Plan de confianza en el ámbito digital

Junio 2013

ÍNDICE

Introducción general

El 15 de febrero de 2013 el Gobierno aprobó la Agenda Digital para España como "marco de referencia para establecer una hoja de ruta en materia de Tecnología de la Información y las Comunicaciones (TIC) y de administración electrónica; establecer la estrategia de España para alcanzar los objetivos de la Agenda Digital para Europa; maximizar el impacto de las políticas púbicas en TIC para mejorar la productividad y la competitividad; y transformar y modernizar la economía y sociedad española mediante un uso eficaz e intensivo de las TIC por la ciudadanía, empresas y Administraciones".

La Agenda, configurada como estrategia global, define los objetivos a alcanzar y sus indicadores asociados, así como las líneas de actuación que se deben desarrollar para conseguirlos. Como estrategia global, la Agenda se ha utilizado y se sigue utilizando como guía principal de las actuaciones que el Gobierno ha desarrollado y desarrolla en el ámbito de las TIC en España.

Para el desarrollo óptimo de la Agenda se contemplaba la elaboración de un conjunto de planes específicos, de los cuales siete de ellos estarían disponibles en la primera parte del año y dos en la segunda parte, una vez se dispusiera de las conclusiones de la Comisión para la Reforma de las Administraciones Públicas.

En este documento se presenta el Plan de confianza del ámbito digital, uno de los siete planes que debía estar disponible en la primera parte del año. Este Plan concreta en medidas específicas, con calendarios precisos y con los presupuestos requeridos las actuaciones a desarrollar para conseguir los objetivos establecidos en la Agenda. En este sentido, se podría decir que muestra cómo hacer lo que la Agenda indicaba que había que hacer.

En el proceso de elaboración de todos los planes se ha partido de un análisis detallado de la situación actual y de los resultados de planes anteriores; se han analizado las debilidades, amenazas, fortalezas y oportunidades de la situación actual así como las consecuencias de las distintas alternativas de actuación que se presentaban. Finalmente se ha realizado la selección de las medidas que se incluyen en cada uno de los planes.

Las medidas presentadas tienen un alcance temporal hasta el 2015, si bien, de acuerdo con lo establecido en la Agenda, cada año se realizará una revisión de los planes para evaluar los resultados conseguidos, determinar la necesidad o no de adaptación de objetivos y medidas y, en su caso, prolongar el alcance temporal para cumplir los objetivos ya marcados en la Agenda Digital para Europa o aquellos adicionales que se establezcan. Este mecanismo de revisión podrá extenderse hasta el año 2020.

En el proceso de elaboración de cada uno de los planes han participado diversos agentes, dependiendo del contenido y alcance del plan. Existen planes cuyo desarrollo corresponde íntegramente a la Administración General del Estado y otros en los que no sólo en su concepción, sino que incluso en su desarrollo, se contempla ya de partida la participación de otros agentes.

Estos planes han sido elaborados, mayoritariamente, en el marco de las actuaciones la Administración General del Estado pero tienen la vocación de ser "planes abiertos". Es decir, planes sometidos a un proceso de revisión y adaptación continuo, abiertos a la participación y a la colaboración con el resto de Administraciones y con los agentes económicos y sociales, así como con las actuaciones que estos desarrollen.

La publicación de los planes facilita la coordinación con las actuaciones que tanto administraciones como sociedad están desarrollando y permite buscar sinergias adicionales a las ya presentes en los planes actuales. Los siete planes correspondientes a la primera mitad del año 2013 son:

Plan de telecomunicaciones y redes ultrarrápidas

El Plan de telecomunicaciones y redes ultrarrápidas tiene como objetivo impulsar el despliegue de redes de acceso ultrarrápido a la banda ancha, tanto fijo como móvil, y fomentar su adopción por ciudadanos, empresas y administraciones. Para ello, el Plan combina medidas normativas con el fomento de la oferta de redes y el estímulo de la demanda. Si bien las medidas tienen un alcance temporal al 2015, el Plan se ha diseñado con un horizonte a 2020 para dar cumplimiento a los objetivos de banda ancha fijados por la Agenda Digital para Europa.

