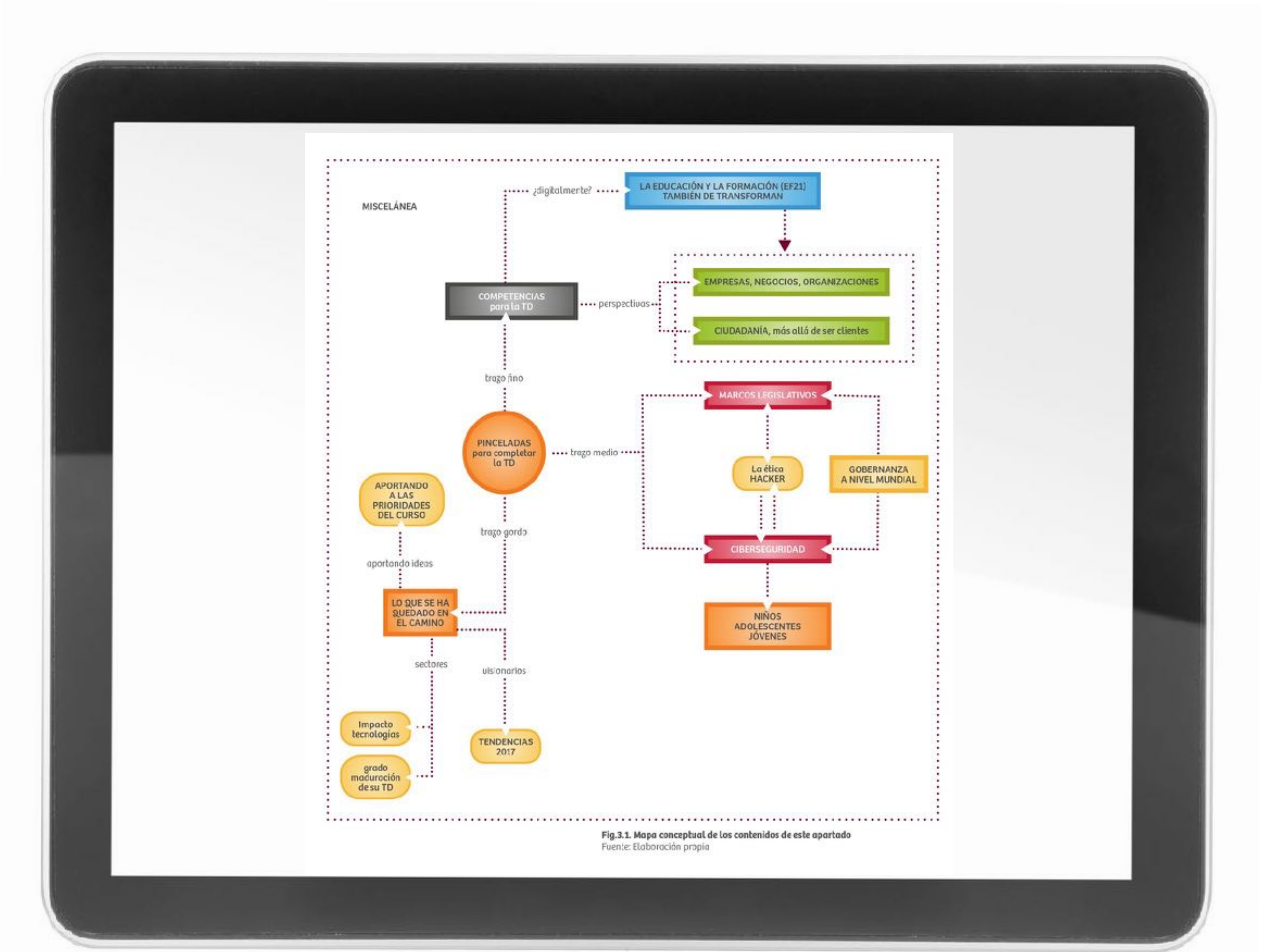


PINCELADAS PARA COMPLETAR LA INTRODUCCIÓN A LA TD

**PINCELADAS PARA COMPLETAR
LA INTRODUCCIÓN A LA TD**

El contenido de este último capítulo se sintetiza visualmente en el siguiente mapa conceptual.





En el mismo se abordan, a distintos grados de profundidad (trazo fino, medio y gordo) de más a menos -dentro de la brevedad que nos hemos impuesto- los temas que se han considerado que deben cerrar el módulo. Se trata de tres temas cuya priorización tiene sus propias razones: se considera esencial -si la TD va de personas más que de tecnología- tratar de las competencias que deben adquirir, desarrollar y adaptar las mismas, según la responsabilidad y uso que hacen de la misma los distintos segmentos de personas; a las mismas va asociada unos conocimientos básicos de legislación y de la ciberseguridad ante los ataques que se pueden sufrir en el espacio virtual; y, por último, de unos aspectos que no están incluidos en el diseño (ya que había que priorizar y seleccionar) de este curso, sea cual fuere el nivel en que se aborde el aprendizaje.



3

**PINCELADAS PARA
COMPLETAR LA
INTRODUCCIÓN A LA TD**

3.1

**COMPETENCIAS
NECESARIAS PARA LA
TD**

La TD va de personas, luego de tecnología. Las personas son la clave de la transformación no el software. Estas son frases y conceptos repetidos en capítulos anteriores de este módulo, y que a menudo se reflejan en los medios de comunicación. En relación con las personas y la TD hay, al menos, dos aspectos a considerar:

- a) capacitarlas digitalmente.
- b) orientar la TD para cambiar y mejorar la sociedad, mediante el uso de la Innovación Social, con las TIC como palanca. Este segundo aspecto, muy importante, no se aborda en este curso.





Por lo tanto, nos centramos en la capacitación o habilitación de las personas para la TD, a través de la educación y formación. Se suele utilizar una hipérbole para caracterizar la nueva situación: “educación y formación para el siglo 21 (EF21)”. Sea cual fuere la forma de denominarla, lo cierto es que la capacitación para la TD es una parte incluida en la necesidad de su habilitación para la nueva sociedad posindustrial y el nuevo entorno VUCA.

El apartado aborda este aspecto de las necesidades de EF21, partiendo de lo más general al caso específico de este curso: la TD de empresas, negocios, u organizaciones.

3

**PINCELADAS PARA
COMPLETAR LA
INTRODUCCIÓN A LA TD**

3.1

**COMPETENCIAS
NECESARIAS PARA LA
TD**

3.1.1.

**La educación y la
formación también se
transforman: EF21**



La educación y la formación se transforman no solo debido a la aparición del hecho digital, sino a los cambios, de todo tipo, que está experimentando el mundo y las diferentes localidades (es decir, lo global y lo local), las personas individual y colectivamente, y las organizaciones de todo tipo. Cambios que dan lugar a nuevos retos, amenazas, necesidades y oportunidades; así como al replanteamiento de la finalidad de la educación y la necesidad de nuevas formas, tiempos, agentes, entornos, momentos de formación, porque el futuro no va a ser el que se pensaba, hasta hace relativamente poco. En una palabra se hace necesario desarrollar, asumir y poner en práctica nuevas culturas para la identificación y la coherencia del YO, para vivir, convivir, trabajar, organizarse, etc. Este es un proceso en marcha, abierto e incompleto.





En este sentido ya se afirmó que la TD es más que un cambio en el que “lo digital sustituya a lo analógico”, implica cambios en todas las producciones humanas e incluso desarrollar una “estrategia de supervivencia”, como mínimo. Se trata de un cambio cultural profundo. La educación y la formación también se transforman, quizá a un ritmo menor que el que les gustaría a las personas con más visión e innovadoras.

Sin hablar de un cambio de paradigma en la EF, por el momento, sí que es conveniente fijar unos pilares en los que fundamentar la EF21. Unos pilares que no se pretende que sean ni exclusivos ni excluyentes, y que siempre podrán parecer incompletos. Para ello, hemos recurrido de nuevo a las preguntas del círculo de oro, ya que permiten centrar la cuestión y hacerlo de forma visual, simple y concisa.

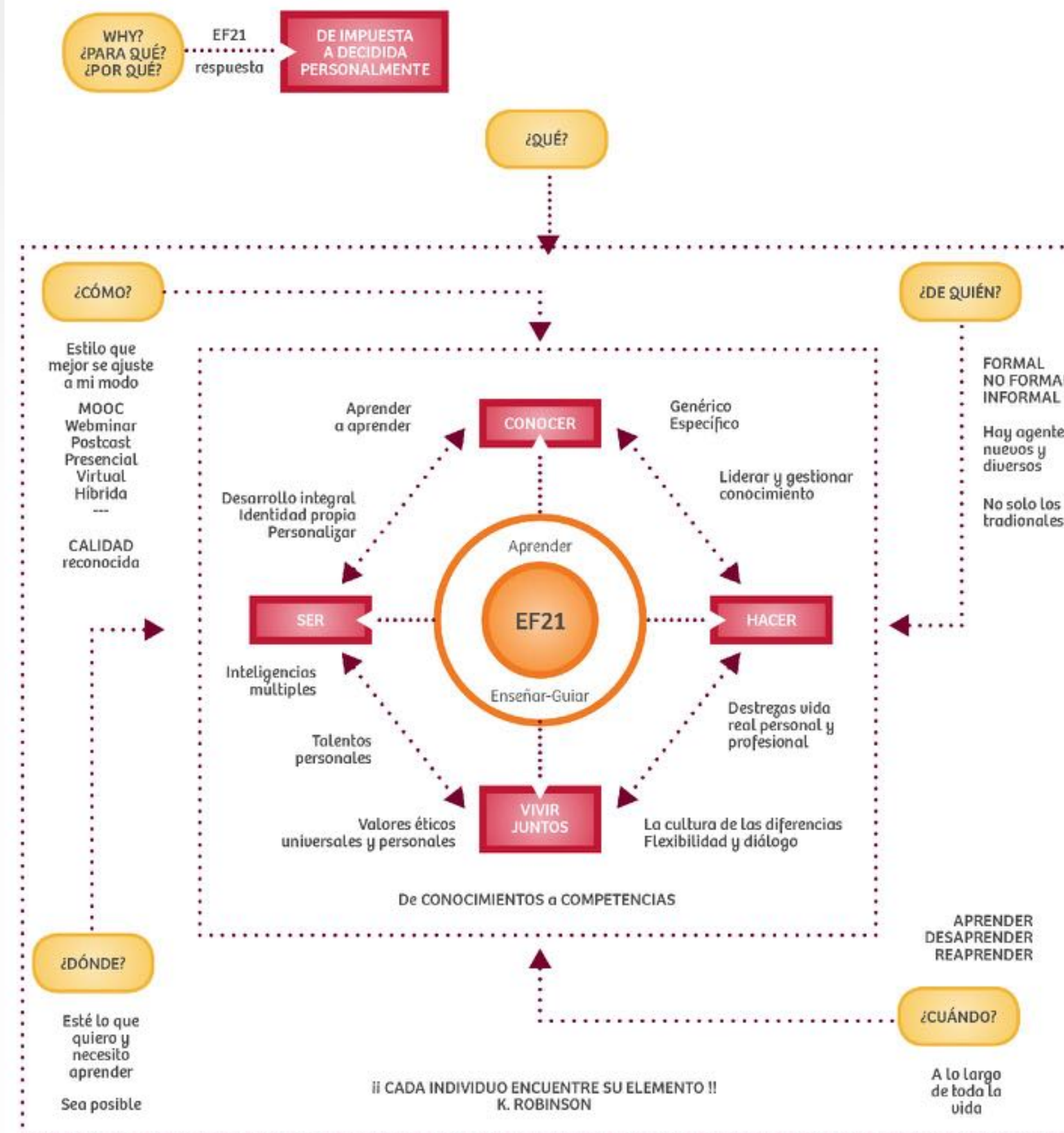


Fig.3.2.- Una visión de la Educación y Formación para el siglo XXI
Fuente: Elaboración propia, a partir de "la educación encierra un tesoro", J.Delors-Unesco, 1999.



La idea básica de dicha figura es del Informe Delors (1999) integrada con la metodología del círculo de oro ampliado, y con respuestas propias para este módulo. De la misma se quiere destacar, como relevante para el propósito de este apartado, que por diversas razones la educación y la formación pasa de:

Estar centrada solo en **CONOCIMIENTOS**, artificialmente compartimentados en asignaturas (e incluso en partes de las mismas), con poca coordinación y relación entre ellas, a una educación basada en **COMPETENCIAS** que permitan al ser humano y a sus organizaciones alcanzar su finalidad para o en el “siglo XXI”



Este es un proceso del que se habla mucho y se avanza poco.

Conviene comenzar fijando una definición, entre las muchas que pueden haber, que no obstante presentan elementos comunes, que son los que se quieren resaltar

Es un sistema denso, complejo, integrado y dinámico de saberes conceptuales, procedimentales y actitudinales que un ser humano ha conseguido desarrollar a ciertos niveles de calidad; y que le hacen apto para resolver problemas y seguir aprendiendo (significativa, funcional y permanente); esencialmente estos saberes hacen al sujeto capaz de realizarse como ser humano, como ciudadano y como trabajador profesional, o en diversos oficios y tareas”





Los saberes integrados que constituyen las competencias, tienden a hacer crecer los niveles de los cuatro aprendizajes fundamentales que propone el informe Delors-UNESCO: “Aprender a aprender”; “aprender a hacer”; “aprender a ser”; “aprender a convivir”.

Esta definición corresponde a un colegio jesuita de Guatemala y, personalmente, la consideramos muy acertada. Por otra parte, los alumnos pueden acceder a las orientaciones y propuestas de la UE, del Fondo Monetario Internacional, del Banco Mundial, de la OCDE, etc.



De dicha fuente, con aportaciones propias, se ha construido la imagen que sintetiza la Figura adjunta. En la misma se hace una aproximación al desarrollo del concepto y características de las competencias. Incidiendo en las **competencias genéricas**, que son las adecuadas para este módulo de introducción a la TD de las empresas, negocios y organizaciones.

