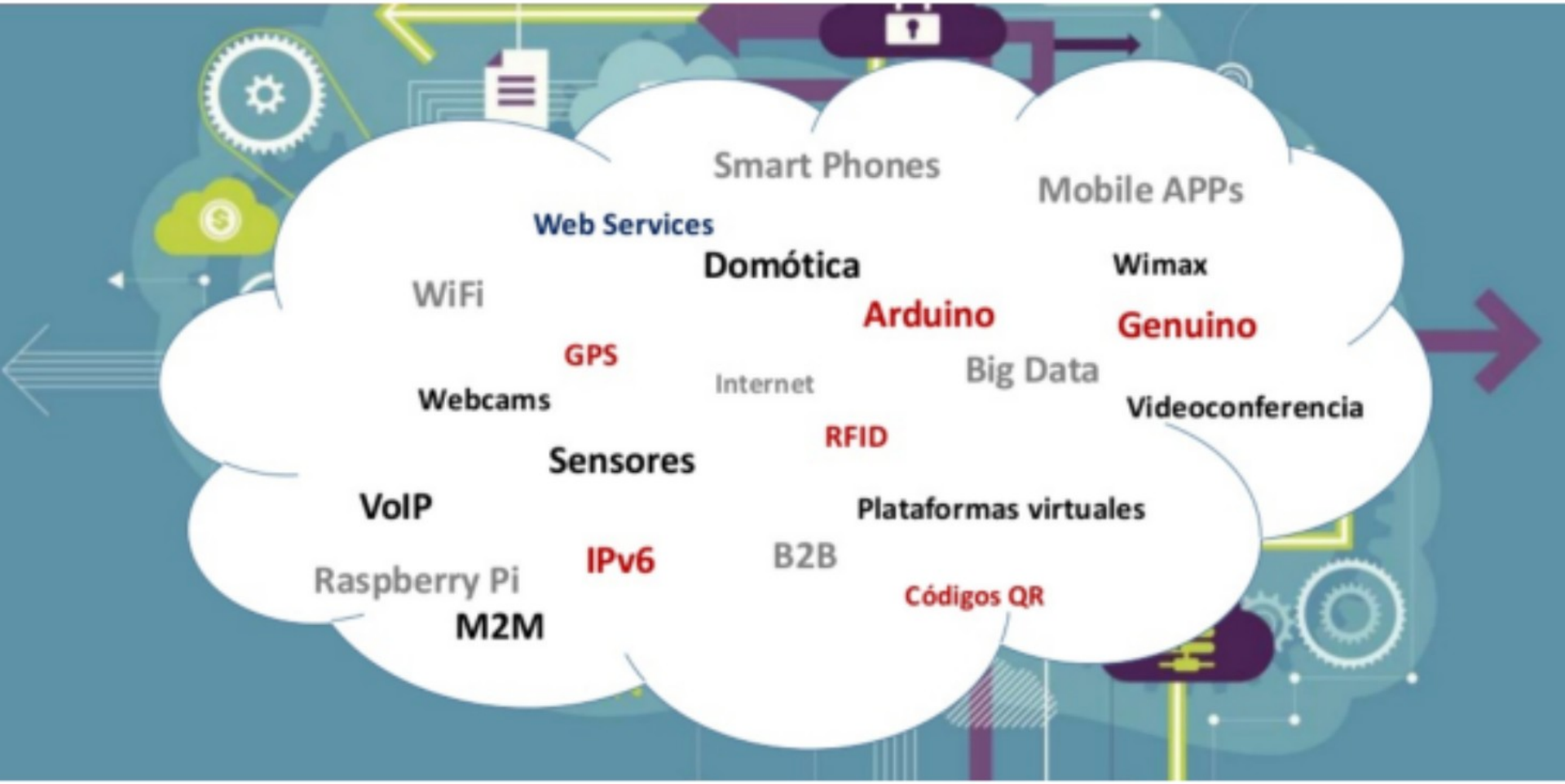
2.- Concepto

En definitiva, cuando hablamos de IoT, nos referimos a la capacidad de que cualquier cosa pueda conectarse a Internet para transmitir o recibir información.