Plan de TIC en PYME y comercio electrónico

Las TIC son una de las palancas para mejorar la competitividad de las empresas de forma sostenible, fomentar su crecimiento e innovación, ayudar en su expansión internacional y contribuir a la mejora del empleo desde una perspectiva tanto cuantitativa como cualitativa. El Plan de TIC en PYME y comercio electrónico se orienta a conseguir que las empresas realicen un uso más eficiente e intensivo de las tecnologías digitales, transformando así sus procesos y estructuras en aras de mejorar su productividad y competitividad. Para ello el Plan establece medidas para incentivar el uso transformador de las TIC en las PYME, para fomentar el uso de la factura electrónica y para impulsar el comercio electrónico en España.

Plan de impulso de la economía digital y los contenidos digitales

En España, la importancia estratégica de la economía digital y de los contenidos digitales ha sido reconocida por la Agenda Digital para España como motor de crecimiento, de empleo y de oportunidades futuras. El Plan de impulso de la economía digital y los contenidos digitales ha sido diseñado con la participación de la administración pública y el sector privado, y persigue el desarrollo de la economía digital mediante un conjunto integral de medidas que impactan en los distintos agentes del ecosistema de la economía digital. Para ello el Plan establece medidas para incrementar el talento en torno a este nuevo sector, facilitar el emprendimiento y el crecimiento de las empresas, incrementar la producción de contenidos digitales y fomentar la reutilización de la información del sector público.

Plan de Internacionalización de empresas tecnológicas

El Plan de Internacionalización de empresas tecnológicas, acordado en el marco del Grupo de Trabajo Interministerial para la Internacionalización de la Empresa, tiene como objetivo ayudar a las empresas tecnológicas a iniciar el camino de la internacionalización, proporcionarles las

condiciones y soporte necesario para continuar en ese camino con las mayores garantías de éxito y facilitar la inversión extranjera directa en el sector TIC.

Plan de confianza en el ámbito digital

El Plan de Confianza Digital hace suyo el mandato conjunto de la Agenda Digital para España, de la Estrategia Europea de Ciberseguridad y de la Estrategia de Seguridad Nacional para avanzar en los objetivos conjuntos de construir un clima de confianza que contribuya al desarrollo de la economía y la sociedad digital, disponer de un ciberespacio abierto, seguro y protegido, garantizar un uso seguro de las redes y los sistemas de información, y responder a los compromisos internacionales en materia de ciberseguridad.

Plan de desarrollo e innovación del sector TIC

El Plan de Desarrollo e Innovación del sector TIC tiene como objetivo general la mejora de la competitividad de las industrias del sector TIC. Este Plan se alinea con el Plan Estatal de Investigación Científica y Técnica y de Innovación 2013-2016 en el que se ha recoge una Acción Estratégica en Economía y Sociedad Digital 2013-2016. El Plan implementa los instrumentos transversales de la Agenda Digital para, a través de mecanismos de concurrencia competitiva, impulsar el desarrollo de la I+D+i para superar los retos planteados en la evolución hacia una economía y una sociedad digital.

Plan de inclusión digital y empleabilidad

El Plan de Inclusión Digital y Empleabilidad se ha desarrollado con la participación de un conjunto amplio de agentes público y privados y sirve de paraguas a las iniciativas de todos ellos, aúna esfuerzos y multiplica el efecto de las medidas que se adopten. El Plan es el resultado de las aportaciones de múltiples actores, públicos y privados, que se han incorporado para sumar esfuerzos en el objetivo común de aumentar la accesibilidad de Internet, avanzar en la alfabetización digital, disminuir la brecha digital de género y mejorar la empleabilidad en España.