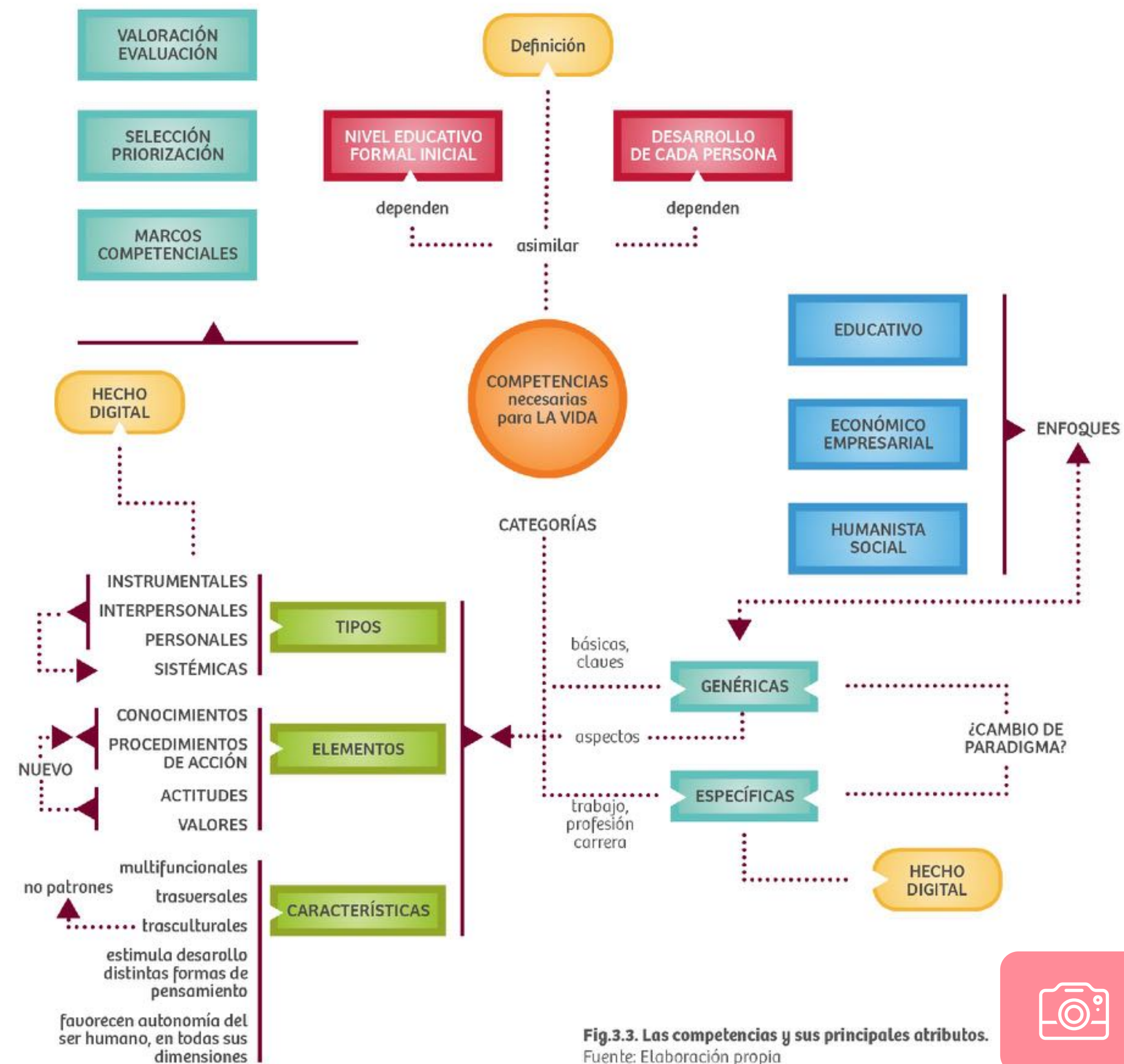


Fig.3.3. Las competencias y sus principales atributos.
Fuente: Elaboración propia



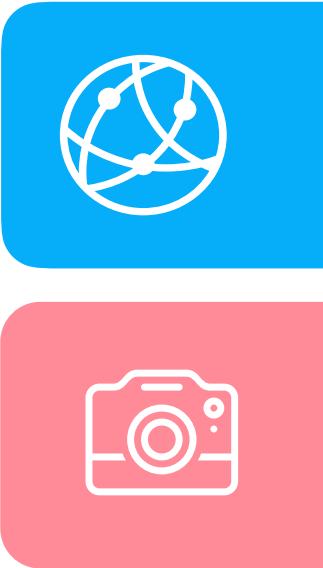
Al ser un sistema denso, complejo y dinámico es necesario -y así ocurre- que cada agente (escuela de negocios, universidad, consultora, organización global, ideales de cada comunidad educativa, empresa, gobierno con competencias legislativas, familia, y es deseable que también cada persona desde su individualidad) seleccione y priorice aquellas que considera más básicas y necesarias para cumplir con sus fines y propósitos. Estas competencias serán valoradas y evaluadas en cada circunstancia, mediante indicadores y procedimientos establecidos.



En nuestro caso el propósito es la TD de empresas de cualquier tamaño, naturaleza y sector. La metodología a seguir, partiendo de lo general a lo particular, se muestra en la Figura. Las competencias digitales son consideradas como una de las ocho competencias clave, para el aprendizaje permanente en un Marco de Referencia Europeo (UE), 2007; recomendadas a seguir desde la educación obligatoria de cada país miembro (y algunos de ellos ya las han ampliado a etapas anteriores a la obligatoria en España).



Fig.3.4. De lo general a lo específico de este curso
Fuente: Elaboración propia



Nos centraremos en los dos subapartados siguientes en las competencias digitales clave para la TD en las empresas (que serán fundamentalmente específicas con acompañamiento de algunas genéricas) y en la ciudadanía para beneficiarse y ser palanca de la misma (que serán fundamentalmente genéricas acompañadas de algunas específicas o técnicas).



3

**PINCELADAS PARA
COMPLETAR LA
INTRODUCCIÓN A LA TD**

3.1

**COMPETENCIAS
NECESARIAS PARA LA
TD**

3.1.2.

**Competencias desde
la perspectiva de la
empresa**



Como existen distintos marcos, como se ha comentado, elegimos uno de ellos, que creemos adecuado. El propuesto por RocaSalvatella:

Lo digital es una fuerza transformadora. Lo es, desde luego, desde el punto de vista de la demanda de clientes y empleados que están utilizando intensivamente las nuevas tecnologías digitales, y lo debería ser también desde el punto de vista de la oferta, con empresas y organizaciones. Pero, salvo algunos casos conocidos por todos, las organizaciones no están aprovechando totalmente las oportunidades que la economía digital parece ofrecer. Son ya muchas las organizaciones que han incorporado lo digital en su relación con los clientes, en sus procesos de comunicación y marketing e incluso en sus operaciones, pero todavía son pocas las que realmente han alcanzado el grado de madurez digital necesario para optimizar sus beneficios. Los datos indican que aquellas organizaciones y empresas que poseen la suficiente madurez digital (Digirati), no sólo para incorporar innovación digital sino también para llevar a cabo una transformación integral y beneficiarse desde el punto de vista del negocio, son un 26% más rentables que sus competidoras y obtienen un 9% más de ingresos.



En este contexto (de los cuatro segmentos de la maduración digital de una empresa), se ha desarrollado un modelo que reúne las 8 competencias que debe desarrollar un profesional, para transformar digitalmente -y de manera integral toda la organización- y garantizar su madurez digital. En el enlace anterior afirman:

El modelo de competencias aquí expuesto es un modelo basado en la experiencia. Reúne las 8 competencias básicas que desde RocaSalvatella consideramos debe adquirir y desarrollar todo profesional para afrontar el actual proceso de transformación digital. Individualmente nos hacen mejores profesionales. Aplicadas sobre el conjunto de una organización producen un gran impacto. Colectivamente nos permiten enfrentar con éxito el desafío digital.

En ultima instancia **todas deben estar orientadas a resultados**. Mirar cada una de las 8 competencias bajo el prisma de la orientación a resultados las transforma en poderosas herramientas de negocio y en competencias imprescindibles para cualquier profesional del siglo XXI.



MODELO COMPETENCIAS DIGITALES

RocaSalvatella



Se trata de competencias genéricas para la TD, en el sentido que afectan a todos los aspectos a transformar o crear en una empresa. Algunas de ellas son competencias genéricas de las personas para el siglo XXI, no asociadas, necesariamente, con la TD; como por ejemplo: la gestión de la información, la comunicación digital, y trabajo en red, y la del aprendizaje continuo; incluso la de conocimiento digital.

1

CONOCIMIENTO DIGITAL



2

GESTIÓN DE LA INFORMACIÓN



3

COMUNICACIÓN DIGITAL



4

TRABAJO EN RED



5

APRENDIZAJE CONTINUO



6

VISIÓN ESTRATÉGICA



7

LIDERAZGO EN RED



8

ORIENTACIÓN AL CLIENTE



Y en este aspecto faltan algunas, que se visualizan en la presente Figura, tan importantes al menos como las señaladas. Las que nos gustaría añadir (a las que le podía objetar, también, que no son solo esas) se sintetizan en dicha imagen; la incluimos ya que es una competencia que deberían tener -en mayor o menor grado- todas las personas (la ciudadanía).

Es la competencia de cómo alcanzar las metas y objetivos que una persona se plantee; en el caso de una empresa, obtener los resultados deseados.



Figura: Factores (competencias) esenciales para tener éxito en la consecución de resultados
Fuente: Plan by Accesory webinar, 2016.



El profesional con la competencia de “conocimiento digital” es capaz de:

UTILIZAR DE FORMA EFICIENTE RECURSOS Y HERRAMIENTAS DIGITALES

HACER USO DE HERRAMIENTAS Y MEDIOS DIGITALES EN SU DESARROLLO

COMPRENDER LA HIPERTEXTUALIDAD Y MULTIMODALIDAD DE LOS NUEVOS MEDIOS DIGITALES

INTEGRAR LAS NUEVAS LÓGICAS DIGITALES EN SU TRABAJO PROFESIONAL

USAR HERRAMIENTAS DIGITALES PARA EL PENSAMIENTO REFLEXIVO, LA CREATIVIDAD Y LA INNOVACIÓN

GESTIONAR DE MANERA APROPIADA LA IDENTIDAD DIGITAL CORPORATIVA Y PROPIA.

INTERVENIR DE FORMA RESPONSABLE, SEGURA Y ÉTICA EN ENTORNOS DIGITALES CORPORATIVOS O PROPIOS.

EVALUAR CRÍTICAMENTE PRACTICAS SOCIALES DE LA SOCIEDAD DEL CONOCIMIENTO



Si las incorpora, dicho profesional **aporta** a la organización:



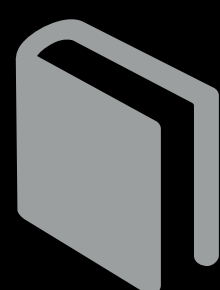
GESTIÓN TALENTO

Cambia la manera de gestionar el talento y los procesos.



FLEXIBILIDAD

Mejora la flexibilidad y la capacidad de reacción y anticipación.



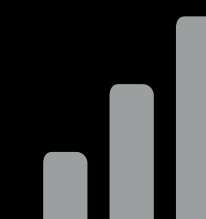
CONOCIMIENTO

Aumenta el conocimiento del entorno.



SEGURIDAD

Genera seguridad ante los cambios y la incertidumbre.



PRODUCTIVIDAD

Aumenta la productividad y acelera la innovación

3

**PINCELADAS PARA
COMPLETAR LA
INTRODUCCIÓN A LA TD**

3.1

**COMPETENCIAS
NECESARIAS PARA LA
TD**

3.1.3.

**Competencias desde
la perspectiva de la
ciudadanía**



La orientación de este subapartado se quiere que exceda a la de considerar a las personas como clientes para una empresa u organización, sin que esta afirmación implique posicionamiento peyorativo alguno. Es un planteamiento desde la perspectiva de los individuos y las personas, que tienen que desarrollarse y conseguir sus propósitos en un mundo dominado por el hecho digital, en una sociedad de la información y del conocimiento, y en un entorno VUCA.

Para ello se propone comenzar por los marcos de alfabetización digital que ha elaborado la UE, y que hasta el momento, pocos países han implementado y seguido, a no ser en sus niveles más básicos.



PLAN DE ALFABETIZACIÓN DE LA UE

La UE está desarrollando -desde 2015- un ambicioso plan de alfabetización para la ciudadanía que consta de cuatro estudios interrelacionados, necesarios y complementarios: DigCom, DigComEdu, DigComOrg, CompuThink.. Todos ellos atienden a distintos agentes básicos del sistema educativo, con una perspectiva innovadora del mismo.

DigCom



DigComOrg



DigComEdu



CompuThink



A woman with long dark hair is wearing a white and black VR headset. She is sitting in a white office chair and has her hands raised in front of her, as if interacting with a virtual environment. She is wearing a dark-colored button-down shirt. The background is a bright, modern office with large windows, a desk with a laptop, and some office supplies. The entire image has a light blue tint. The word "DIGCOM" is written in white, bold, sans-serif capital letters in the center of the image.

DIGCOM

Ser digitalmente competente; una tarea para el ciudadano del siglo XXI

El Marco de Competencias Digitales para la Ciudadanía: DigCom 2.0, fue actualizado en 2016. El mismo propone cinco áreas claves y veintiuna competencias, La propuesta distingue tres niveles de suficiencia, a nivel de usuario, y propone ejercicios de autoevaluación.

NIVELES DE SUFICIENCIA

1

USUARIO BÁSICO

2

USUARIO INDEPENDIENTE

3

USUARIO COMPETENTE



Al mismo tiempo, establece cuáles son los pasos a seguir a partir de ahora. Estas acciones forman parte del plan de acción de la estrategia Europa 2020.

DigComp's five key areas and 21 competences

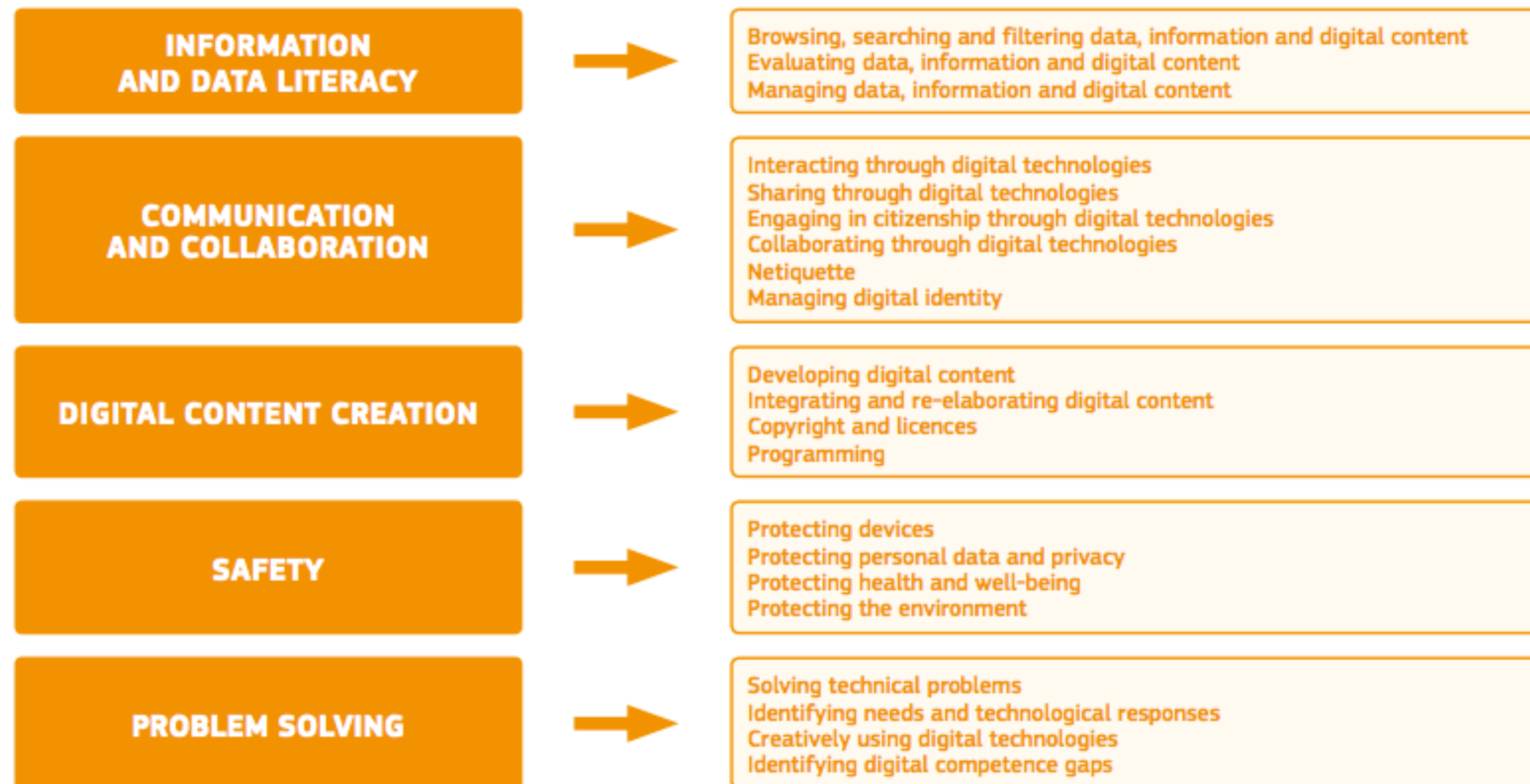


Figura: Marco de competencias digitales 2.0 para la ciudadanía.
Fuente: DiGCom, UE, 2016.