Taller 3. Conectividad

2.- Concepto



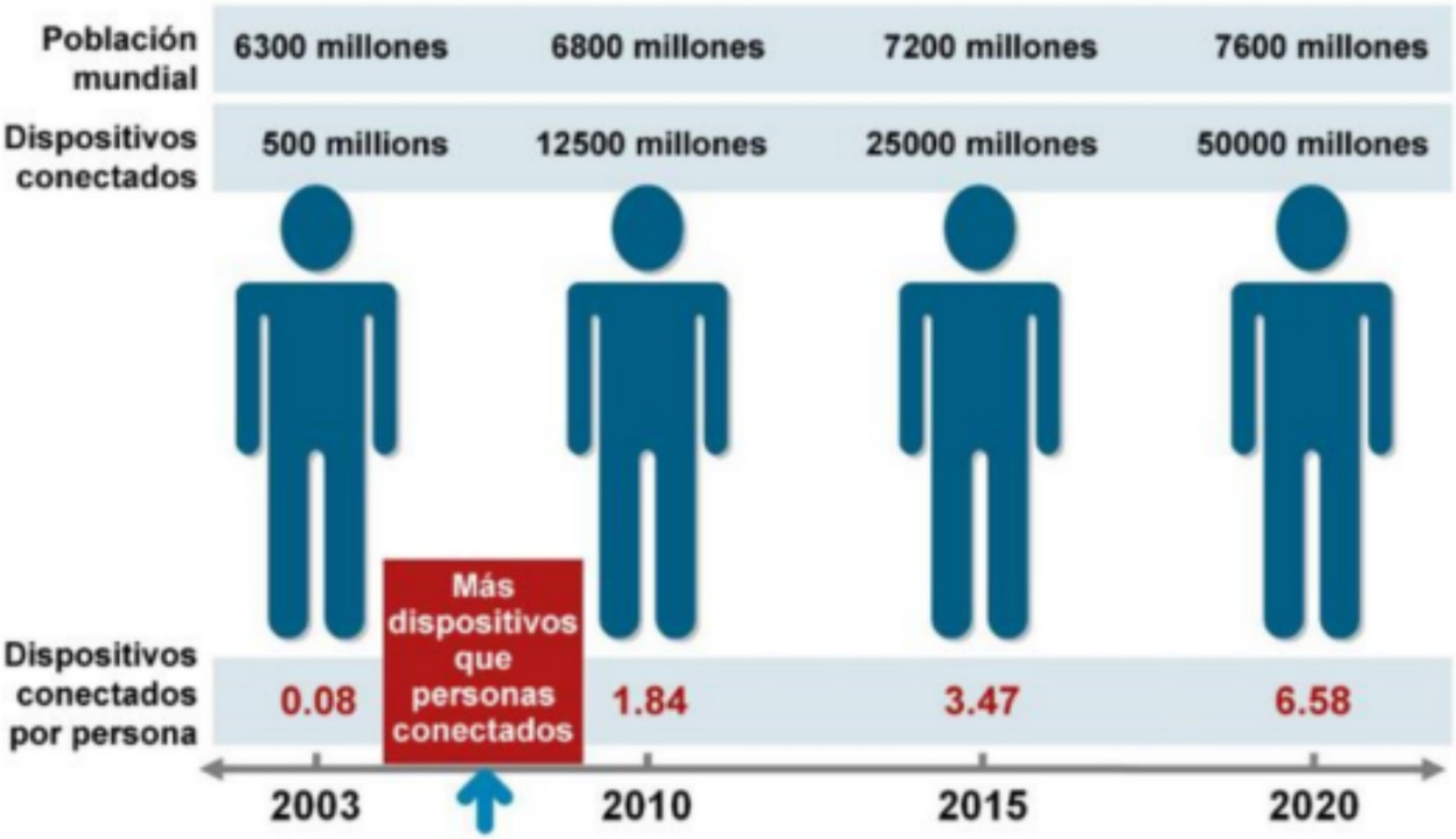
Taller 3. Conectividad

2.- Concepto

https://www.youtube.com/watch?v=542oTWpKPlE

Taller 3. Conectividad

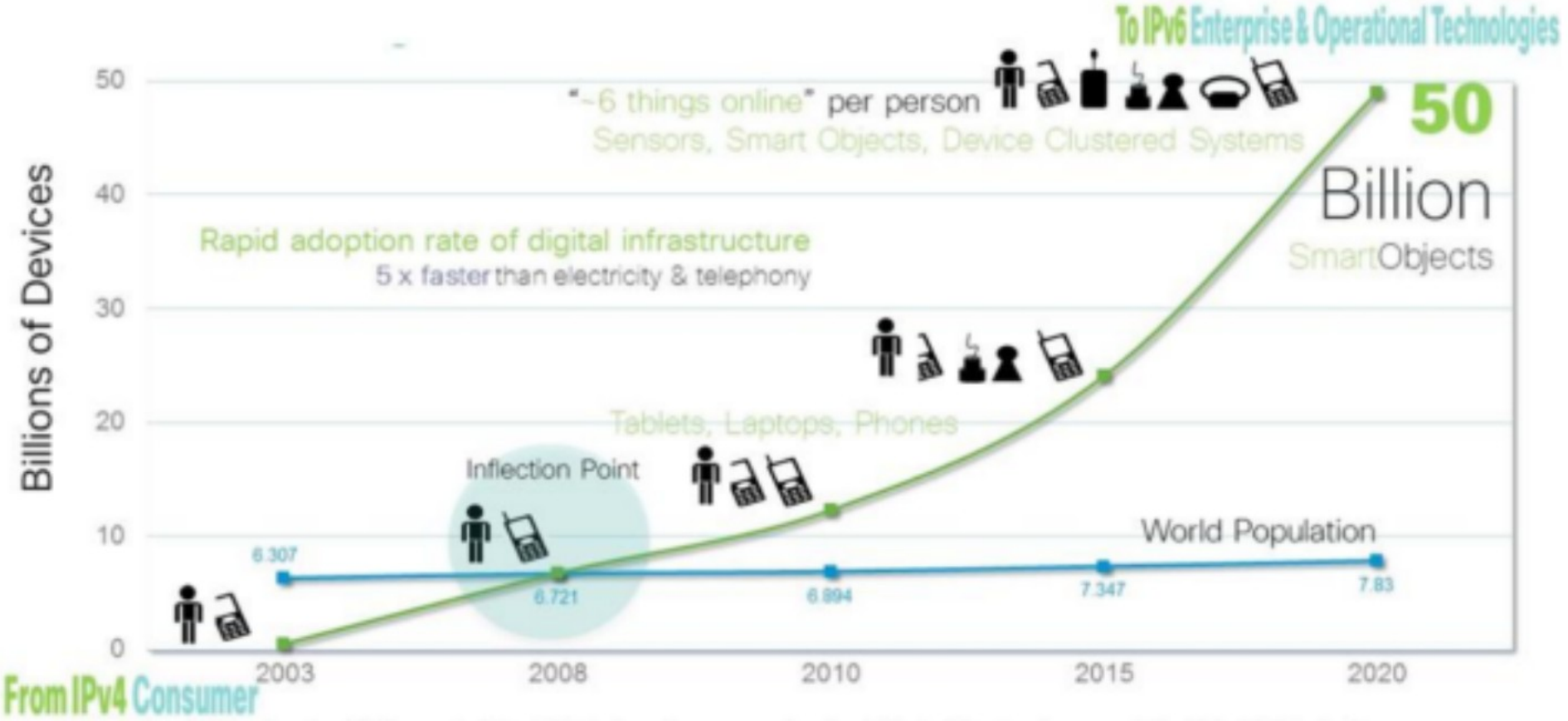
3.- IoT en números



Fuente: IBSG de Cisco

Taller 3. Conectividad

3.- IoT en números



Source: Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf

Taller 3. Conectividad

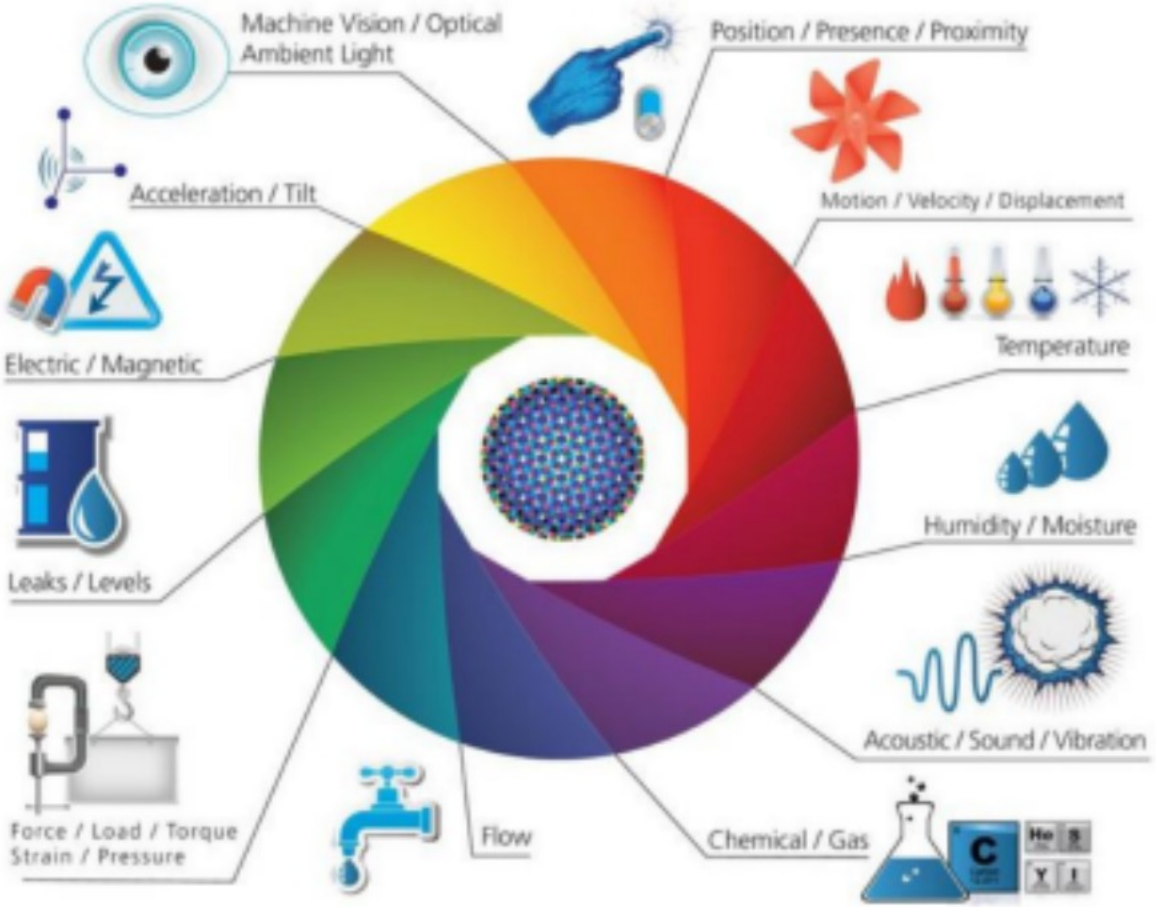
4.- Componentes

Componentes de IoT

Taller 3. Conectividad

4.- Componentes

Sensores



Taller 3. Conectividad

4.- Componentes

Tipos de sensores

Proximidad

Temperatura

Magnéticos

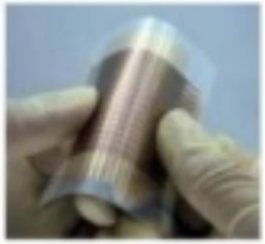
Sonido

Presión

Iluminación