Plan de confianza en el ámbito digital

Introducción

El establecimiento de un clima de confianza en el ámbito digital es imprescindible para que las TIC contribuyan al desarrollo económico y social del país. Conseguirlo es una tarea compleja que precisa del compromiso de las administraciones, de las empresas y de la ciudadanía.

La construcción de un clima de confianza requiere actuar sobre diferentes ámbitos, entre ellos la ciberseguridad, el respeto y la protección de la privacidad, el uso responsable y seguro de servicios y contenidos, la protección de colectivos especialmente vulnerables, la resistencia y fortaleza de las infraestructuras tecnológicas de las que somos especialmente dependientes, la gobernanza, la seguridad jurídica de las relaciones personales y económicas en dicho entorno, así como la protección del consumidor en Internet.

Por todo ello, la Agenda Digital para España (ADpE) incorporó como uno de sus objetivos principales el compromiso de desarrollar las medidas necesarias para contribuir a la construcción de un clima de confianza en el ámbito digital. Este compromiso se materializa a través de un Plan específico cuyo alcance se restringe exclusivamente al mercado digital interior, la ciudadanía, las empresas, la industria, los profesionales y con carácter prioritario las empresas de especial trascendencia económica.

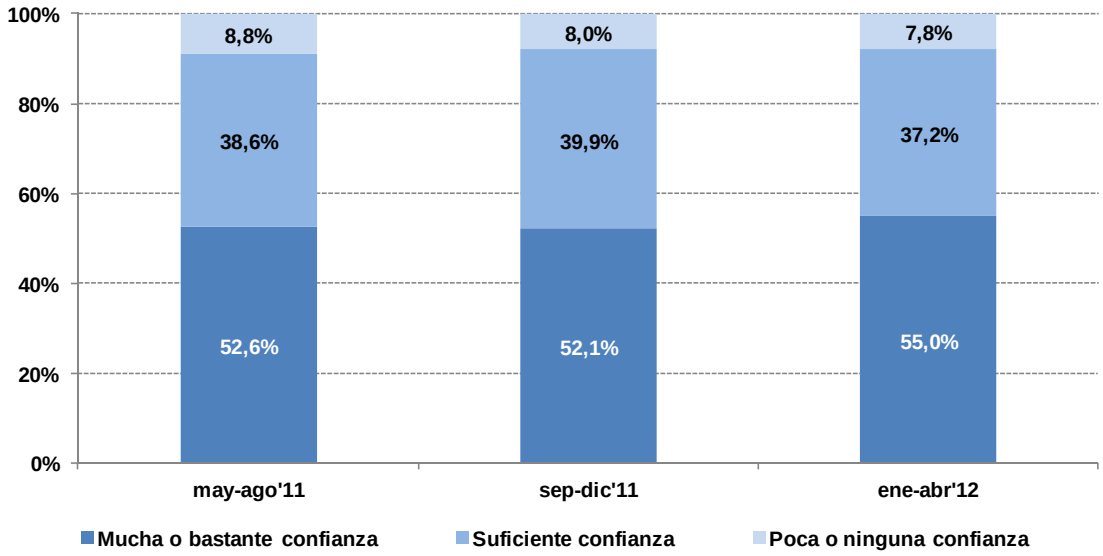
El Plan de confianza en el ámbito digital incorpora además los compromisos que se derivan de otras estrategias o políticas públicas relacionadas con la confianza digital, que se dirigen al alcance objetivo de este Plan, pero que se han publicado con posterioridad a la ADpE. En primer lugar responde a la Estrategia Europea de Ciberseguridad (EUCS), reforzada por las Conclusiones de Consejo de la Unión Europea del 25 de junio de 2013, que tiene por objetivo un ciberespacio abierto, seguro y protegido. En segundo lugar, responde también a la Estrategia de Seguridad Nacional (ESN), de 31 de mayo de 2013, que reserva una línea de acción para la ciberseguridad con el objetivo de garantizar un uso seguro de las redes y los sistemas de información a través del fortalecimiento de nuestras capacidades de prevención, detección y respuesta a los ciberataques.