El nivel de implementación de los países y regiones miembros, se muestra en la Figura

Member State implementations

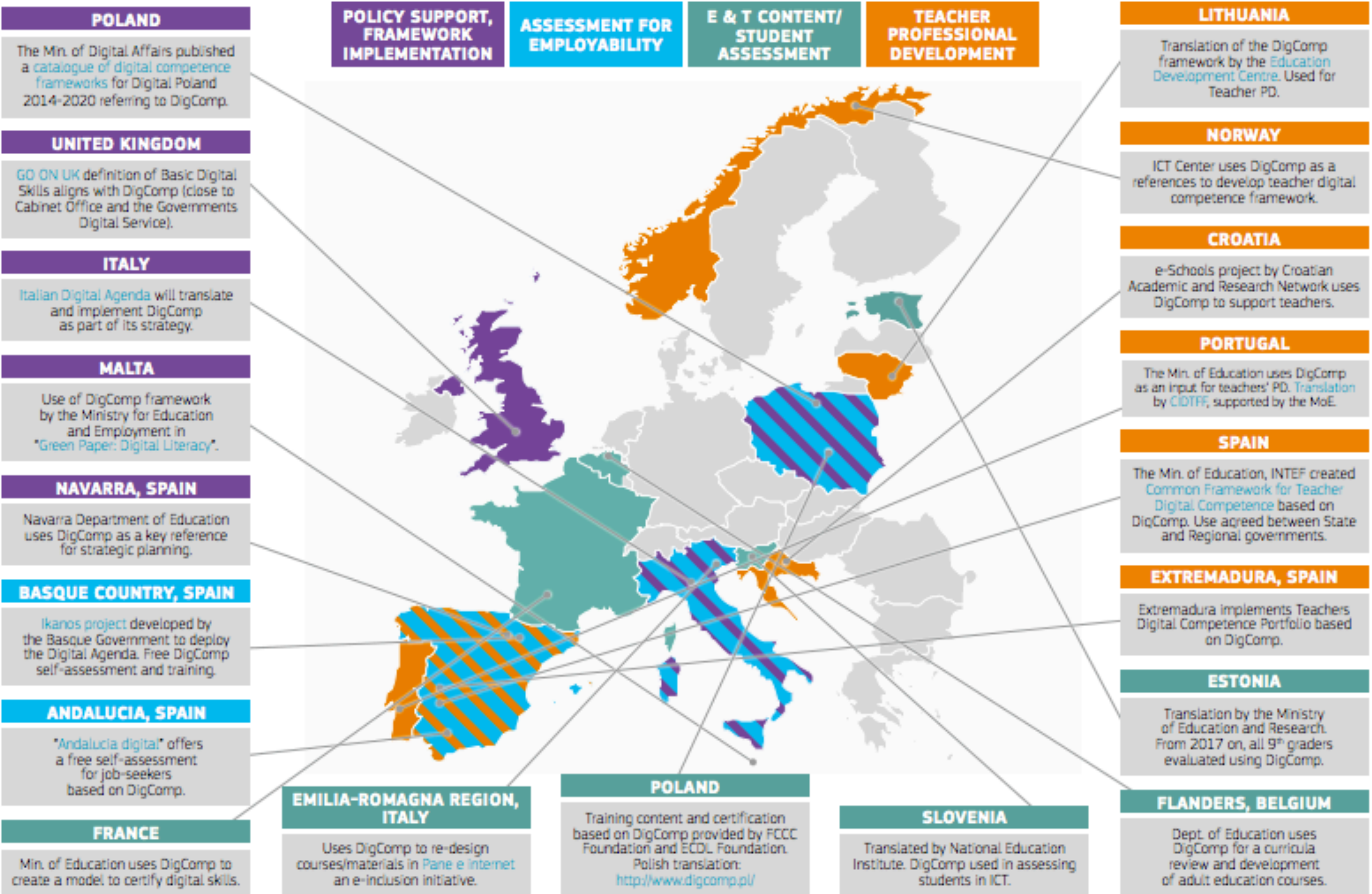


Figura: Niveles de implementación de los Estados Miembros
Fuente: DiGCom, UE, 2016.





DIGCOMEDU

Marco de Competencias Digitales para los Educadores o Docentes

Se pretende crear un marco de referencia a nivel europeo, orientado a todos los niveles docentes del sistema formal, que supere la amplia variedad de ellos que existen (o que no existen) en diferentes Estados Miembros. Hasta el momento existe una propuesta de competencias.

1. Compromiso profesional	2. Recursos Digitales	5. Empoderar a los Estudiantes	6. Facilitar la Competencia Digital de los Estudiantes
1.1 Gestión de datos	2.1 Selección de recursos digitales		6.1 Información y alfabetización mediática
1.2 Comunicación de la organización	2.2 Organizar, compartir y publicar		6.2 Comunicación y colaboración digital
1.3 Colaboración profesional	2.3 Creación y modificación	5.1 Accesibilidad e inclusión	6.3 Creación de contenido digital
1.4 Práctica reflexiva	3. Pedagogía Digital <i>Usar herramientas digitales para mejorar e innovar</i>	5.2 Diferenciación y personalización	6.4. Bienestar
1.5 Desarrollo Profesional Continuo Digital (CPD)	3.1 Instrucción	5.3 Participación activa	6.5 Solución digital de problemas
	3.2 Interacción profesor-alumno		
	3.3 Colaboración de los estudiantes		
	3.4 Aprendizaje autodirigido		
	4. Evaluación digital <i>Usar herramientas digitales para mejorar e innovar</i>		
	4.1 Formatos de evaluación		
	4.2 Analizar pruebas		
	4.3 Retroalimentación y planificación		

Figura: Visión general del marco DigComEdu.,
Fuente: DigComEdu, EU, 2017.



Propuesta de competencias de los niveles de valoración y denominación en los docentes

	Novato (A1)	Explorador (A2)	Entusiasta (B1)	Profesional (B2)	Experto (C1)	Pionero (C2)
1. Compromiso profesional	Poco uso; No estar seguro	Ser consciente ; Uso de herramientas básicas	Uso eficiente, responsable, experimentar	Práctica creativa, responsiva, transparente, refleja	Evaluar, discutir, reflexionar de manera crítica y estratégica	Rediseñar, Innovar
2. Recursos Digitales	Usar poco; No estar seguro	Estar consciente ; Uso de herramientas básicas	Criterios y estrategias basicos y a veces avanzados	Estrategias avanzadas , criterios complejos ; crear recursos	Usar herramientas avanzadas de manera comprensiva ; publicar recursos	Crear y publicar de manera profesional
3. Pedagogía Digital	Usar poco; No estar seguro	Estar consciente ; Uso de herramientas básicas	Integración y implementación de manera significativa	Mejorar; orquestrar	Adaptar métodos de manera flexible, estratégica, intencional	Innovar en la enseñanza
4. Evaluación Digital	Usar poco; No estar seguro	Uso de herramientas básicas para reforzar estrategias tradicionales	Uso de herramientas digitales para mejorar estrategias tradicionales	Uso estratégico y eficiente	Práctica comprensiva, crítica y refelja	Innovar en la evaluación
5. Empoderar a los Estudiantes	Usar poco; No estar seguro	Estar consciente ; Uso de herramientas básicas	Considerar empoderar a los estudiantes	Usar varias herramientas de manera estratégica	Mejorar de manera comprensiva y crítica	Innovar métodos
6. Competencia Digital Estudiantes	Poco uso de las estrategias para la CD del estudiante	Animar a los estudiantes a usar herramientas digitales	Implementar actividades para fomentar la CD de los estudiantes	Usar varios métodos de manera estratégica	Métodos comprensivos y críticos	Usar formatos innovadores para formentar la CD de los estudiantes

Figura: Propuesta de un Marco Común Europeo de referencia para las competencias digitales de los docentes
Fuente: DigComEdu, EU, 2017.



A woman with long dark hair is wearing a VR headset and smiling. She is pointing her right index finger upwards. She is sitting at a wooden desk with a laptop and a tablet. The background is a blurred office or home workspace. The entire image has a teal color overlay.

DIGCOMORG

Marco Europeo para las organizaciones educativas digitalmente competentes

En este caso se trata de organizaciones, de un cierto sector y naturalezas, que pueden y deben transformarse digitalmente. Ya existe una propuesta de marco, con siete áreas clave y quince competencias.



Figura: Marco Europeo para las organizaciones educativas digitalmente competentes.
Fuente: DigComEdu, EU, 2016.



Todas estas propuestas, con sus actualizaciones, surgen del JRC (Joint Research Center) de la Comisión Europea, uno de cuyos institutos es el JRC-Institute for Prospective Technological Studies, European Commission tiene su sede en Sevilla, España.

En el informe elaborado en 2015 se incluyen todas las características de la propuesta, que la Comisión ha hecho suya, con las enmiendas presentadas por los Estados Miembros.

:



A woman with long dark hair is smiling while wearing a white VR headset. She is sitting in a modern office chair, and her hands are raised near the headset. The background shows a blurred office environment with a desk lamp, a bicycle, and some office supplies. The entire image has a teal overlay. The word "COMPUTHINK" is written in white, bold, sans-serif capital letters across the center of the image.

COMPUTHINK

Se trata de un estudio para el desarrollo del Pensamiento Computacional (PC) desde las primeras etapas escolares, como competencia esencial para el siglo XXI.

El pensamiento computacional (Computational Thinking, CT) es una abreviatura para referirse a "pensar como un ingeniero o experto informático"; es decir, la capacidad de utilizar los conceptos de la informática para formular y resolver problemas y desarrollar otras competencias esenciales para el siglo XXI. El pensamiento computacional ha sido promovido en los últimos años como una competencia [instrumental] que es tan fundamental como la aritmética o la alfabetización (saber leer y escribir). A pesar del gran interés en el desarrollo de la CT entre los escolares, y la gran inversión pública y privada en iniciativas de CT, existen una serie de problemas y desafíos para la integración de CT en los programas escolares, no resueltos hasta el momento.



Antes de terminar este apartado, una pregunta sin respuesta

SI LA TD DE LAS EMPRESAS, NEGOCIOS U ORGANIZACIONES ES UNA REALIDAD (SE PRETENDE QUE LO SEA O SE ESTÁ EN VÍAS DE SERLO), ¿POR QUÉ NO TAMBIÉN LA TD DE LA EDUCACIÓN CON LAS MISMAS ORIENTACIONES Y CONSIGUIENTES ADECUACIONES?

P.D. La respuesta no es que no se trata de una empresa, negocio u organización.



3

**PINCELADAS PARA
COMPLETAR LA
INTRODUCCIÓN A LA TD**

3.2

**LEGISLACIÓN Y
CIBERSEGURIDAD**



En este apartado se dan unas pinceladas, en este caso con “brocha gorda”, de estos dos aspectos relacionados con la TD. Se ha puesto el símil indicado, ya que en este caso (al contrario del apartado anterior, con “pincel fino”) se trata de dos aspectos de la transformación a los que se les dedican módulos específicos: el módulo (perteneciente a consultor digital), “Ciberseguridad y finanzas en entornos empresariales”; el módulo (transferencia de conocimiento), “Propiedad intelectual. Protección del conocimiento”; el módulo, “Normativa reguladora I”; y el módulo, “Normativa reguladora II”. Ahora bien, es cierto que al existir diferentes niveles o itinerarios habrán alumnos que no estudien estos aspectos.

Las pinceladas solo se pueden desarrollar de manera muy básica y concisa; se trata, simplemente de que conozcan su existencia y de dónde se pueden documentar, hasta que estudien los niveles superiores.

Por otra parte, hay que resaltar que ambos aspectos solo se consideran en relación con la TD de empresas, negocios u organizaciones no con el hecho digital en general, ni con la TD de otro sector de la economía o la sociedad en general; nos parece importante esta matización.





Los aspectos relevantes, a priori, deben ser los que se tratan en los niveles indicados en los posteriores módulos del curso. La dificultad radica en que este módulo, se ha diseñado y escrito cuando aquellos aún no lo habían sido, y solo se disponía de las líneas maestras de los mismos; situación que no se dio en relación con el módulo 2, por ello la “introducción a la TD” tiene poco de “Tecnologías para la TD”.

La orientación dada, a la legislación y a la ciberseguridad, se focaliza en los aspectos generales y básicos de las mismas.

3

**PINCELADAS PARA
COMPLETAR LA
INTRODUCCIÓN A LA TD**

3.2

**LEGISLACIÓN Y
CIBERSEGURIDAD**

3.2.1.

**Pinceladas de
legislación**



Creemos que, en este caso la orientación debe ser la de considerar los “aspectos jurídicos de la transformación digital”, para que el alumno tenga su propio criterio acerca de la problemática que subyace.

Hay que destacar que las normas van a ir siempre detrás de la realidad; es lógico. Esta afirmación es más rotunda si cabe en el momento actual, de cambios profundos, rápidos, continuos y de transmisión inmediata. Ahora bien, **no hay que pasar de unos “vacíos legales” a una sobrerregulación.**

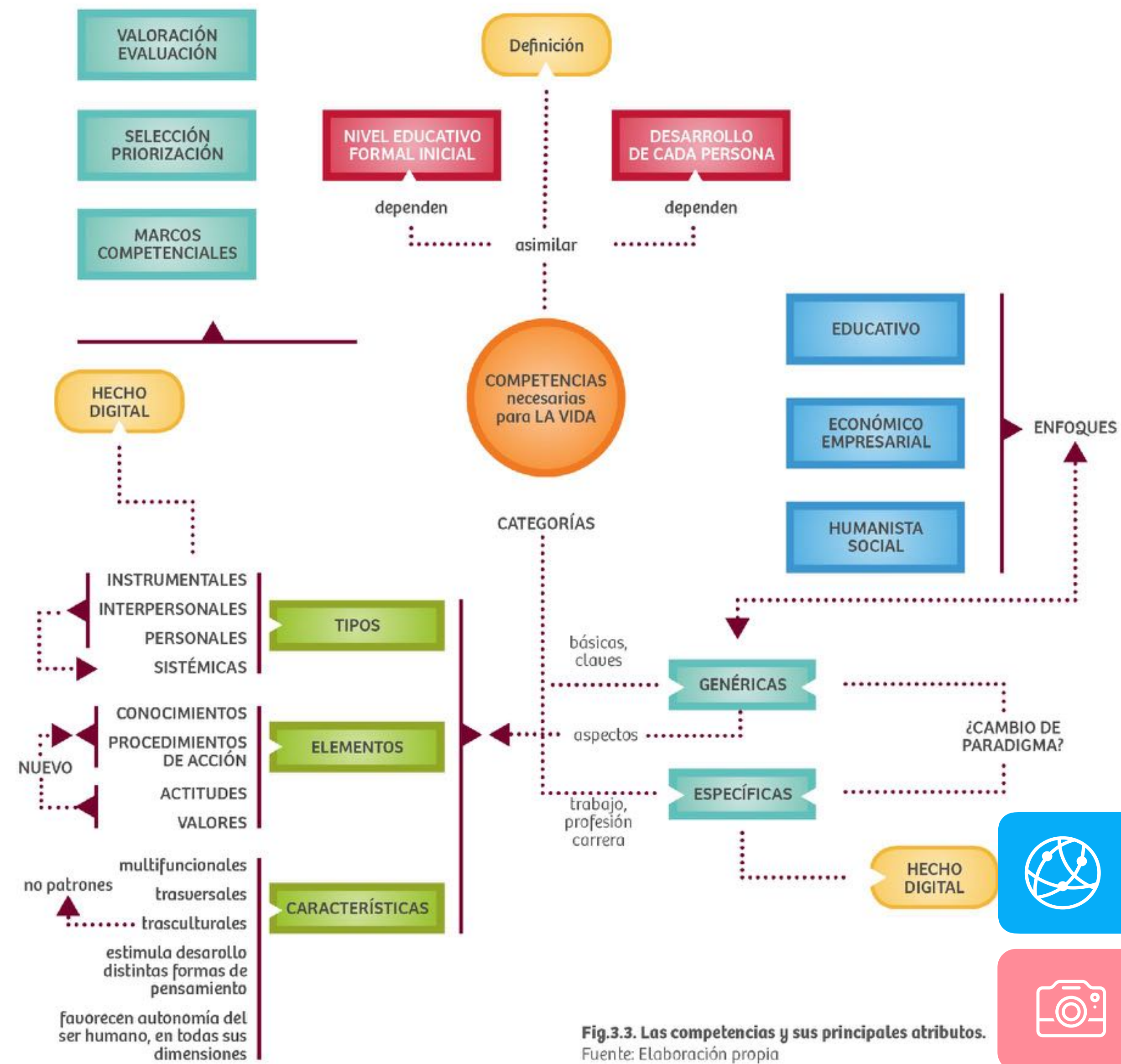


Fig.3.3. Las competencias y sus principales atributos.
Fuente: Elaboración propia



La cuestión es, más bien, decidir cuál es la mejor forma de regular los cambios o las tecnologías disruptivas. No se puede olvidar que las normas de un país (y las decisiones judiciales que las aplican) tienen un efecto directo sobre la innovación. En un mundo globalizado como el actual, es difícil pensar que un emprendedor -con una idea brillante- vaya a constituir su start up en un territorio con abundantes restricciones a nuevos servicios o escasa protección de la propiedad intelectual e industrial.