Inclinación

Táctil, piel robótica



Microinterruptores

Taller 3. Conectividad

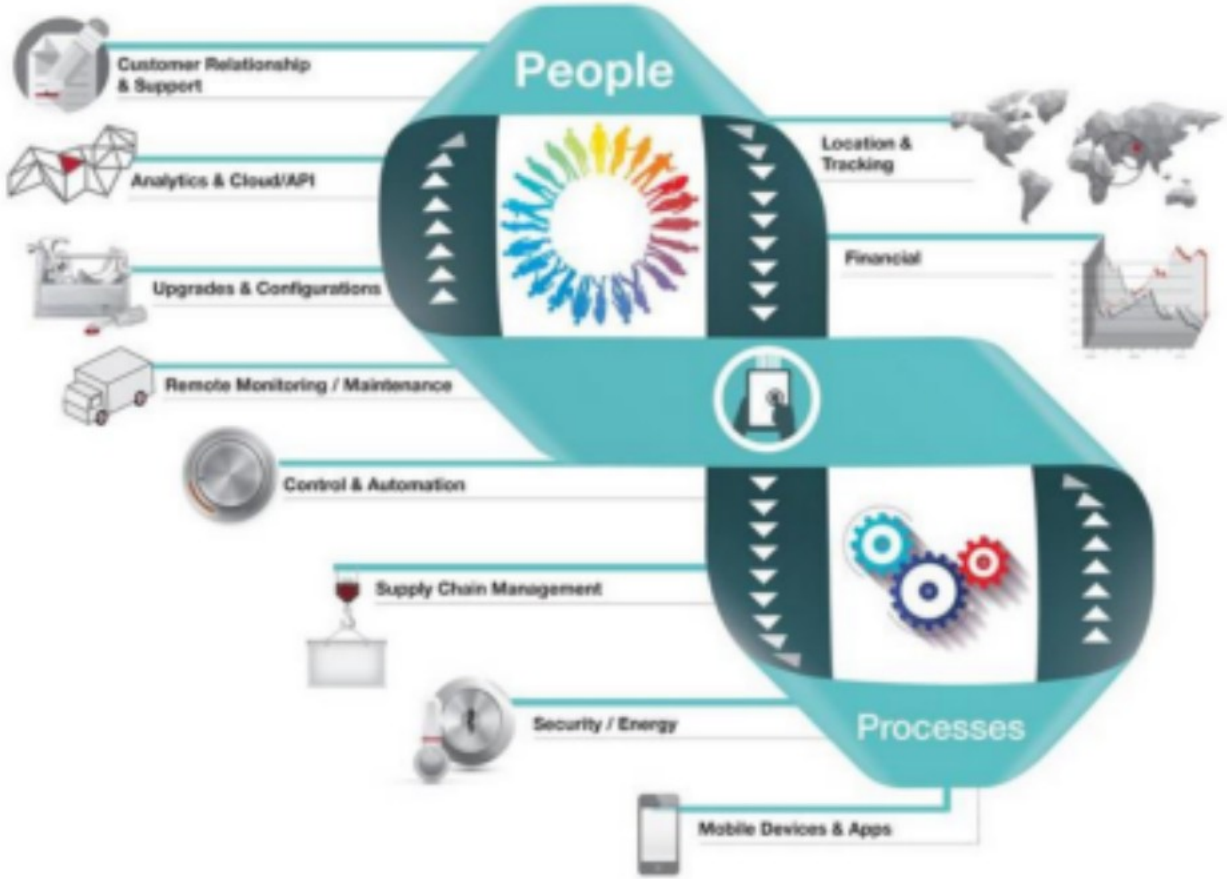
4.- Componentes

Conectividad

Taller 3. Conectividad

4.- Componentes

Personas y procesos

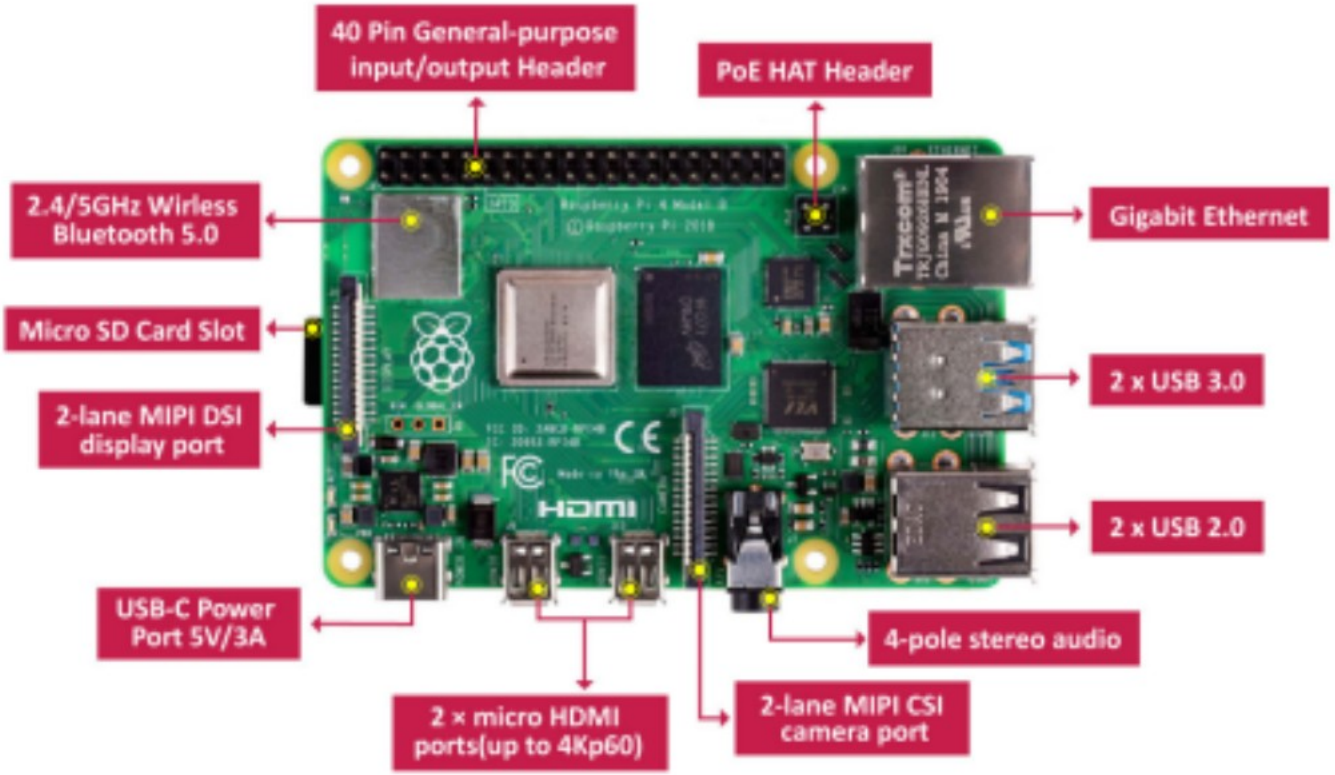


Taller 3. Conectividad

5.- Dispositivos y plataformas

Taller 3. Conectividad

5.- Para empezar...