El Plan de confianza en el ámbito digital, por tanto, hace suyo los compromisos de la ADpE, de la EUCS y de la ESN en los ámbitos de la confianza digital y en alcance objetivo del mercado digital interior, la ciudadanía, las empresas, la Industria y los profesionales, proponiendo un conjunto de medidas que contribuyen a darles cumplimiento y alcanzar los objetivos conjuntos, en colaboración con todos los agentes implicados.

Situación actual

Para que las nuevas tecnologías digitales puedan desarrollar todo su potencial es preciso que inspiren confianza a los ciudadanos y a las empresas. Desafortunadamente, una encuesta del Eurobarómetro[1] de 2012 mostraba que casi una tercera parte de los europeos dudaba de su capacidad para utilizar Internet en sus trámites bancarios o sus compras.

En España, en el primer cuatrimestre de 2012, el 55% de los usuarios confiaban mucho o bastante en Internet[2]. El reto de elevar este indicador hasta el 70% en 2015 ha sido recogido por la ADpE en su objetivo de confianza digital.



Pregunta: En general, ¿cuánta confianza le genera Internet?
Fuente: INTECO

En cuestiones de privacidad, la encuesta del Eurobarómetro muestra que en relación con el resto de países de la Unión Europea, España ocupa la primera posición en cuanto a preocupación de los ciudadanos sobre la protección de la información de datos personales, tanto en el ámbito público como en el privado.

Según un reciente Barómetro del CIS[3], entre las preocupaciones destacan las dificultades para hacer un buen uso de las políticas de privacidad y la percepción que de ellas tiene la ciudadanía. Esta afirmación se pone de manifiesto en:

- El 31,2% reconoce que nunca lee las políticas de privacidad de las páginas de Internet que visita y un 28% lo hace raramente.

[1] Comisión Europea (2012): Eurobarómetro especial sobre ciberseguridad. Número 390. Más información disponible en: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf
[2] INTECO (2012): Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles, 1er cuatrimestre de 2012 (18ª oleada). Más información disponible en: http://www.inteco.es/Estudios/Estudio_hogares_1C2012
[3] Centro de Investigaciones Sociológicas (CIS). Barómetro. Mayo 2013. Más información disponible en: http://www.cis.es/cis/opencms/ES/9_Prensa/Noticias/2013/prensa0256.html

- El 34,2% indica que más que informar correctamente, lo que buscan es evitar problemas legales y un 42,3% está bastante de acuerdo con dicha afirmación.
- El 70,3% considera que las políticas de privacidad y la información que se ofrece en los sitios de Internet sobre el tratamiento de datos son poco o nada claras.
- Finalmente el 65,5% señala que los sitios web intentan que no se sepa qué van a hacer con los datos personales de los que disponen.

Respecto a los ciberataques, los afectados en 2012 fueron más de 556 millones de personas en todo el mundo, más de 1,5 millones de personas cada día, estimándose el impacto económico en Europa en 12 mil millones de euros[4]. La mayor amenaza actual es el ciberespionaje provocado por ataques dirigidos, cuyo coste medio per cápita se calcula en torno a 72 euros en Italia, 90 euros en el Reino Unido, 119 euros en Francia y 143 euros en Dinamarca, encabezando la lista Estados Unidos con 145 euros per cápita.

En cuanto a las transacciones electrónicas la falta de confianza ha sido el principal inhibidor del desarrollo y extensión de las relaciones a distancia, sean o no de naturaleza comercial.

En Europa, para el año 2011 el 42,7% de la población realiza habitualmente compras por Internet. España aún queda lejos de esa cifra con un 27,3%. Comparado con la media de los países de la Unión Europea, los españoles muestran una mayor desconfianza en la utilización de Internet para realizar actividades como la banca online o compra de productos online, con una diferencia de un 20%[5].