Los reguladores habitualmente se fijan más en los peligros que en los beneficios de las nuevas tecnologías. Lo vemos por ejemplo en el caso de los drones. Como apunta Enrique Dans, “todo retraso impuesto al desarrollo del tejido emprendedor, supone un retraso global para el país como tal”. Las leyes no deberían poner trabas o frenos injustificados, ni mucho menos crear limbos jurídicos, como pasa actualmente con esas aeronaves no tripuladas y el resto de ejemplos citados.



La innovación y la transformación tienen sus propios retos jurídicos, que hay que ponderar. Ahora bien, la situación tiene también la otra “cara de la moneda”: estos vacíos legales, de los que se aprovechan lícitamente aquellas empresas más innovadoras y con visión, están creando problemas (compitiendo) con las empresas que no se han transformando todavía, de los mismos sectores y que cumplen con la legislación actual.

La cuestión clave es:

¿Hasta dónde legislar, en relación con los cambios de modelo de negocio y tecnologías disruptivas, sin limitar el tejido innovador y emprendedor de una país -que se aprovechan, lícitamente, de los “vacíos legales”- y al mismo tiempo no permitir una cierta “competencia desleal” con las empresas y actividades tradicionales, que cumplen con las normas jurídicas existentes y pagan sus impuestos?





Hablando de normas e innovación o transformación, es pertinente preguntarse: **¿cómo está asumiendo el propio sector legal la transformación digital?** Una vez más los anglosajones han tomado la delantera. En el caso del Reino Unido, en el año 2007 se aprobó la Legal Services Act, que admitía la posibilidad de que los dueños de los bufetes no fueran abogados. Es lo que se conoce como ABS (Alternative Business Structures) y ha permitido que empresas con base tecnológica puedan ser titulares de bufetes. Una de las más exitosas es Riverview Law.





Pero Riverview Law no es un caso aislado. RocketLawyer y Legalzoom llevan ya varios años poniendo a disposición de individuos y pequeñas empresas documentos legales básicos y asesoramiento legal online a precios muy competitivos. Otras empresas en cambio prefieren apostar por nichos concretos: Diligence Engine ofrece una herramienta muy potente para la revisión de todo tipo de acuerdos; Juristat pone a disposición información relevante en los procesos de patentes; Picture It Settled comercializa un software de análisis, que puede aportar mucho valor y ahorrar tiempo en las negociaciones y Modria apuesta fuerte por su sistema de resolución de conflictos online, que ha ayudado a Paypal y a eBay a solucionar más de 400 millones de casos.



Sin duda uno de los productos que más interés está despertando es Watson, creado por IBM. Se trata de una tecnología que procesa la información más como un ser humano que como un ordenador tradicional, puesto que es capaz de comprender el lenguaje natural oral y escrito, de generar hipótesis basadas en la evidencia, y de hacerse “más inteligente” cada vez, aprendiendo de las interacciones previas. Además analiza y procesa datos no estructurados (80% de la información actual de internet). IBM lo denomina computación cognoscitiva y es un concepto que va más mucho más allá del big data. Hay expertos que consideran que probablemente es la tecnología más importante que ha llegado al mundo legal y que permitirá a los abogados pensar y actuar de manera mucho más innovadora, sobre todo a los más jóvenes, que serán los primeros en adoptarla.

La situación legal afecta a gobiernos (en sus diferentes niveles competenciales), a empresas y a consumidores. Cada uno de estos agentes con sus propias perspectivas, competencias, necesidades, oportunidades, capacidad de innovación y de transformación o adaptación al cambio. La figura pretende orientar en el autoaprendizaje al estudiante hacia aquellos aspectos importantes y, sobre todo, que le puedan interesar en cada momento, para su ampliación.

En su parte inferior se han resaltado aspectos que se consideran importantes, para este módulo:

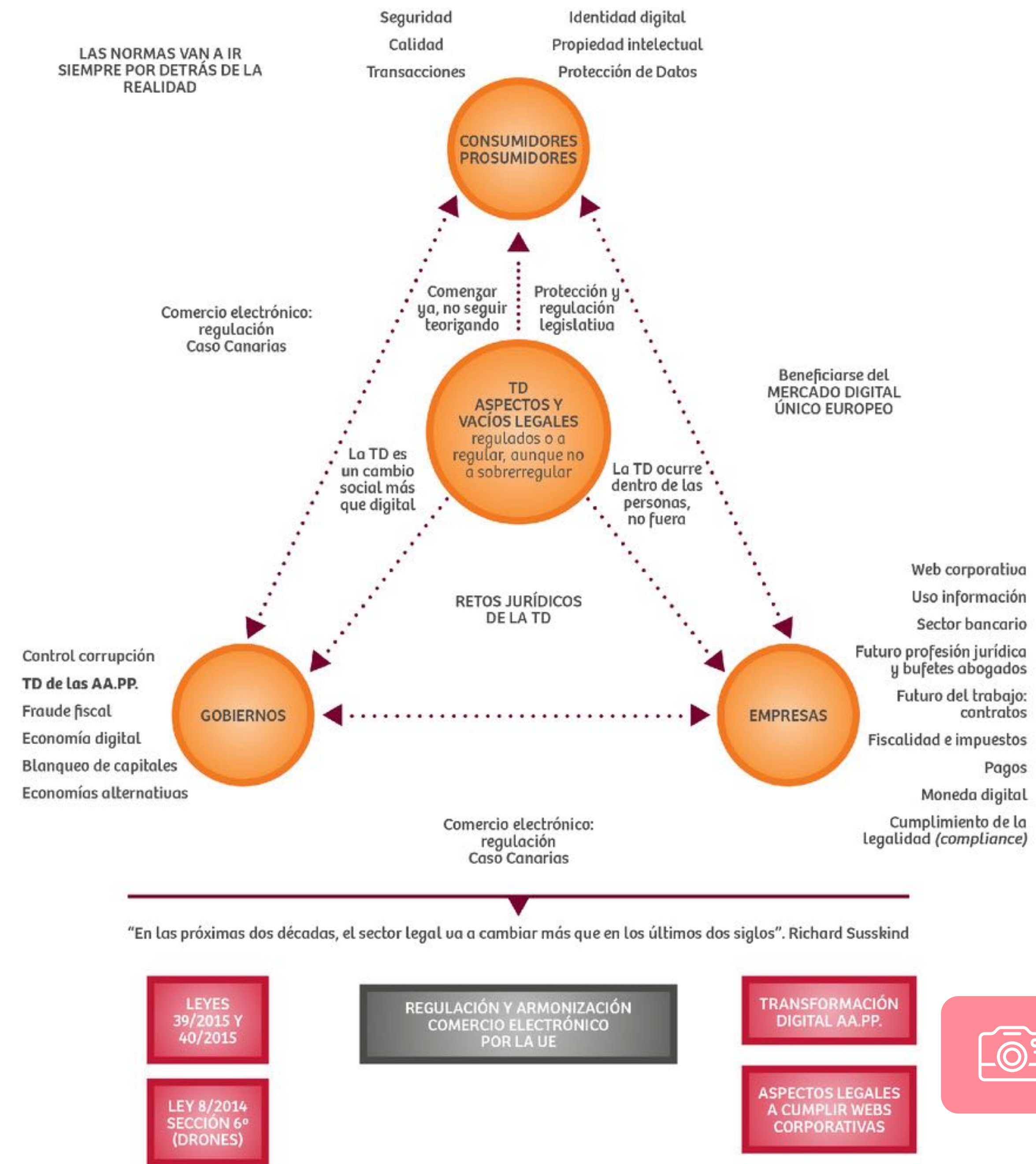


Fig. 3.10. Algunos aspectos legales relacionados con la TD.
Fuente: Elaboración propia

La TD de las AA.PP, que aunque no se trata explícitamente en este curso, es de vital importancia para todos los agentes de interés implicados en la TD de empresas, negocios y organizaciones (y que ya sido regulada por las leyes 39 y 40 de 2015, ya en vigor) ; la ley 8 de 2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia, en su sección 6ª, que regula el uso de drones, y que es un ejemplo de cómo se regulan las innovaciones disruptivas (después de tanto tiempo siguen vigentes las normas que se dictaron de manera temporal); la situación normativa y reguladora del comercio electrónico, quizá, la transformación digital más conocida y utilizada por la ciudadanía (bueno, por parte de ella al menos); las ultimas regulaciones de la UE respecto al mismo; y un aspecto de especial relevancia para PYMES, microempresas y start ups, los [estándares](#) y [cumplimientos](#) que deben incorporar, legales y normativos, las páginas (o sitios) web de las mismas, para evitar fraudes y proteger a los clientes o consumidores.



3

**PINCELADAS PARA
COMPLETAR LA
INTRODUCCIÓN A LA TD**

3.2

**LEGISLACIÓN Y
CIBERSEGURIDAD**

3.2.2.

**Pinceladas sobre
ciberseguridad**



Es un aspecto estrechamente relacionado con el anterior; realmente la ciberseguridad es una parte de los aspectos legales de la TD; ahora bien, es eso y mucho más.

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.



Es decir: define todos los conceptos que rigen la seguridad a través de Internet. Datos personales, información bancaria, claves, compras online,... La cantidad de información que circula por Internet es enorme; los riesgos se hacen patentes cada día con mayor intensidad y variedad para todas las personas, pero también para las empresas, las instituciones e incluso los países. El ciberentorno es cada día más grande, y precisamente la ciberseguridad debe garantizar la seguridad de nuestra “presencia” y “movimientos” en la red.



Se considera pertinente mostrar una visión del ámbito de la ciberseguridad esquemáticamente, como se hizo en el apartado anterior. De la misma se priorizarán algunos de los aspectos que figuran en su parte inferior, para describirlos de forma concisa.

La figura pretende dar una primera -y particular- visión general del marco de la ciberseguridad. Se trata de una tarea ardua ya que a la misma se le dedican cursos y libros completos. No obstante, mediante la misma el alumno puede comprender su ámbito, y abordarlo en experiencias y aprendizajes posteriores. De las tres categorías, arbitrarias, en que se han clasificado los entes que hay que proteger de los nuevos y emergentes delitos asociados a la TD, a las tecnologías digitales y a Internet nos centraremos en las empresas, negocios y organizaciones, que constituyen el foco de este curso.

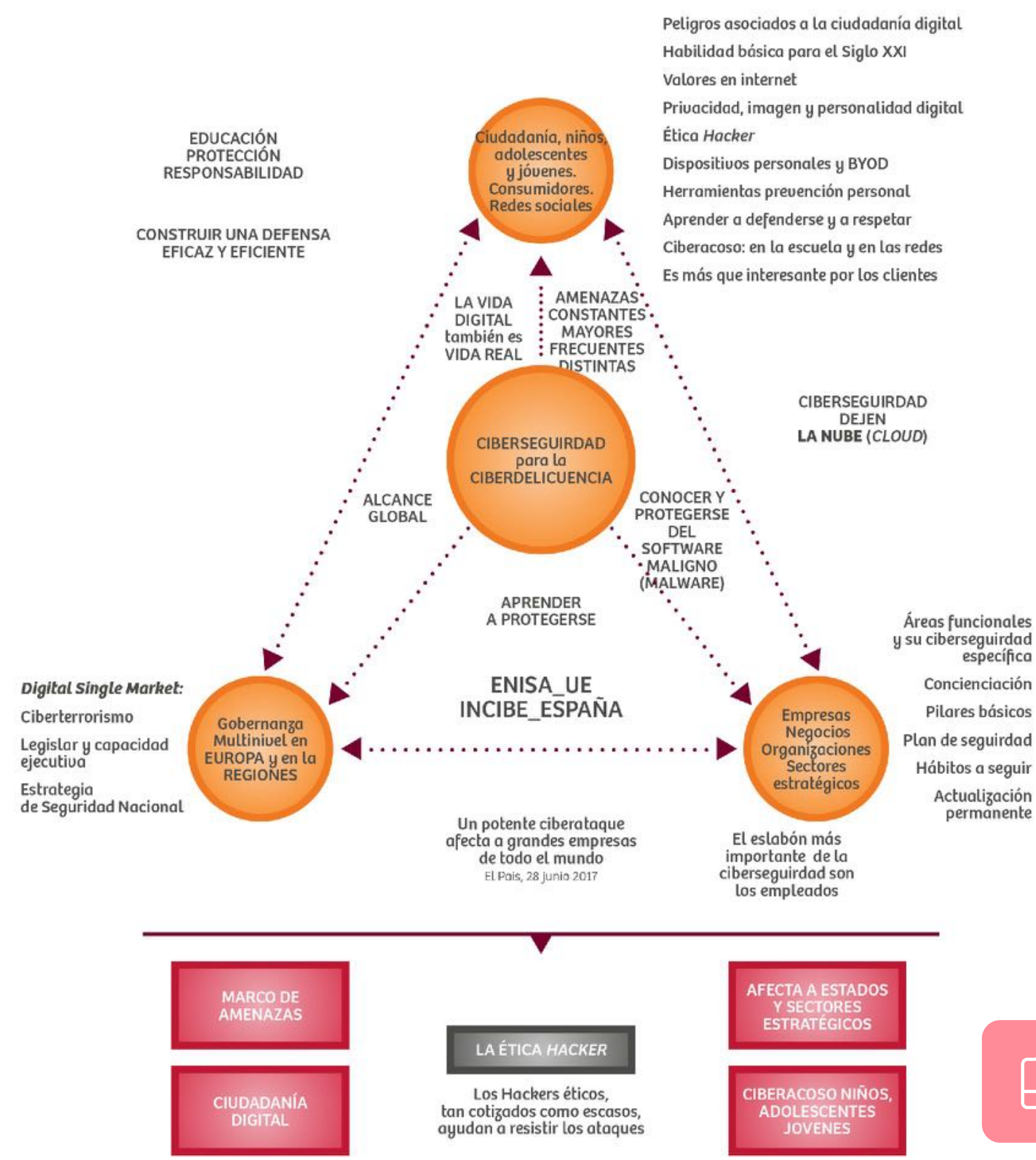


Fig. 3.13. ámbito de la ciberseguridad para defenderse de la ciberdelincuencia.
Fuente: Elaboración propia

Esta focalización en si misma es la que va a constituir la “pincelada” que se aborda en este módulo 1.