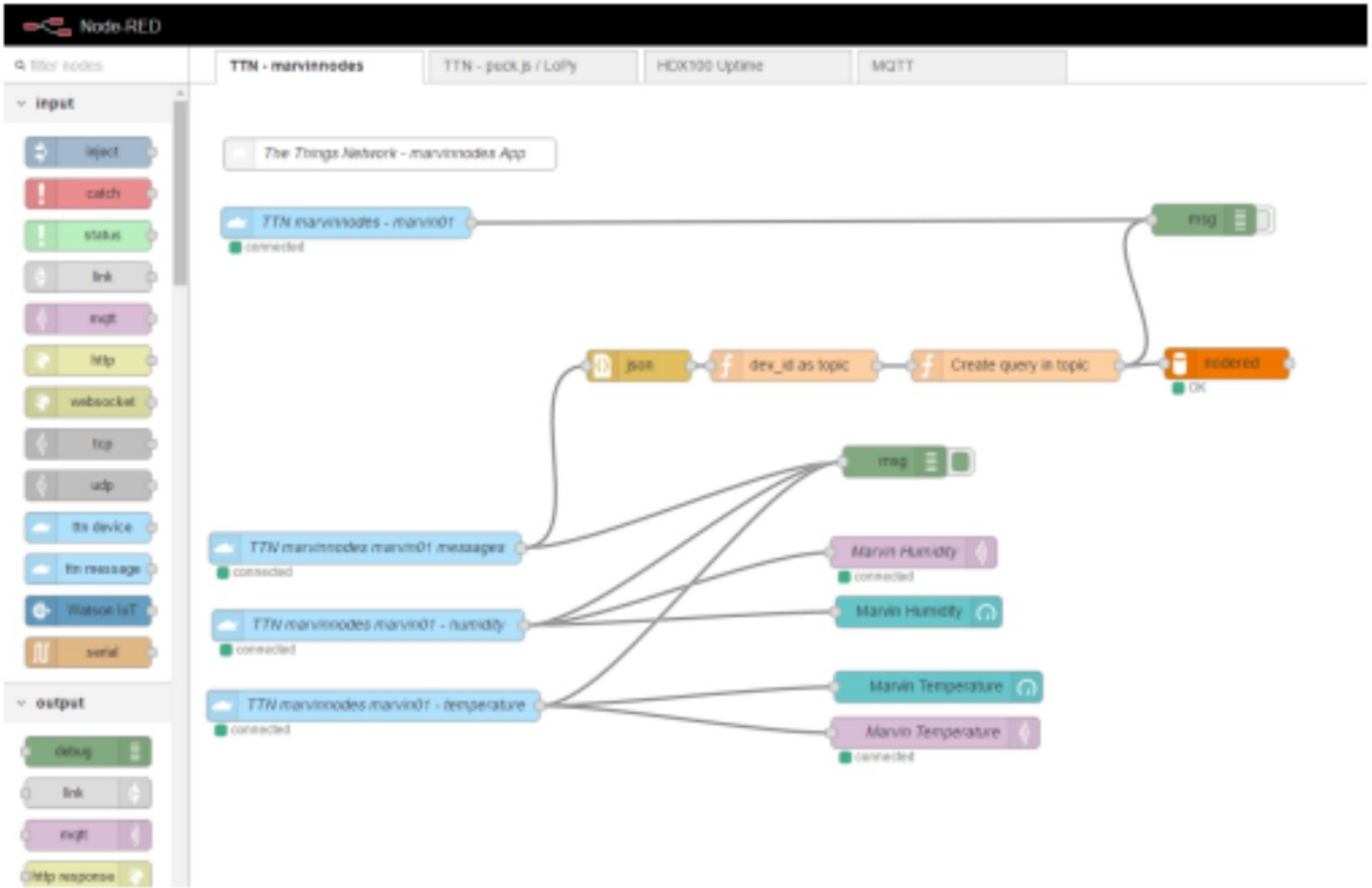


Taller 3. Conectividad

5.- Para empezar...

Taller 3. Conectividad

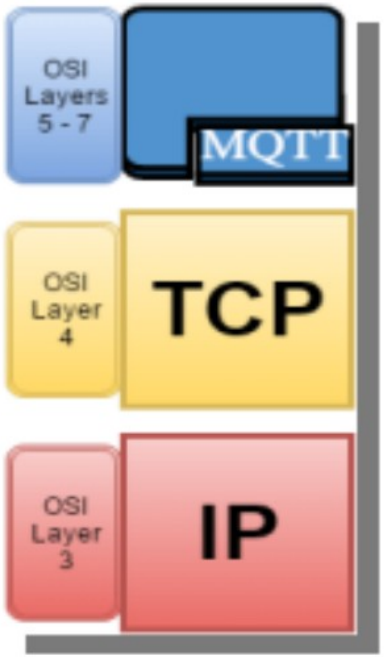
5.- Para empezar...



Taller 3. Conectividad

6.- Protocolo: MQTT

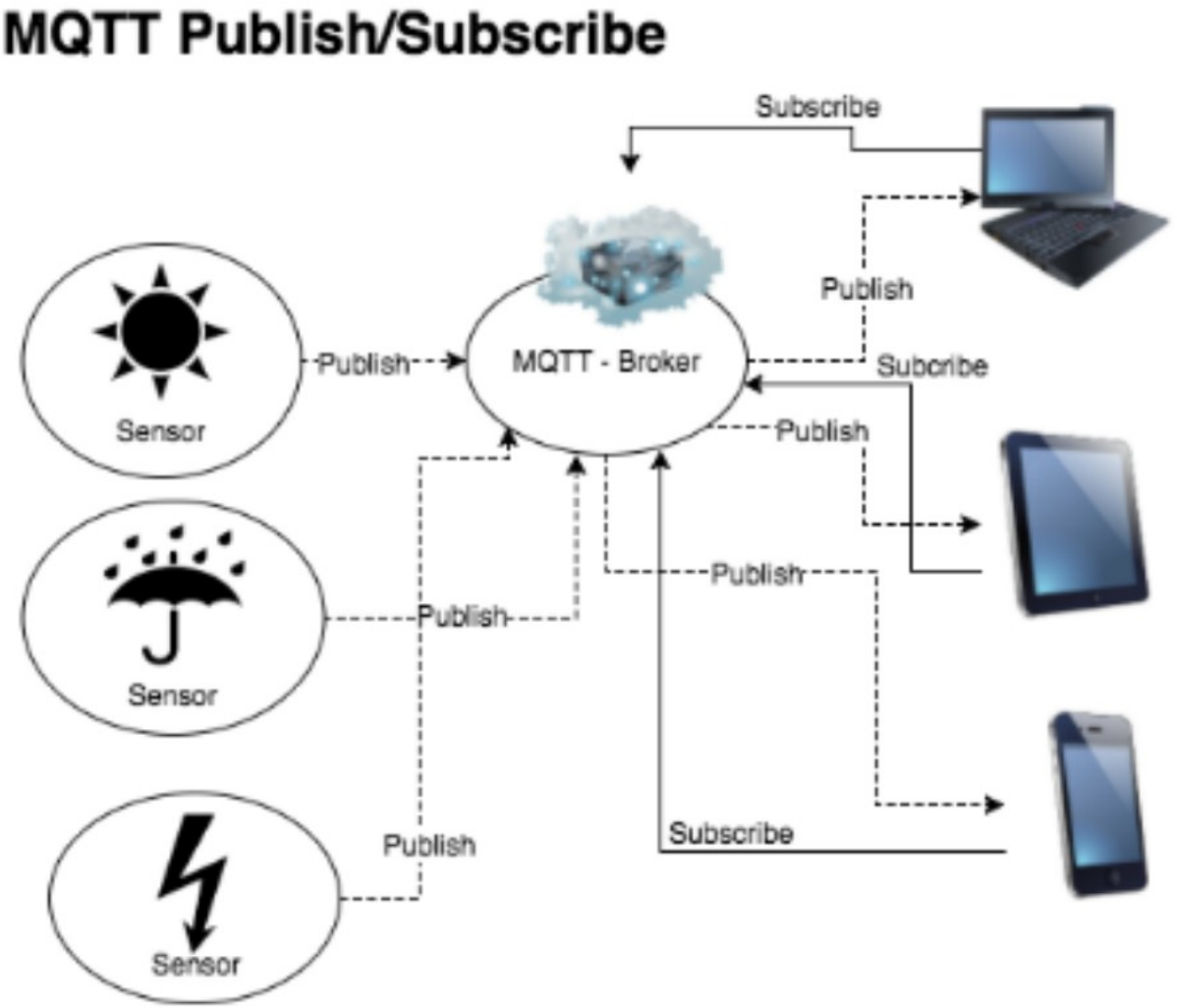
* Protocolo enfocado a la conectividad M2M (machine-to-machine).
* Se localiza en las capas superiores de OSI.
* Open-Source.
* Basado en una arquitectura suscriptor/publicador.
* Protocolo ligero.
* Ofrece ciertos mecanismos de QoS.