[4] Symantec (2013): Internet Security Threat Report 2013, Volume 18. Más información disponible en: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[5] Comisión Europea (2012): Eurobarómetro especial sobre ciberseguridad. Número 390. Resultados en España. Más información disponible en http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_fact_es_es.pdf

Objetivos del Plan

El objetivo del Plan de confianza en el ámbito digital para el mercado digital interior, la ciudadanía, las empresas, la industria y los profesionales es dar respuesta a los compromisos en materia de confianza digital contemplados en las siguientes estrategias:

1. El objetivo cuatro de la Agenda Digital para España (ADpE).
2. Las prioridades relativas a la ciberresiliencia, la concienciación y el desarrollo de los recursos industriales y tecnológicos de la Estrategia Europea de Ciberseguridad (EUCS).
3. La línea estratégica de ciberseguridad de la Estrategia de Seguridad Nacional (ENS).

El análisis de los compromisos anteriores junto al análisis de la situación, permiten identificar los siguientes objetivos específicos para el Plan de confianza en el ámbito digital:

1. Experiencia digital segura: Impulsar las medidas que permitan a la ciudadanía y las empresas disfrutar de una experiencia segura y confiable aprovechando todas las oportunidades de la economía y la sociedad digital, tomando conciencia sobre los riesgos que el ecosistema digital puede presentar, adoptando prácticas excelentes para la gestión adecuada, responsable e informada de los riesgos, en particular para las empresas de especial trascendencia económica y los colectivos más vulnerables como son la infancia y la adolescencia.
2. Capacidades para la resiliencia: Desarrollar las capacidades necesarias para afrontar el reto de la ciberseguridad en la economía y sociedad digital y hacer frente a los compromisos de prevención, detección y respuesta que necesita el mercado interior digital, la industria, las empresas, el mundo académico y la ciudadanía, y con carácter prioritario las empresas de especial trascendencia económica, contribuyendo en su caso a la seguridad pública mediante instrumentos de colaboración.
3. Oportunidad para la industria y los profesionales: Contribuir a que la industria, el sector académico y los profesionales aprovechen la oportunidad de la confianza digital para la innovación, la generación de talento y la investigación avanzada, especialmente en materia de ciberseguridad, construyendo un mercado de productos y servicios competitivo y de referencia internacional.

En cuanto a los indicadores, se emplearán los de la ADpE en este ámbito:

Indicadores objetivo del Plan de confianza en el ámbito digital	Valor a alcanzar	Año	Valor base España (2011)	Valor base UE27 (2011)
Personas que han usado medios de seguridad	70%	2015	56% (2010)	60% (2010)
Confianza generada por Internet (% de usuarios que confían mucho o bastante en Internet)	70%	2015	52%	s.d.
Empresas que utilizan firma digital en alguna comunicación enviada desde su empresa (% sobre el total de empresas con conexión a Internet)	85%	2015	70,7% (2012)	s.d.
Empresas que disponen en su sitio web de una declaración de política de intimidad o de una certificación relacionada con la seguridad del sitio web (% sobre el total de empresas con conexión a Internet y página web)	75%	2015	61,2% (2012)	s.d.

Estructura del Plan

Las medidas que se proponen contribuyen a dar respuesta a los compromisos estratégicos de la ADpE, la EUCS y la ESN, así como a los objetivos establecidos en el Plan, reconociendo, complementando y reforzando, en su caso, las iniciativas que en materia de confianza digital se están realizando por distintos agentes públicos y privados en el ámbito y alcance de este Plan, favoreciendo la coordinación de todos los actores, impulsando la racionalización de los esfuerzos y la mejora de la eficacia y del impacto de las actuaciones. Las medidas se organizan en los siguientes ejes:

Eje I: Experiencia digital segura

La ADpE, la EUCS y la ESN y las estrategias para la protección de la infancia y la adolescencia, consideran esencial la sensibilización y la concienciación de los usuarios para aumentar la confianza y el buen uso de Internet.