La orientación que se le da al alumno para su estudio es que acceda a la página corporativa del INCIBE, en la que existen datos, información y conocimiento extensos, actuales, claros y sencillos, adaptados al entorno español y gratuitos. La aportación nuestra es estructurar las líneas maestras, que pueden encontrar en dicho sitio web. En el mismo existe una colección completa de documentos, con el epígrafe “protege tu empresa”, a los cuales se sugiere que acceda el alumno.

El Gobierno de España, dado que la situación era (y cada vez lo es más) potencial y realmente tan peligrosa creó el **INCIBE** (Instituto Nacional de Ciberseguridad)



El INCIBE, anteriormente Instituto Nacional de Tecnologías de la Comunicación (INTECO), es una sociedad dependiente de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD), y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

Con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE contribuye a construir ciberseguridad a nivel nacional e internacional.

.



Esta es la mejor referencia a seguir, en una introducción a este tema tan importante. Para desarrollar una estrategia de seguridad, que proteja una empresa, negocio, organización o sectores estratégicos hay que seguir la siguiente secuencia dinámica, que se realimenta constantemente,

El INCIBE ha elaborado un kit de concienciación para empresas, que se puede descargar gratuitamente desde el enlace anterior.

En el proceso de definir e implementar la ciberseguridad de una empresa tienen una participación principal, aunque ni exclusiva ni excluyente, los responsables de Tecnologías de Información en la empresa. Este plan debe estar alineado e integrado en el plan estratégico de TD de la empresa.



Fig.3.12. Proceso para definir e implementar la ciberseguridad de una empresa

Fuente: Elaboración propia



SECURITY BREACH

PILARES ESTRATÉGICOS BÁSICOS

HACKING DETECTED

INTRUSION DETECTED

56%

18%

23%

32%

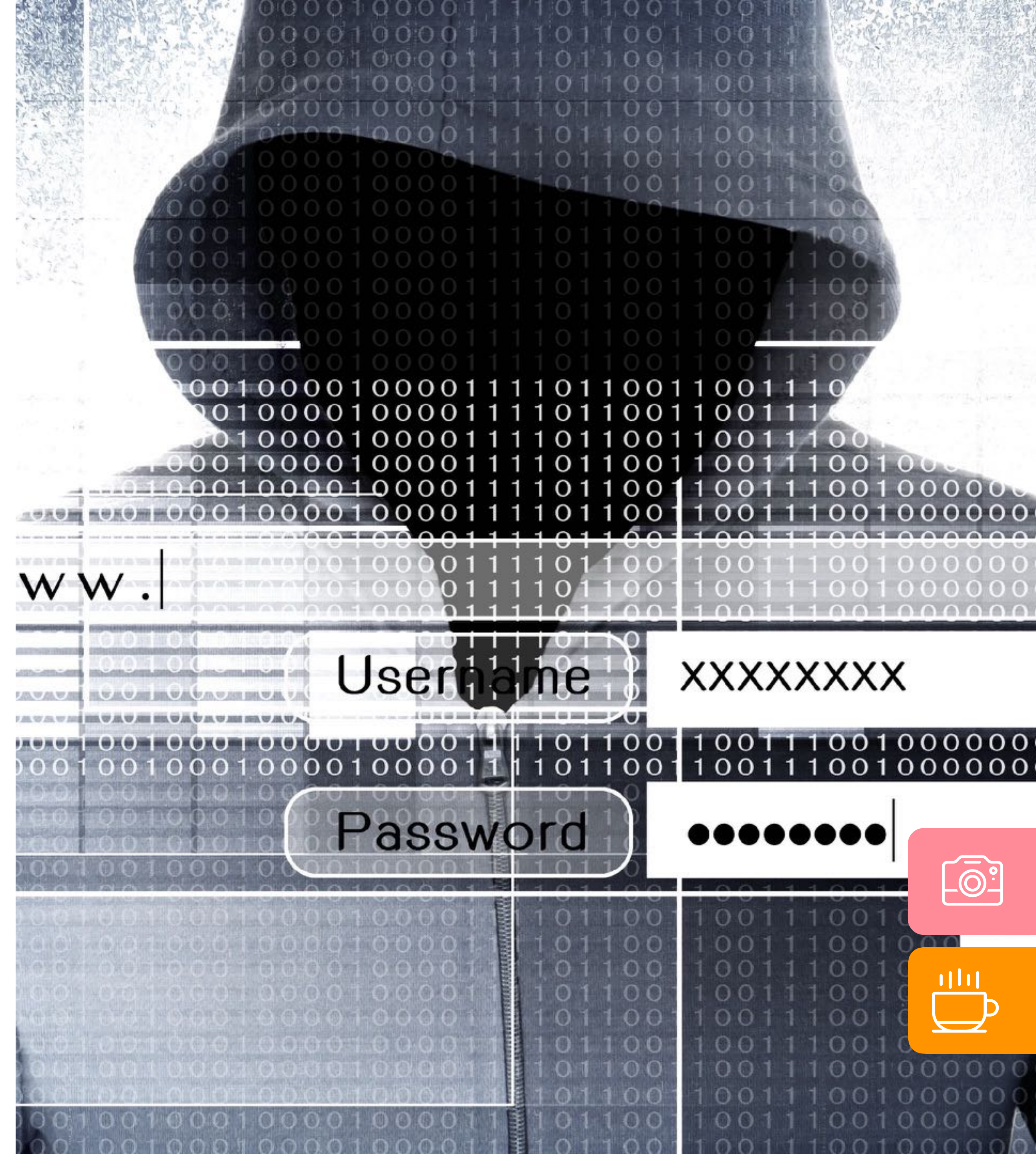
74%

67%

47%

Se cree conveniente comentar los cuatro pilares estratégicos que han seleccionado en el proceso anterior:

En los últimos años el mundo de la seguridad de las Tecnologías de la Información (TIC) ha vivido una revolución. Comenzó con la profesionalización de los hackers, que dejaron de ser esos seres legendarios que luchaban por «unos ideales poco definidos, hasta desarrollar una verdadera industria basada en estafar al mayor número de incautos y así obtener un mayor beneficio económico». Por si fuera poco, las nuevas tendencias como el BYOD no facilitan nuestra labor, ya que no solo tenemos que proteger los dispositivos en la oficina, sino también en cualquier lugar que se encuentren.



Hay que tener en cuenta que las estrategias tradicionales, basadas en proteger el endpoint (el terminal final o propio), no son suficientes; **la seguridad no está garantizada instalando antivirus**. Es obvio que un antivirus neutralizará muchas de las amenazas existentes, pero su eficacia es limitada en algunos casos, por lo que se deben implementar otras soluciones y extremar la precaución. Se deben plantear soluciones de seguridad completa, si es que existen, ya que un área sin proteger daría al traste con todas las otras medidas que se implementasen.



Antes de abordar la metodología inquisitiva conviene que se familiarice más con la pregunta clave: eso de la TD ¿de qué va?; como se verá no es la pregunta más importante, aunque puede ser la más motivadora para una persona que se inicia en el liderazgo para la gestión del cambio y la incorporación del hecho digital en las organizaciones.



PILARES POLÍTICA DE SEGURIDAD

A continuación se reproducen los 4 pilares sobre los que se deben fundar las políticas de seguridad

1

REDUCIR EL ÁREA DE
ATAQUE



Minimizar el riesgo controlando todo aquello que pueda aportarlo, como vulnerabilidades o aplicaciones.

2

PROTECCIÓN EN
CUALQUIER LUGAR



Los usuarios deben estar protegidos estén donde estén y sin importar los dispositivos que utilicen.

3

DETENER AMENAZAS Y
FUGAS DE DATOS



La estrategia debe incluir soluciones capaces de detectar y prevenir amenazas y fugas de datos. Si se trata de motores antimalware, p.e., no se puede quedar solo en el uso de firmas, sino que habrá que utilizar tecnologías proactivas y en tiempo real, para poder detener nuevas amenazas, incluso desconocidas, automáticamente.

4

MANTENER A LOS
EMPLEADOS
TRABAJANDO



Tanto usuarios como el departamento de TI (TIC) deben poder trabajar sin que la seguridad sea un impedimento. La seguridad ha de ser lo más transparente para el usuario, aunque ésta no debe interponerse en su trabajo.





EL PLAN DIRECTOR DE SEGURIDAD





¿Por dónde empezar? Cuando se decide abordar la ciberseguridad es importante tener una planificación de las actividades a realizar, que cuente con el compromiso de la alta dirección (al igual que ocurre con el proceso de la TD). Este plan va a marcar las prioridades, los responsables y los recursos que se van a emplear, para mejorar nuestro nivel seguridad en el mundo digital.

A esta planificación se le llama Plan Director de Seguridad. Contendrá los proyectos que se vayan a abordar, tanto técnicos como de contenido legal y organizativos. Así, habrá proyectos de instalación de productos o de contratación de servicios, pero otros serán para cumplir con las leyes de privacidad y comercio electrónico, formar a los empleados o para poner en marcha procedimientos y políticas internas,.



Un Plan Director de Seguridad (PDS) consiste en

La definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial. Es fundamental para la realización de un buen Plan Director de Seguridad, que se alinee con los objetivos estratégicos de la empresa, incluya una definición del alcance e incorpore las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización así como terceros que colaboren con ésta.

En la Figura. se indican un conjunto de proyectos que se pueden incluir en un PDS, y a los que se puede acceder desde la página de INCIBE. Dependiendo de cada empresa el plan tendrá mayor o menos complejidad y completitud; de todos ellos, hay uno especialmente importante: el análisis de riesgos, que todas las empresas deben hacer periódicamente.

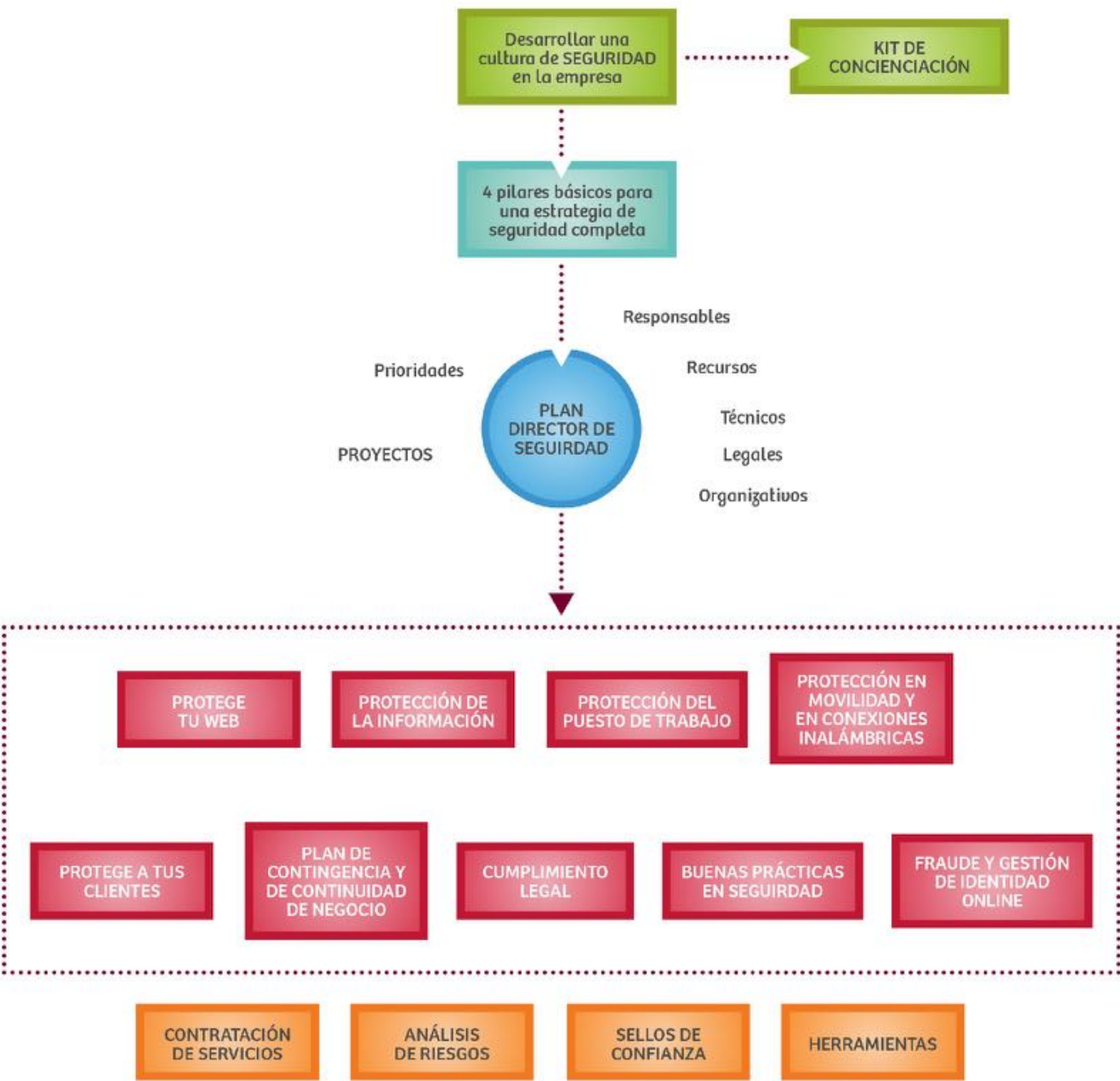


Fig.3.13.- Un visión del ámbito de la ciberseguridad para defenderse de la ciberdelincuencia.
Fuente: Elaboración propia





HÁBITOS A INCORPORAR

HÁBITOS PARA MEJORAR LA CIBERSEGURIDAD

Algunos hábitos, a adquirir, para mejorar la ciberseguridad de una empresa, negocio u organización son:

RESCATAR LAS
POLÍTICAS DE
SEGURIDAD DEL
PUESTO DE TRABAJO

DESARROLLAR UNA
CULTURA DE
SEGURIDAD

LANZAR UNA
CAMPAÑA DE
CONCIENCIACIÓN

HACER UNA BUENA
COPIA DE SEGURIDAD

ACTUALIZAR TODO EL
SOFTWARE

PROTEGER LA WIFI,
LOS MÓVILES Y LAS
CONEXIONES DESDE EL
EXTERIOR

SEGUIR Y CUIDAR LA
REPUTACIÓN Y LA
IDENTIDAD EN LA RED

CONTRATAR SERVICIOS
TIC, SI ES NECESARIO,
TENIENDO EN CUENTA
LA SEGURIDAD

HACER ANÁLISIS DE
RIESGOS PERIÓDICOS Y
ANTE CONTINGENCIAS

COMPROBAR LA
SEGURIDAD DE LA
PÁGINA WEB



PLAN DE CONTINGENCIA Y DE CONTINUIDAD EN EL NEGOCIO





La seguridad al 100% no existe. Las empresas deben estar preparadas, protegerse y reaccionar ante posibles incidentes de seguridad, que pudieran dañar su capacidad operativa o hacer peligrar la continuidad del negocio. Hay que estar preparados y ser capaces para dar una respuesta rápida y eficaz ante cualquier contingencia grave, de manera que se pueda recuperar la actividad normal, en un plazo de tiempo tal que no se vea comprometido el negocio.