Taller 3. Conectividad

6.- Protocolo: MQTT

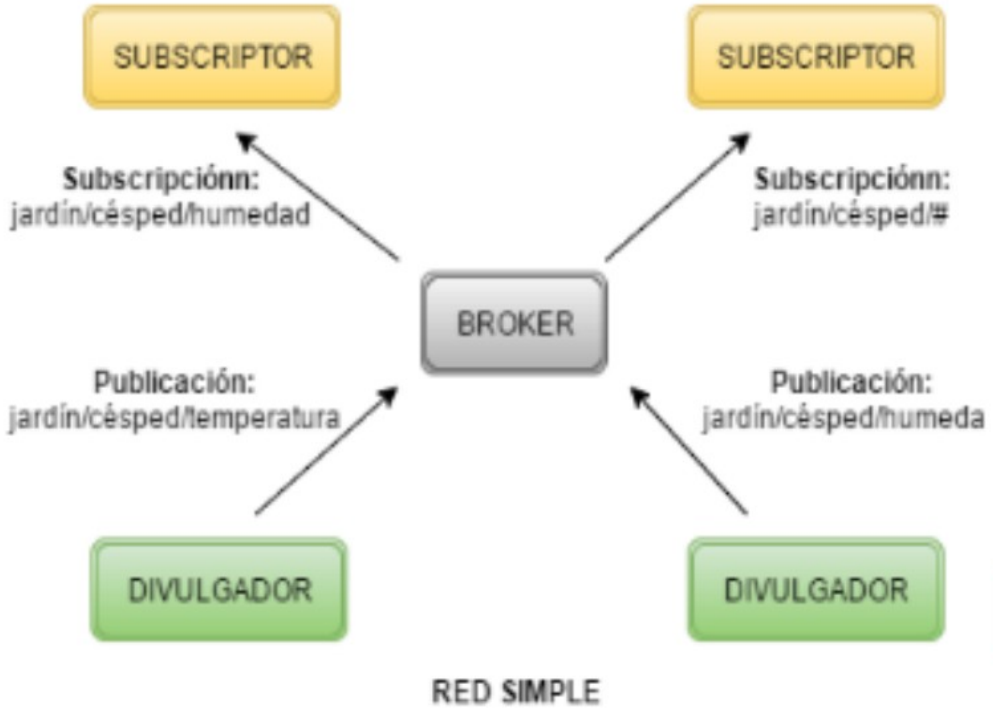
Arquitectura:



Taller 3. Conectividad

6.- Protocolo: MQTT

Elementos:

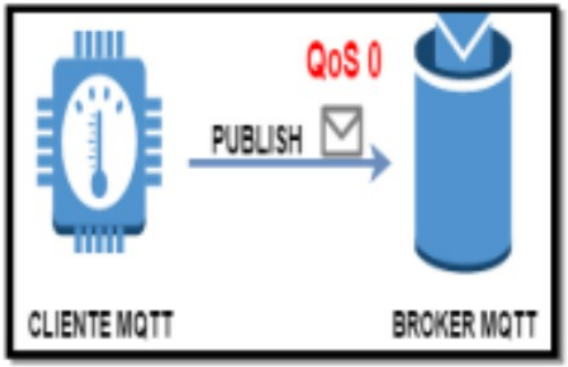


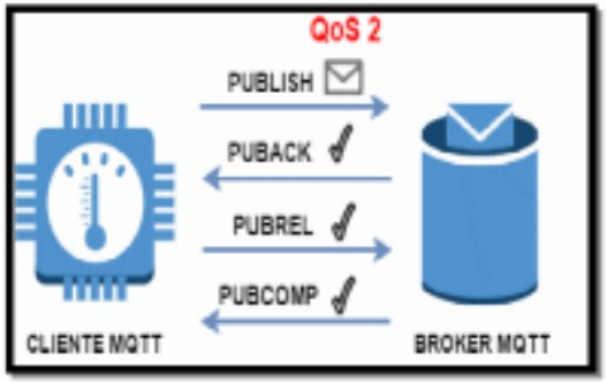
RED SIMPLE

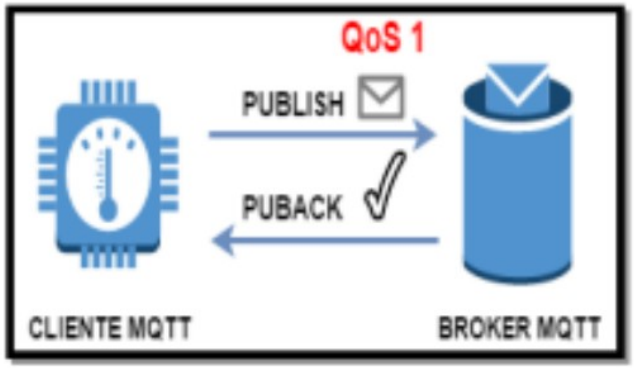
Taller 3. Conectividad

6.- Protocolo: MQTT

QoS:







Taller 3. Conectividad

6.- Protocolo: MQTT

QoS:

52	15.225956733	127.0.0.1	127.0.0.1	MQTT	103	Connect Command
54	15.227047720	127.0.0.1	127.0.0.1	MQTT	70	Connect Ack
56	15.227620816	127.0.0.1	127.0.0.1	MQTT	80	Subscribe Request (id=1) [prueba2]
57	15.227937247	127.0.0.1	127.0.0.1	MQTT	71	Subscribe Ack (id=1)
62	42.446106766	127.0.0.1	127.0.0.1	MQTT	103	Connect Command
64	42.447000922	127.0.0.1	127.0.0.1	MQTT	70	Connect Ack
66	42.447440648	127.0.0.1	127.0.0.1	MQTT	81	Publish Message [prueba2]
67	42.447646795	127.0.0.1	127.0.0.1	MQTT	68	Disconnect Req
68	42.447709610	127.0.0.1	127.0.0.1	MQTT	81	Publish Message [prueba2]

179	165.6173683…	127.0.0.1	127.0.0.1	MQTT	80	Subscribe Request (id=1) [prueba2]
180	165.6176306…	127.0.0.1	127.0.0.1	MQTT	71	Subscribe Ack (id=1)
185	169.6415131…	127.0.0.1	127.0.0.1	MQTT	103	Connect Command
187	169.6418952…	127.0.0.1	127.0.0.1	MQTT	70	Connect Ack
189	169.6423842…	127.0.0.1	127.0.0.1	MQTT	83	Publish Message (id=1) [prueba2]
190	169.6427548…	127.0.0.1	127.0.0.1	MQTT	70	Publish Ack (id=1)
191	169.6428733…	127.0.0.1	127.0.0.1	MQTT	83	Publish Message (id=1) [prueba2]
193	169.6431865…	127.0.0.1	127.0.0.1	MQTT	70	Publish Ack (id=1)
194	169.6434656…	127.0.0.1	127.0.0.1	MQTT	68	Disconnect Req

246	401.7544714…	127.0.0.1	127.0.0.1	MQTT	80	Subscribe Request (id=1) [prueba2]
247	401.7548162…	127.0.0.1	127.0.0.1	MQTT	71	Subscribe Ack (id=1)
252	407.7691486…	127.0.0.1	127.0.0.1	MQTT	103	Connect Command
254	407.7696581…	127.0.0.1	127.0.0.1	MQTT	70	Connect Ack
256	407.7701187…	127.0.0.1	127.0.0.1	MQTT	83	Publish Message (id=1) [prueba2]
257	407.7704039…	127.0.0.1	127.0.0.1	MQTT	70	Publish Received (id=1)
258	407.7705995…	127.0.0.1	127.0.0.1	MQTT	70	Publish Release (id=1)
259	407.7717012…	127.0.0.1	127.0.0.1	MQTT	70	Publish Complete (id=1)
260	407.7717485…	127.0.0.1	127.0.0.1	MQTT	83	Publish Message (id=1) [prueba2]
262	407.7718533…	127.0.0.1	127.0.0.1	MQTT	70	Publish Received (id=1)
263	407.7719262…	127.0.0.1	127.0.0.1	MQTT	68	Disconnect Req
265	407.7721394…	127.0.0.1	127.0.0.1	MQTT	70	Publish Release (id=1)
268	407.7729585…	127.0.0.1	127.0.0.1	MQTT	70	Publish Complete (id=1)

Taller 3. Conectividad

6.- Oportunidades y desafíos

Oportunidades

Taller 3. Conectividad

6.- Oportunidades y desafíos

Nuevos modelos de negocios

Taller 3. Conectividad

6.- Oportunidades y desafíos

Taller 3. Conectividad

6.- Oportunidades y desafíos

Algunas organizaciones trabajando

IEC Compliant International Electrotechnical Commission

oneM2M Global Standards for Machine to Machine & Internet of Things

ISO International Organization for Standardization

ITU International Telecommunication Union

W3C World Wide Web Consortium

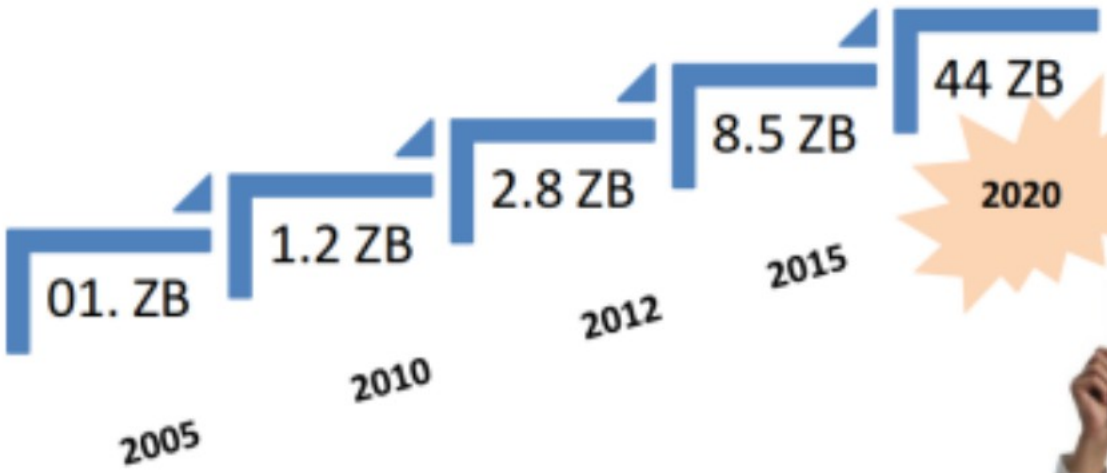
ETSI World Class Standards

ALLSEEN ALLIANCE

Taller 3. Conectividad

6.- Oportunidades y desafíos

Crecimiento del volúmen de información



Taller 3. Conectividad

6.- Oportunidades y desafíos

¿Cómo gestionamos esta información?