En este ámbito, se han realizado numerosas actuaciones públicas[6] y privadas[7] en los últimos años con el objetivo de incrementar la confianza en Internet, especialmente en aspectos relacionados con la seguridad de la información, la protección de la privacidad, el comercio electrónico seguro y el uso responsable y seguro de la tecnología por la infancia y la adolescencia, entre otros.

Sin embargo, en España son pocos los casos de colaboración público-privada para el desarrollo de estas iniciativas, a pesar del éxito que esta colaboración ha reportado en otros países de nuestro entorno[8]. Por ello, se propone impulsar la cooperación público-privada para las acciones de sensibilización y concienciación, diseñando una estrategia conjunta y explorando en paralelo la oportunidad y viabilidad del desarrollo de itinerarios educativos para la confianza digital que pudieran ser adoptados por las autoridades competentes en la materia.

Eje II: Oportunidad para la industria TIC

La ADpE, la ESN y la EUCS establecen líneas de acción estratégica para el impulso de la industria de la ciberseguridad y de los servicios de confianza. Las tres estrategias apuestan por establecer mecanismos de impulso a la I+D+i, de estímulo a la demanda por medio de la adopción de normas y buenas prácticas, la apuesta por la normalización como valor diferencial, el estímulo de los esquemas de certificación y acreditación, y la apuesta por la cooperación público-privada como herramienta para la mejora de los ciclos de innovación entre la industria y el mundo académico.

La ADpE ya contempla entre sus objetivos el impulso de la I+D+i en TIC cuyo compromiso se llevará a cabo a través del Plan de desarrollo e innovación del sector TIC y del Plan de internacionalización de empresas tecnológicas. El impacto de estos instrumentos en materia

[6] Policía 2.0 (https://twitter.com/policia) o la Oficina de Seguridad del Internauta (http://www.osi.es)

[7] www.protegetuinformacion.com es un proyecto promovido por la Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, financiado con fondos del Plan Avanza de la SETSI.

[8] Destacan la plataforma Plataforma "getsafeonline" del gobierno UK (http://www.getsafeonline.org) o la del gobierno US en www.staysafeonline.org. Otras referencias de plataformas son las de la República Checa (http://www.saferinternet.cz/o-nas/o-nas.html) y la de Noruega (http://www.sikkert.no)

de confianza digital es necesario que se refuerce mediante el establecimiento de estructuras de coordinación entre los distintos agentes implicados que aseguren la necesaria eficiencia, que compartan prioridades e información de demanda temprana, que dispongan de asesoramiento experto para la evaluación de proyectos, que sincronicen convocatorias y que construyan una oferta unificada e integrada para todo el ciclo de la I+D+i. Estas medidas estarán acompañadas de iniciativas para promover el desarrollo de normas técnicas, la adopción de buenas prácticas y el impulso de esquemas certificados de productos y servicios.

Eje III: Nuevo contexto regulatorio

La adopción temprana de la nueva regulación europea combinada con el impulso de la autorregulación y la disponibilidad de un mapa de indicadores fiable sobre el nivel de confianza digital en España, se configuran como elementos claves para aumentar la confianza de ciudadanos y empresas en Internet, así como para mejorar los niveles de ciberseguridad en España.

Eje IV: Capacidades para la resiliencia: INTECO 2.0

La EUCS y la ESN plantean la necesidad de reforzar las capacidades de prevención, detección y respuesta frente a los ciberataques. La ADpE por otro lado, plantea como línea de actuación convertir a INTECO en un centro de referencia para la confianza digital, especialmente en materia de ciberseguridad.

En el alcance objetivo de este Plan, INTECO es la entidad de referencia que viene prestando estos servicios para empresas y ciudadanos desde 2007. Durante 2012 se han gestionado más de 100.000 incidentes de seguridad y se han producido más de 6 millones de visitas y accesos al año a sus servicios. En consecuencia, es necesario aprovechar e incrementar la capacidad de INTECO, focalizando su actividad en el área de la confianza digital y la ciberseguridad en el mercado interior digital, la industria, las empresas, el mundo académico y la ciudadanía, y con carácter prioritario en las empresas de especial trascendencia económica.