Para ello hay que disponer de un Plan de Contingencia y Continuidad de Negocio, en el que se regulen los mecanismos a poner en marcha en caso de un incidente grave de seguridad. Estos mecanismos ayudarán a mantener el nivel de servicio en unos límitespredefinidos, establecerán un periodo de recuperación mínimo, recuperarán la situación inicial anterior al incidente, analizarán los resultados y los motivos del incidente, y evitarán la interrupción de las actividades corporativas.

En caso de desastre, el hecho de tener definido y poder aplicar un Plan de Contingencia y Continuidad de Negocio repercutirá positivamente en nuestra imagen y reputación, además de mitigar el impacto financiero y de pérdida de información crítica ante estos incidentes. En el enlace activo que se incluye se tratan los distintos tipos de proyectos de continuidad y las fases necesarias para implantar un plan.



El tema es tan importante que existen en la red una variedad de posgrados, títulos propios de universidades, cursos patrocinados por CC.AA. y de MOOCs gratuitos acerca de este aspecto crítico. Mediante cualquier buscador se puede acceder a los mismos; el mismo [INCIBE ofrece uno](#).

En la Figura se muestran tres categorías de agentes respecto de los que se toman medidas de ciberseguridad:

- Las empresas, negocios, organizaciones y sectores estratégicos.
- La ciudadanía, con un concepto más amplio que el de consumidor o cliente: “LA GENTE”.
- Los gobiernos en sus diferentes niveles de responsabilidad.

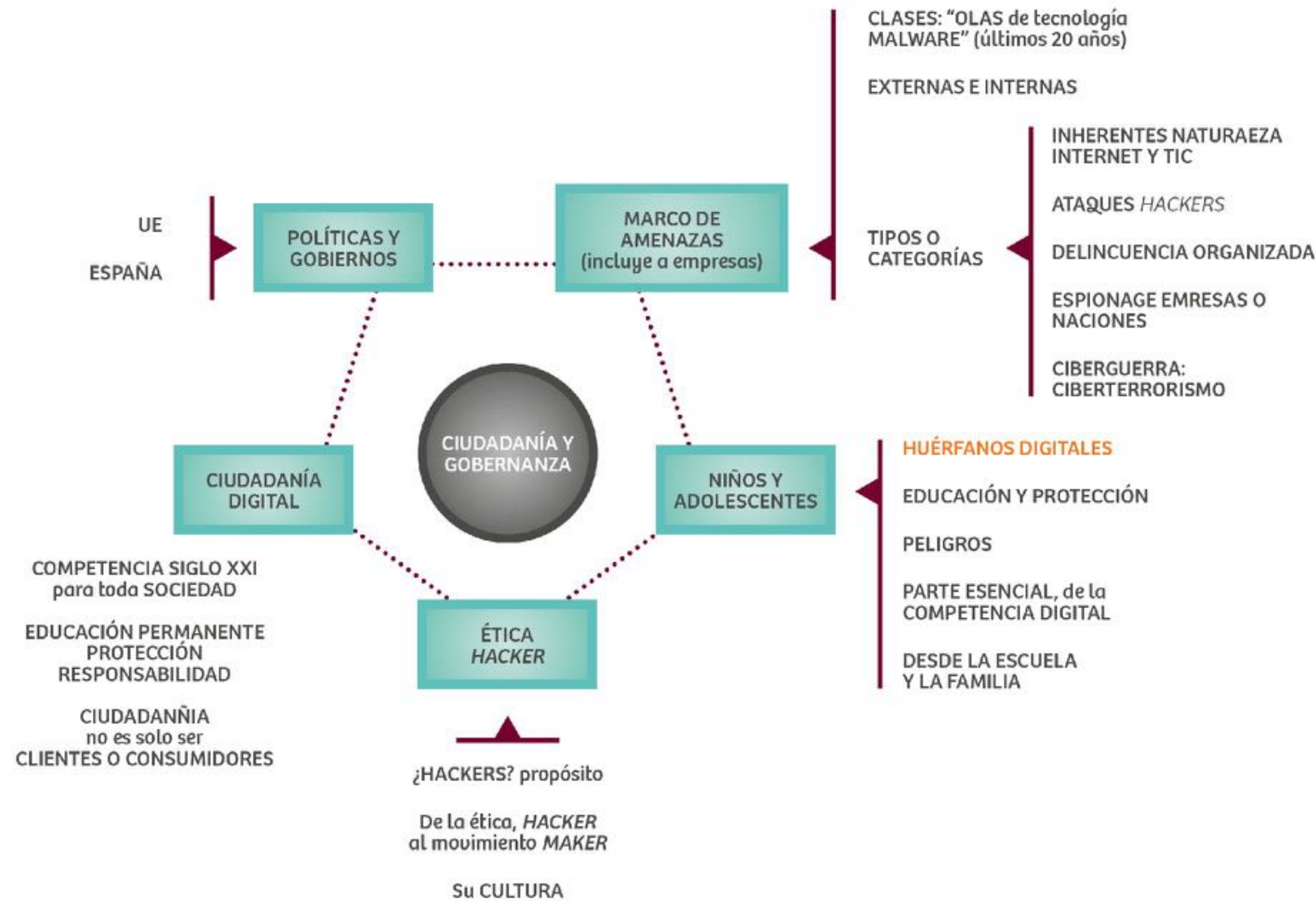


Fig.3.14. Aspectos seleccionados y priorizados, referentes a la ciudadanía y gobernanza multinivel.
Fuente: Elaboración propia



En estas pinceladas, como se indicó, se ha dado prioridad a la primera de ellas (empresas); lo cual no significa que sea la categoría más importante, sino que el curso se focaliza en ella. Por lo tanto, simplemente se dedicarán a la las otras dos unas consideraciones, de la forma más sucinta y visual posible - priorizando la selección que se encuentra en la parte inferior de la Figura además se orientará al alumno hacia fuentes, para ampliar o visitar regularmente los diferentes aspectos incluidos en la selección, cuando los necesite o dese

Por su novedad se tratan dos de ellas, resaltadas en la figura.

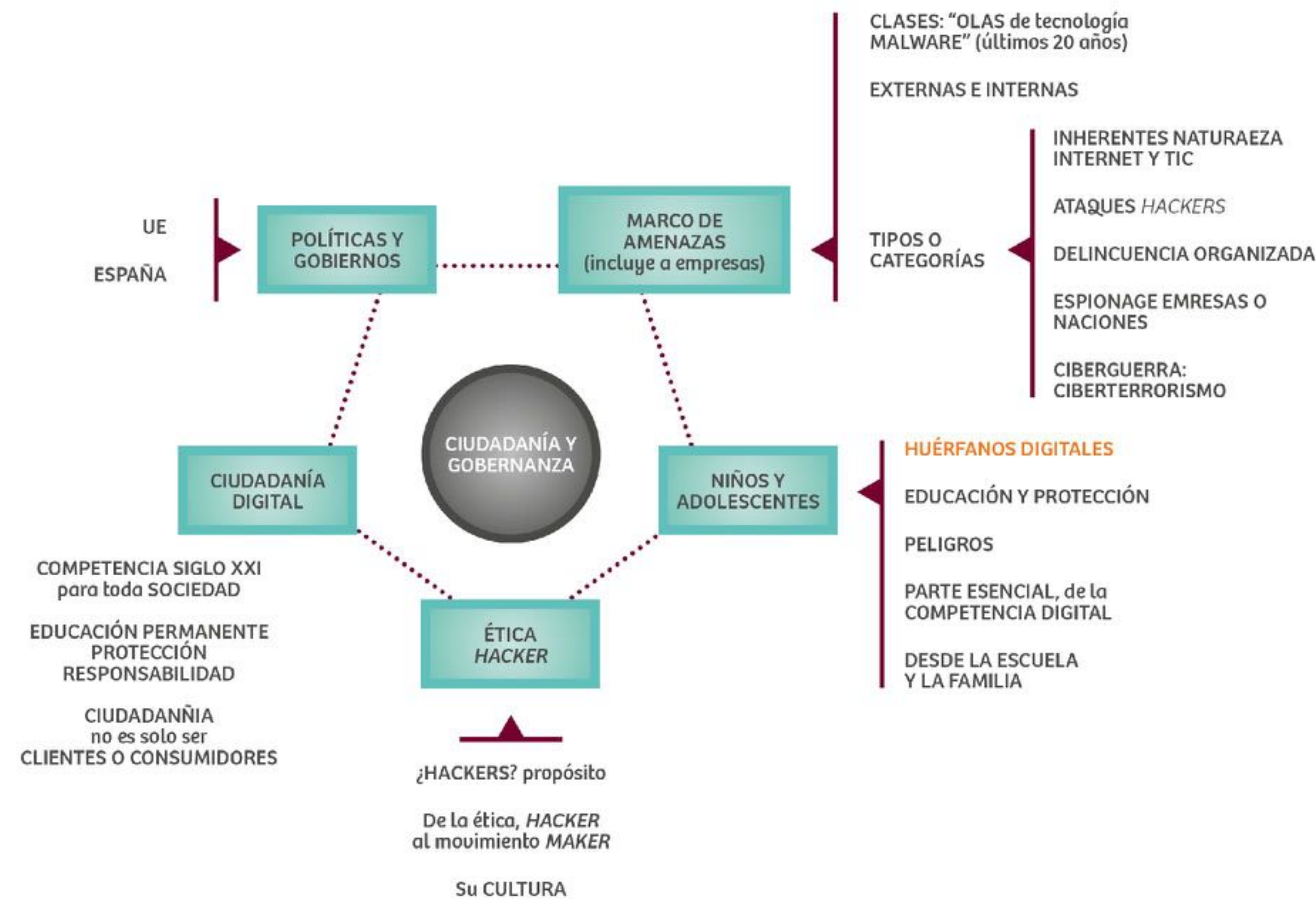


Fig.3.14. Aspectos seleccionados y priorizados, referentes a la ciudadanía y gobernanza multinivel.
Fuente: Elaboración propia



3

**PINCELADAS PARA
COMPLETAR LA
INTRODUCCIÓN A LA TD**

3.2

**LEGISLACIÓN Y
CIBERSEGURIDAD**

3.2.3.

La ética del hacker



La ética hacker es una ética del trabajo para el nuevo milenio, el siglo XXI

El artículo o la reflexión más profunda acerca de este aspecto es la realizada por Pekka Himanen en: “La ética del hacker y el espíritu de la era de la información”, 2011, avalada por el prólogo de Linus Torvalds y el epílogo de Manuel Castells, lo cual es toda una garantía.

Es conveniente conocer esta visión, ya que normalmente se les acusa -a **todos y siempre**- de muchas consecuencias asociadas al uso maligno de las tecnologías digitales, por gente muy creativa e innovadora.

El documento publicado por P. Himanen constituye una maravillosa base para la comprensión de lo que es un hacker, pero sobre todo, de la ética hacker. Así dice textualmente en el documento en español, que se puede descargar gratuitamente desde la red (Comunicación abierta, La Buchaca, entrada de 30 abril 2015):

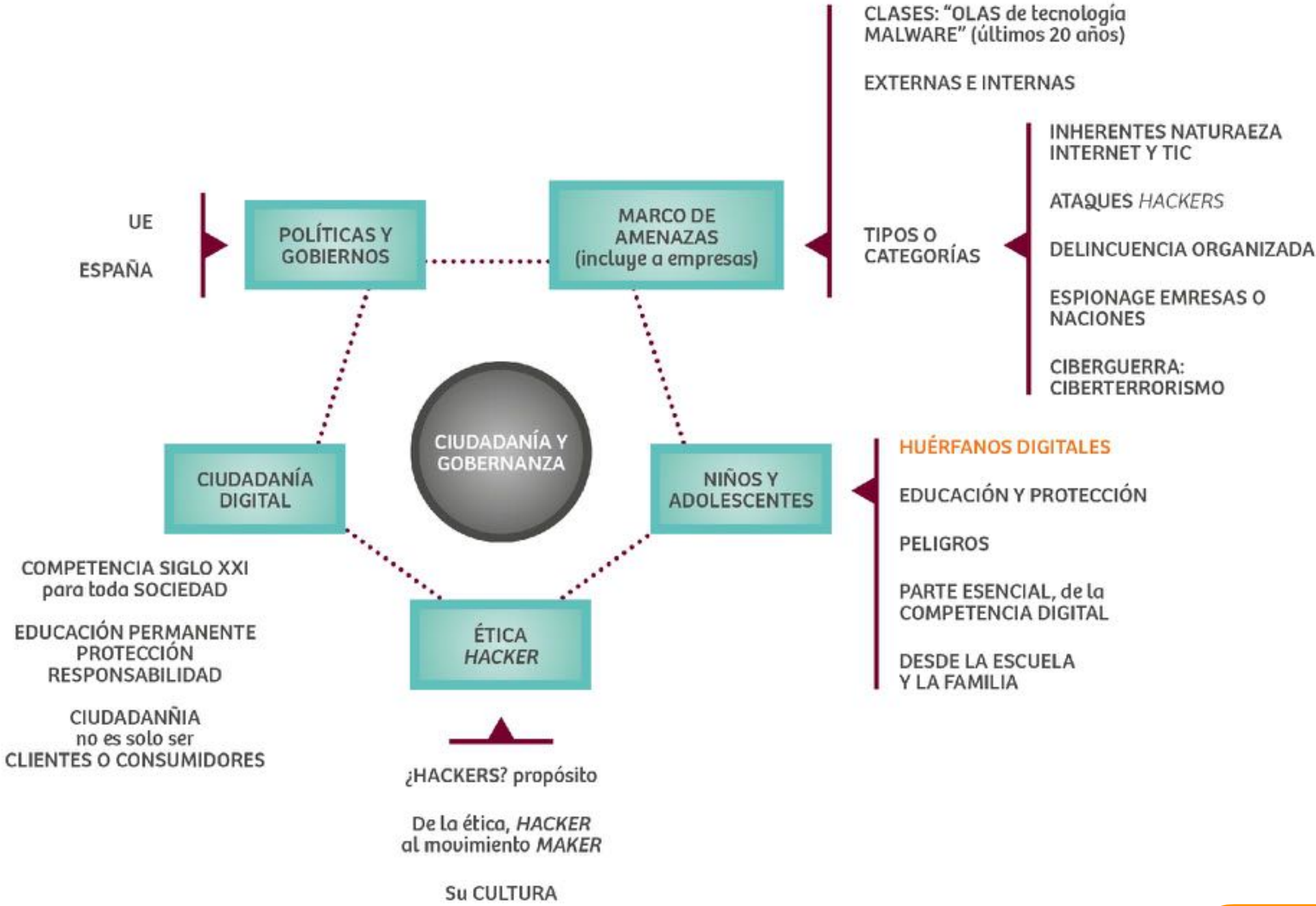
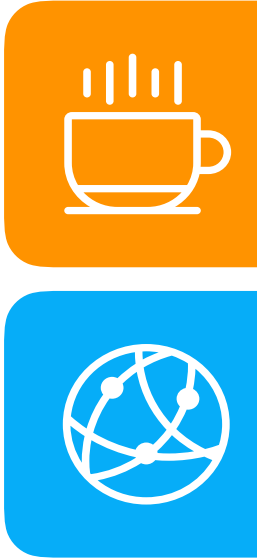


Fig.3.14. Aspectos seleccionados y priorizados, referentes a la ciudadanía y gobernanza multinivel.
Fuente: Elaboración propia





En el centro de nuestra era tecnológica se hallan unas personas que se autodenominan hackers. Se definen a sí mismos como personas que se dedican a programar de manera apasionada, y creen que es un deber para ellos compartir la información y elaborar software gratuito. No hay que confundirlos con los crackers, los usuarios destructivos cuyo objetivo es el de crear virus e introducirse en otros sistemas: un hacker es un experto o un entusiasta de cualquier tipo, que puede dedicarse o no a la informática. En este sentido, la ética hacker es una nueva moral que desafía la ética protestante del trabajo, tal como la expuso hace casi un siglo Max Weber en su obra clásica *La ética protestante y el espíritu del capitalismo*, y que está fundada en la laboriosidad diligente, la aceptación de la rutina, el valor del dinero y la preocupación por la cuenta de resultados. Frente a la moral presentada por Weber, la ética del trabajo para el hacker se funda en el valor de la creatividad, y consiste en combinar la pasión con la libertad. El dinero deja de ser un valor en sí mismo y el beneficio se cifra en metas como el valor social y el libre acceso, la transparencia y la franqueza.