Taller 3. Conectividad

7.- Seguridad y privacidad

BBC | Sign in | News | Sport | Weather | Shop | Earth | M

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Art

Technology

Fridge sends spam emails as attack hits smart gadgets

17 January 2014 | Technology

PCWorld
Week. Life. Productivity.

NEWS | REVIEWS | HOW-TO | VIDEO | BUSINESS | LAPTOPS | TABLETS | PHONES | HARDWARE

Privacy | Encryption | Antivirus

18 Like 111 Tweet 8

Home / Security

Researchers show that IoT devices are not designed with security in mind

Taller 3. Conectividad

7.- Seguridad y privacidad

When 'Smart Homes' Get Hacked: I Haunted A Complete Stranger's House Via The Internet

24 comments, 10 called-out + Comment Now + Follow Comments

"I can see all of the devices in your home and I think I can control them," I said to Thomas Hatley, a complete stranger in Oregon who I had rudely awoken with an early phone call on a Thursday morning.

He and his wife were still in bed. Expressing surprise, he asked me to try to turn the master bedroom lights on and o
flipped the light switch with a cl
turn the television on as well.

"They just came on and now the

http://www.forbes.com/sites/k

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment

Technology

Web baby-monitoring cameras open to hacking, study warns

1 hour ago | Technology

Taller 3. Conectividad

7.- Seguridad y privacidad

BBC Sign in News Sport Weather Shop Earth

NEWS

Home Video World UK Business Tech Science Magazine Entertainment

ADVERTISEMENT

Technology

Smartwatches have security flaws says HP

23 July 2015 | Technology

HOME FREE eNEWSLETTER CONTACT US ADVERTISE WITH US

IoT EVOLUTION

M2M DRONE FOG SMART & CONNECTED EVENTS

M2M FEATURE NEWS

WeMo Vulnerabilities Latest Example of IoT Security Risks

By Rachel Ramsey / February 19, 2014

El Confidencial

'Hackers' chinos logran vulnerar la seguridad del coche Tesla

La firma de seguridad Qihoo 360 ha confirmado el primer 'hackeo' del Tesla Model S. Los asaltantes controlaron el cierre de las puertas y luces a distancia

Taller 3. Conectividad

7.- Seguridad y privacidad

Taller 3. **Conectividad**

7.- Seguridad y Privacidad

¿Que hace a IoT tan diferente en términos de seguridad?

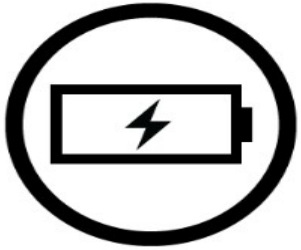
Longevidad

Tamaño del dispositivo

Información Personal

Mentalidad

Ser los Primeros En el Mercado



Eficiencia Energética

Dispositivos incapaces de Implementar seguridad

Taller 3. **Conectividad**

7.- Seguridad y Privacidad

Principales desafíos de privacidad en IoT

8.- Ejemplos de aplicación

8.- Ejemplos de aplicación

https://www.youtube.com/watch?v=ErpNpR3XYUw

Taller 3. **Conectividad**

8.- Ejemplos de aplicación

Nike+

https://www.youtube.com/watch?v=Ob8ElSkptCU

Taller 3. **Conectividad**

8.- Ejemplos de aplicación

Samsung Smart House

https://www.youtube.com/watch?v=_rhBfh-4aOs

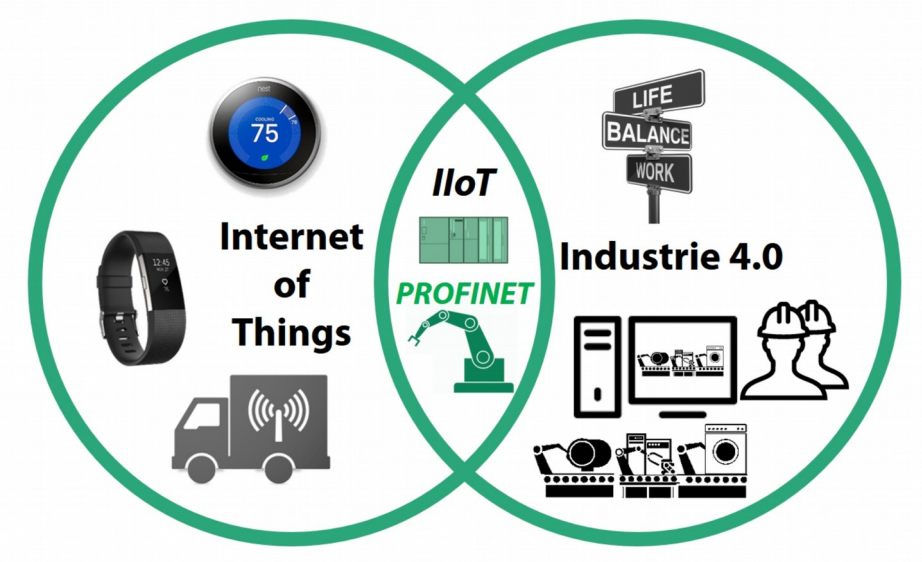
https://www.youtube.com/watch?v=Mcf7FQZifzg

Taller 3. Conectividad

9.- I-IoT

El **Internet de las Cosas** añade valor en uno o más de estos tres importantes aspectos: incrementando la eficiencia (de procesos, por ejemplo); mejorando la seguridad o beneficiando a la salud; creando mejores experiencias.

Pues bien, el **IIoT** es, por decirlo así, **un subconjunto del IoT eliminando todos los productos de consumo** (es decir, productos para aplicaciones domésticas, como un frigorífico conectado, una smart TV o los wearables), y centrándose tan solo en la parte de **incrementar la eficiencia de los procesos, la salud y la seguridad**. El IIoT se centra exclusivamente en las aplicaciones industriales, como la producción en cadena, la manufactura o los procesos de la industria agroalimentaria.



Taller 3. Conectividad

9.- I-IoT

https://youtu.be/QSIPNhOiMoE

https://youtu.be/Xvu92XAOeM0

Taller 3. Conectividad