Este pequeño en extensión es un gran libro que invita a recorrer las cuestiones fundamentales sobre la vida en la sociedad de la información (o posindustrial, sea cual fuere el nombre que se le dé), a emprender un viaje lleno de sorpresas que nos ayudará a orientar nuestras vidas hacia nuevas y apasionantes perspectivas.

La entrada de La Buchaca, sigue afirmando:

La ética hacker se expresa como una nueva relación con el tiempo, el dinero y el trabajo opuestas a la ética protestante en la que Max Weber vio los orígenes del capitalismo. El dinero deja de ser la medida del éxito y el motor de la acción, para dejar que el placer del conocimiento, del trabajo en sí mismo y la interacción y reconocimiento entre iguales ocupen su lugar. Con este nuevo conjunto de móviles, el [hacker](#) no entiende el trabajo como una «maldición» o como un tiempo de «no vida», opuesto y separado del «tiempo libre» o el ocio. Como decía el lema ciberpunk, para el hacker, «la vida es un pack».

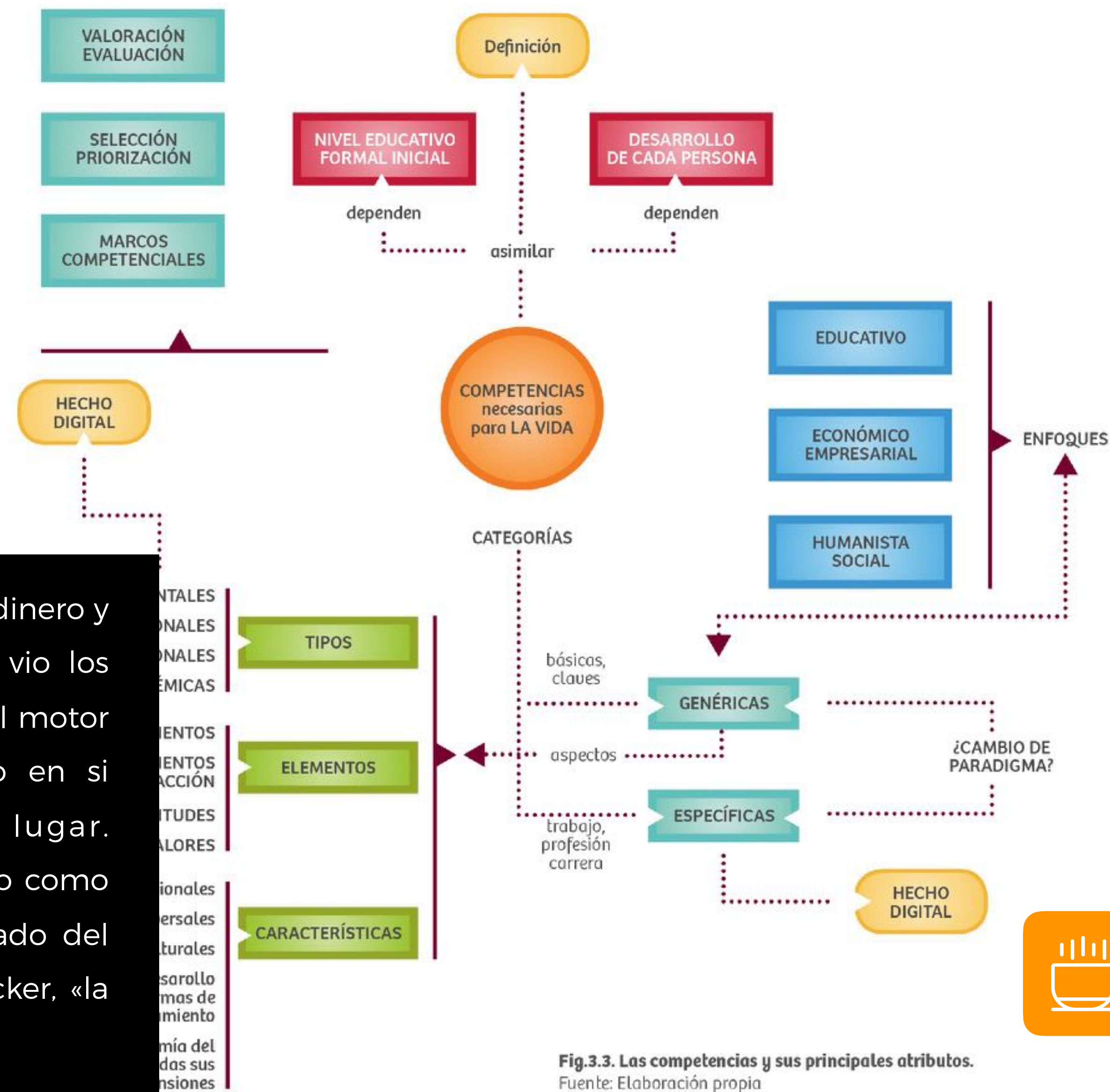


Fig.3.3. Las competencias y sus principales atributos.
Fuente: Elaboración propia



LA ÉTICA HACKER

Desde Indianopedia se hace el siguiente propuesta:

La ética hacker es el conjunto de valores que emergen de las primeras comunidades cooperativas de programadores, que se materializa luego en las primeras expresiones comunitarias en Internet y las comunidades de desarrolladores de software libre, y que podríamos resumir en tres puntos:

1



La afirmación de una nueva ética del trabajo a partir del conocimiento como motor y móvil principal de la actividad productiva, y la vida en comunidad más allá de su remuneración monetaria.

2



La afirmación de la **unidad y autonomía de la propia vida, a partir de la no aceptación de la separación entre tiempo de vida y tiempo de trabajo**, en la producción social de conocimiento (lo que a su vez, al ser la comunidad real el sujeto de esa producción, implica vindicación y práctica del pluriespecialismo).

3



La **libertad** como valor fundamental, materialización de esa autonomía personal y comunitaria. Frente a las instituciones existentes: el hacker no reclama que las cosas «se hagan», las hace él mismo y si reclama algo es que sean retiradas las trabas de cualquier tipo (monopolios, propiedad intelectual, etc.) que le impiden construir las herramientas del cambio por sí mismo en y con su comunidad.





- El mundo está lleno de problemas fascinantes que esperan ser resueltos.
- Ningún problema tendría que resolverse dos veces.
- El aburrimiento y el trabajo rutinario son perniciosos.
- La libertad es buena.
- La actitud no es sustituto para la competencia





Es conveniente tener también en cuenta esta perspectiva, para no dejarse llevar solo por la que transmiten los medios tradicionales y que llega a gran parte de la sociedad.

Posiblemente, en algunos de los hackers, la ética y el espíritu del trabajo se ha hecho materialista con el tiempo. Ahora bien, esta visión romántica y los valores en que subyace todavía la tiene muchos jóvenes, y no tan jóvenes, hackers que la crisis economista convirtió en emprendedores y a algunos en activistas al servicio del dinero.

Otra precisión necesaria es que una cosa es la visión de Himanen y otra la de los componentes de Indianopedia, posiblemente más radical.

3

**PINCELADAS PARA
COMPLETAR LA
INTRODUCCIÓN A LA TD**

3.2

**LEGISLACIÓN Y
CIBERSEGURIDAD**

3.2.4.

**Ciberseguridad a
nivel de la UE y de
España**





La Ciberseguridad tiene una dimensión que excede a las otras dos consideradas en este módulo. La propia defensa a nivel de un Estado Nacional o de la UE frente a los ataques que puede recibir de otros estados o de organizaciones terroristas de diferente índole.

UNIÓN EUROPEA



La UE ha creado [ENISA](#) (European Union Agency for Network and Information Security) es el centro experto en Ciberseguridad a nivel de Europa. Sus actividades se muestran en la infografía de la Figura. El mismo actúa tanto a nivel nacional público como privado; su sede se encuentra en Creta, Grecia.

Al mismo tiempo, ha propuesto (2013) una Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, que actualiza regularmente; una (2017) EU cybersecurity initiatives : working towards a more secure online environment; y, sin ánimo de completitud, el EU Cyber Defence Policy Framework (2014), para protección de las instituciones europeas.







El Estado Español tiene una “Estrategia de Ciberseguridad Nacional” (2013); en el mismo define los riesgos y amenazas a la Ciberseguridad Nacional,

Su objetivo general o meta es: Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques. La estrategia, para alcanzarlo, se articula a través de una serie de líneas de acción.

En un hecho que las fuerzas y cuerpos de seguridad del Estado, las empresas españolas y las AA.PP. necesitan expertos en ciberseguridad.





3

**PINCELADAS PARA
COMPLETAR LA
INTRODUCCIÓN A LA TD**

3.3

**LO QUE SE HA
QUEDADO EN EL
CAMINO**



Para terminar este capítulo y el módulo se ha optado por un apartado de misceláneas, es decir un pequeño conjunto de aspectos distintos y diferentes, que no han sido tratados, bien en esta Introducción bien en el conjunto del curso, cualquiera que sea el nivel que se siga. La selección es completamente subjetiva, como no puede ser de otro modo; podrá parecer adecuada a unas personas y a otras no. Incluso en la red se sugieren con más énfasis unas que otras, dependiendo las fuentes que se consulten, como consecuencia de sus prioridades, intereses y tendencias. Su extensión será corta y visual, y en la que no se incluirán referencias para ampliar o visitar frecuentemente. Los alumnos interesados simplemente tienen que utilizar la nube de etiquetas, que aquí se incluirán para llegar a sitios en Internet donde encontrarán lo que buscan.

Se comienza con la Figura en la que se muestra en unos rectángulos los cinco aspectos seleccionados. Los dos en la parte inferior se consideran que están descritos en la misma. Otros dos, se mostrarán mediante sendas imágenes, que se comentarán brevemente; y el superior que se describirá mediante texto.

:

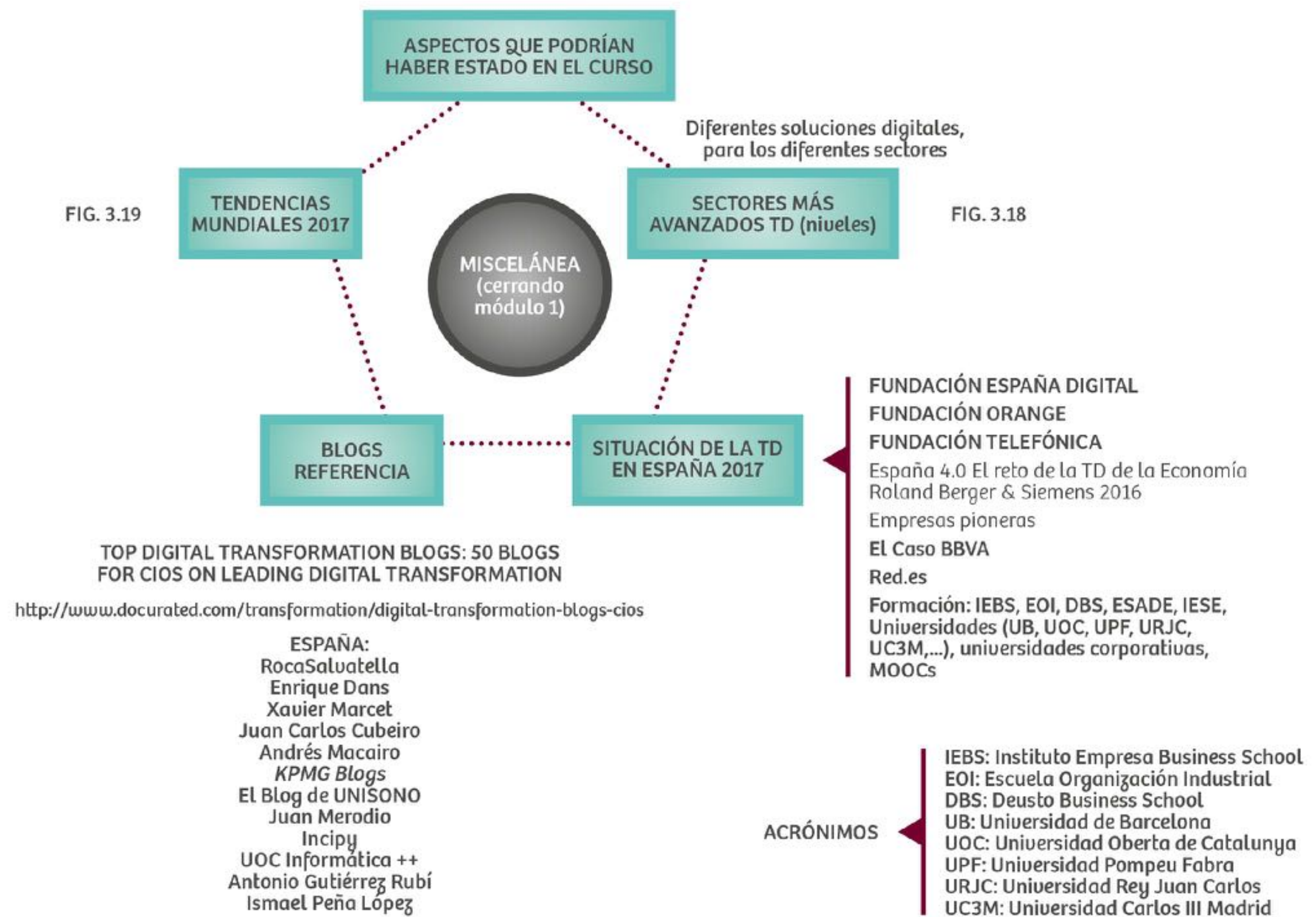


Fig.3.17. Miscelánea del apartado 3.3.
Fuente: Elaboración propia



3

**PINCELADAS PARA
COMPLETAR LA
INTRODUCCIÓN A LA TD**

3.3

**LO QUE SE HA
QUEDADO EN EL
CAMINO**

3.3.1.

**Aspectos que podrían
haberse incluido en
el curso**



ASPECTOS QUE PODRÍAN HABERSE INCLUIDO EN EL CURSO

Se podrían haber incluido a costa de otros que lo han sido, lo cual no es sencillo al definir como meta del curso la **TD de las empresas y negocios y, en menor grado, la de las organizaciones.**

Simplemente se da un listado de posibles aspectos, que pueden servir de orientación para otros cursos o satisfacer los intereses personalizados de cada alumno.

A

IMPORTANTES PARA CANARIAS



- 1.- La TD de la industria turística.
- 2.- La TD de PYMES y microempresas; y del mercado minorista.
- 3.- La TD de la educación.
- 4.- La TD de las AA.PP.
- 5.- La TD de la sociedad: desarrollo de la ciudadanía digital.

B

DE CARÁCTER GENERAL



- 6.- Desarrollo del talento en las organizaciones.
- 7.- La TD en el sector salud.
- 8.- La TD urbana.
- 9.- El cibervoluntariado.
- 10.- Del “Big Data” al “Fast Data”.

3

**PINCELADAS PARA
COMPLETAR LA
INTRODUCCIÓN A LA TD**

3.3

**LO QUE SE HA
QUEDADO EN EL
CAMINO**

3.3.2.

**Sectores de mayor impacto
de las tecnologías digitales
y sectores en que más se
ha avanzado en la TD**



Como se indicó se muestran mediante tres imágenes, ([enlace a las Fig. 3.18a, 3.18b, y 3.18c.](#)) En la primera de ellas se muestra un estudio realizado en agosto 2015, en la que diferentes ejecutivos, fundamentalmente de EE.UU, anticipaban una disrupción moderada o masiva, en diferentes tipos o sectores de actividad económica, en el plazo de un año.



Figura: Barómetro de la disrupción digital por sectores de negocios.
Fuente: Rusell Reynolds Associates, 2015.

:



Los estudios anuales (Digital Pulse) de esta empresa, Russell & Reynolds Associates, son los más reconocidos. En el Digital Pulse: 2017 los resultados son los que se muestran en la Figura anterior.

Conviene comparar este barómetro, para los sectores representados, con los correspondientes a 2015. Resalta: “las compañías de todos los sectores esperan que continúe la disrupción a lo largo de 2017; aunque los servicios financieros, la salud y las empresas industriales serán las que experimenten los cambios más significativos.

INDUSTRY REPRESENTATION
INTERNET/TECHNOLOGY DOMINATION



En un estudio publicado en Harvard Business Review (abril 2016): Which Industries Are the Most Digital (and Why)?, contesta con mayor precisión a la pregunta que interesa, ¿qué sectores son los más digitales y está avanzando la TD de sus empresas y organizaciones,

La imagen que se ha seleccionado es muy instructiva y elocuente en sí misma; conviene analizarla con detenimiento, que es fácil, a pesar de la complejidad que puede aparentar en una primera mirada.

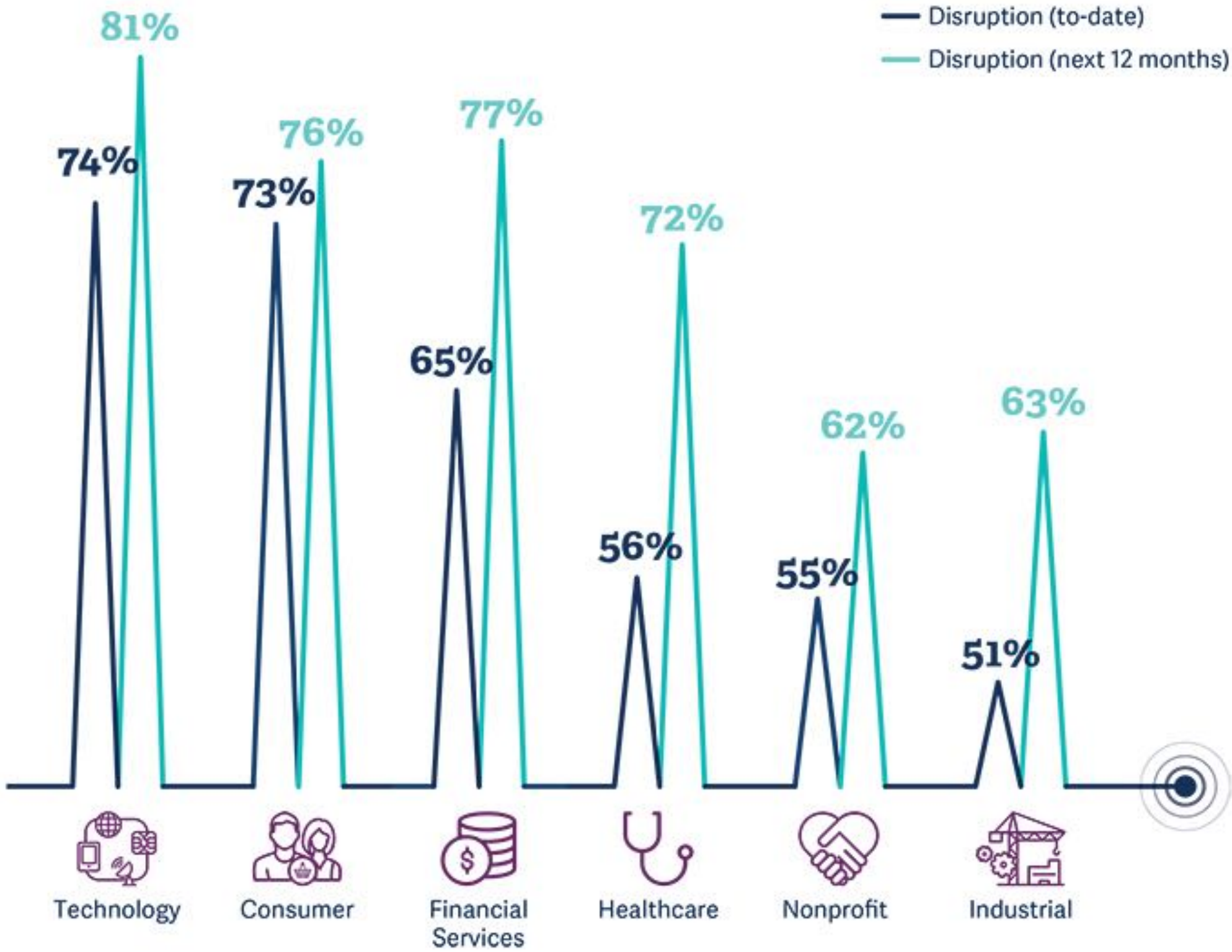


Figura: Barómetro Digital Pilsa: 2017
Fuente: Rusell Reynolds Associates, March 13, 2017.

3

**PINCELADAS PARA
COMPLETAR LA
INTRODUCCIÓN A LA TD**

3.3

**LO QUE SE HA
QUEDADO EN EL
CAMINO**

3.3.3.

**Tendencias
mundiales 2017**



Con las tendencias también ocurre que, dependiendo de las fuentes, se insiste más en unas que en otras. También hay que matizar que existen dos aspectos relacionados, aunque diferentes: a) Tendencias de la TD 2017, y b) Tendencias o innovaciones en tecnologías digitales 2017.

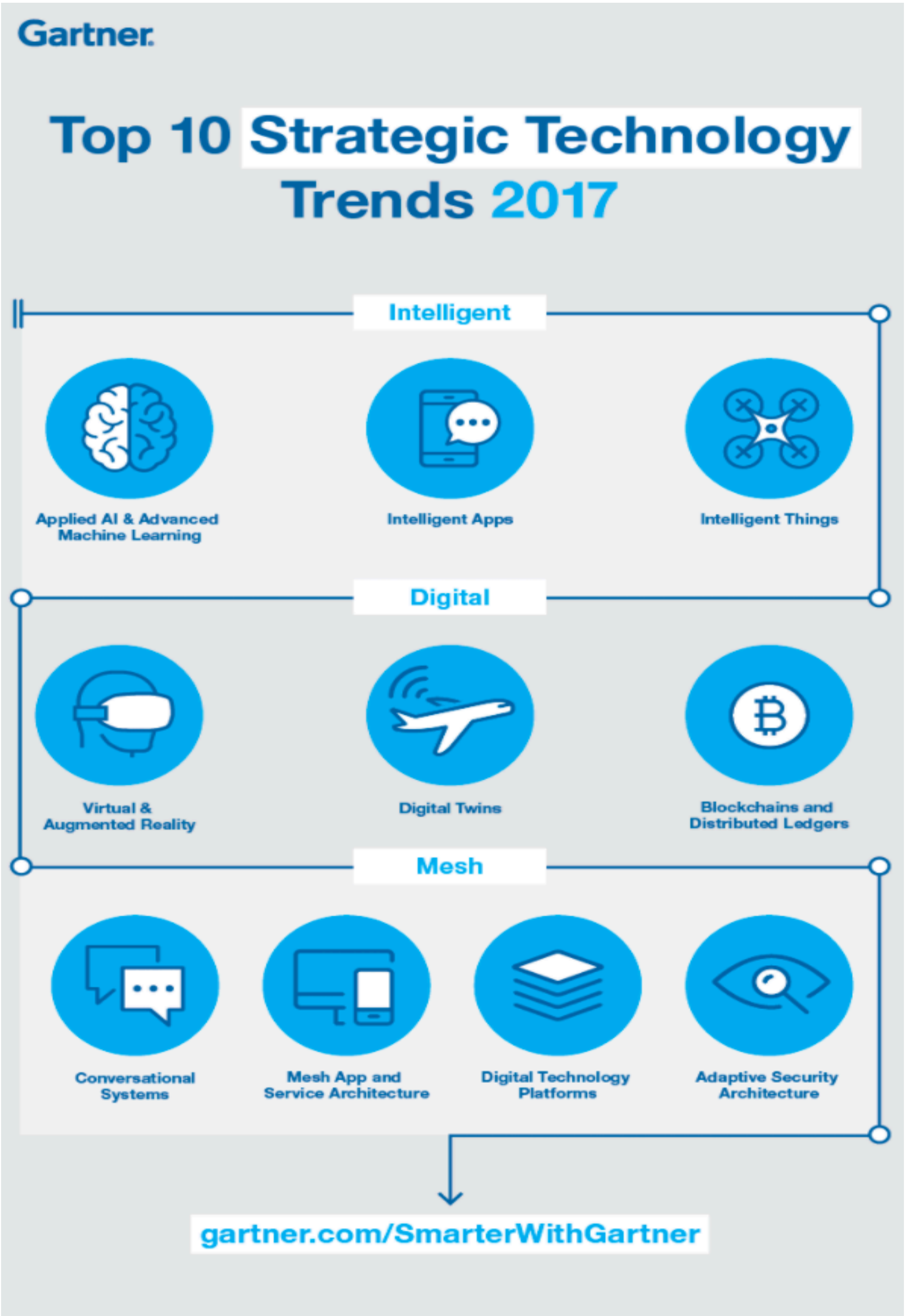


Figura: Tendencias tecnológicas estratégicas para 2017.
Fuente: Gartner, 2016.



En este módulo interesan más las relacionadas con la TD, que con las innovaciones estrictamente tecnológicas, ya que éstas corresponden más al módulo 2 de este curso. Para ello se ha recurrido a una de las consultoras tecnológicas con investigación más reconocidas en este aspecto, Gardner.

Por otra parte, cada vez son más comunes las prospectivas anuales relacionadas con aspectos de la TD en sectores concretos (p.e., salud, finanzas, seguros, etc).

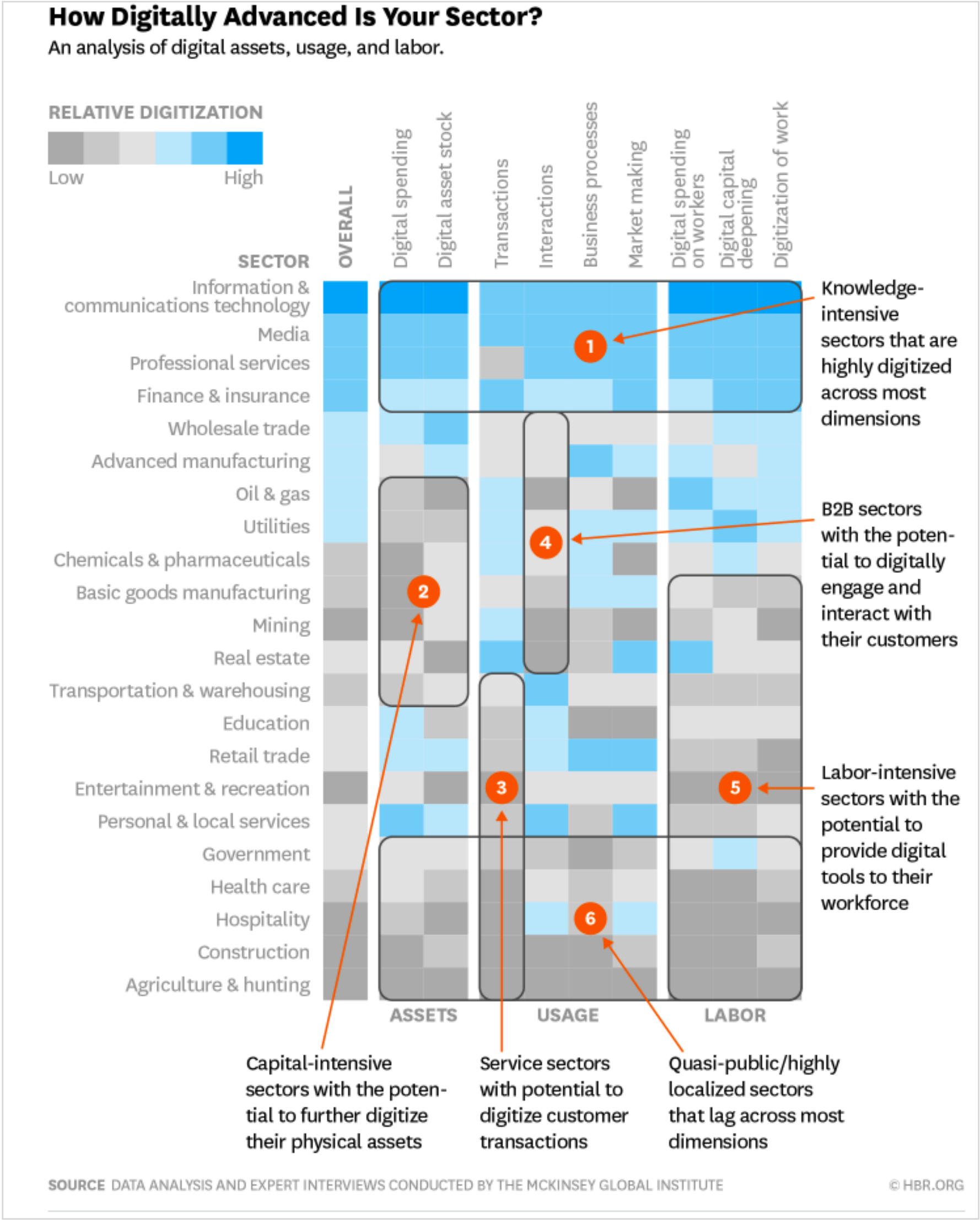
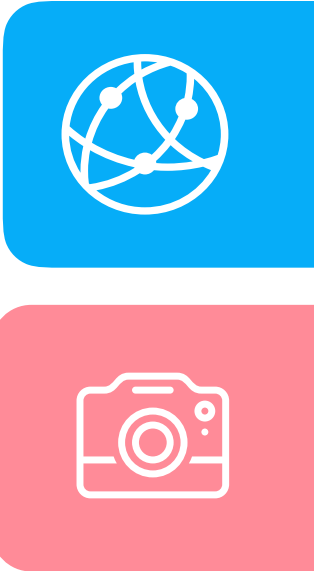


Figura: ¿Qué grado de maduración digital tienen en general las empresas de diferentes sectores económicos? .
Fuente: McKinsey Global Institute, 2016



Las tendencias previstas para 2017, en el aspecto de la TD de empresas y negocios en general, se han tomado las que se publicaron en la revista de negocios y finanzas Forbes, en agosto 2016.

El texto de Daniel Newman sintetiza todo (o parte) el módulo 1 desarrollado. Hay varias palabras y conceptos clave:

- TD no es una opción es una necesidad.
- Las organizaciones, en la TD (y sin ella), deben cambiar, tanto en su cultura como en su tecnología.
- Estamos en una época de negocios disruptivos.
- Necesitamos nuevos modelos de negocio.
- La única constante es el cambio.

ACRÓNIMOS

CIO: Chief Information Officer
CDO: Chief Digital Officer
CCO: Chief Customers Officer



There is no question that digital transformation is no longer an option as the need to build an organization that can change both its technology and its culture rapidly will be core to not only surviving in the time of business disruption, but building a business model that is agile, adaptable and designed to thrive long into the future where change is the only constant

Daniel Newman, Forbes.
AUG, 20, 2016

Fig. 3.19b. Algunas tendencias y previsiones para la TD en 2017.
Fuente: D.Newman en Forbes, 2016.