Eje V: Programa de excelencia en ciberseguridad

La ESN establece como línea de acción estratégica la promoción de la capacitación de profesionales en ciberseguridad al igual que la ADpE plantea la necesidad de crear talento en ciberseguridad. Los principales países de nuestro entorno están llevando a cabo actuaciones innovadoras para la generación de talento en ciberseguridad. España debe hacer un esfuerzo en esta línea para que, una vez formado, los profesionales puedan encaminarse hacia la investigación avanzada, la incorporación a centros de respuesta a incidentes y la formación de otros expertos.

Este eje pretende construir un ecosistema de captación y generación de talento en torno a INTECO, en colaboración con las universidades y la iniciativa privada, buscando siempre la acción complementaria de las iniciativas que otros agentes están desarrollando para la capacitación de profesionales.

Medidas

Plan de confianza en el ámbito digital 2013-2015		59,0 M€
Eje I: Experiencia digital segura		**5,8 M€**
1	**Plan de sensibilización de INTECO** INTECO simplificará, reorientará y reforzará las actuaciones de sensibilización, concienciación, y formación en confianza digital que se venían desarrollando hasta el 2012, incorporando la iniciativa pública y privada que manifieste interés en participar. Además organizará el mes de ciberseguridad en el marco de la Estrategia Europea de Ciberseguridad y colaborará con otras iniciativas europeas y nacionales en la materia. *Fases* • Fase I (2013): Primer mes de ciberseguridad • Fase II (2014-2015): Actuaciones de sensibilización y mes de ciberseguridad	1,6 M€
2	**Plataforma de Colaboración Público-Privada para incrementar la confianza digital** Constitución de una plataforma de colaboración público-privada que lidere las actuaciones nacionales de sensibilización, concienciación y formación con el objetivo de racionalizar recursos para obtener mejores resultados y un mayor impacto en la ciudadanía y las empresas. El Plan de sensibilización de INTECO se integraría dentro de las acciones de la plataforma una vez constituida. *Fases* • Fase I (2014): Constitución de la plataforma • Fase II (2014-2015): Desarrollo de actividades	0,6 M€
3	**Piloto en itinerarios educativos escolares** Puesta en marcha de un piloto que permita evaluar la oportunidad y viabilidad de la incorporación de contenidos de confianza digital en itinerarios educativos escolares. *Fases* • Fase I (2013): Constitución del grupo de trabajo • Fase II (2014): Informe del grupo de trabajo sobre itinerarios educativos • Fase III (2015): Desarrollo piloto	0,6 M€
4	**Plan de Menores en Internet** Entre otras actuaciones, el Plan de Menores en Internet reforzará el portal de chaval.es de RED.ES (www.chaval.es), se estudiará la viabilidad de la implementación de un mecanismo que permita el etiquetado de contenidos digitales en la red para menores y se impulsará un grupo de trabajo específico para la protección del menor donde estén representados, entre otros, el Ministerio del Interior (Guardia Civil, Policía), Fiscalía de Menores, el Ministerio de Educación, Cultura y Deporte, y el Ministerio Sanidad, Servicios Sociales e Igualdad, junto a las CCAA.	1,0 M€

	Fases • Fase I (2013): Constitución del GT de Menores e Internet • Fase II (2014): Plataforma de seguridad de los menores en Internet • Fase III (2014-2015): Proyectos tecnológicos de innovación para la seguridad de los menores • Fase IV (anuales): Acciones de sensibilización y formación (guías pedagógicas) en Internet • Fase V (anuales): Estudios uso Internet por menores	
5	**Punto neutro de gestión de incidentes** Puesta en marcha de un centro técnico y de atención al usuario para dar soporte al código de conducta de gestión de incidentes de seguridad previsto en la modificación de la Ley de Servicios de la Sociedad de la Información (LSSI). Entre otros incidentes atenderá de forma prioritaria la lucha contra los "botnet". *Fases* • Fase I (2014): Puesta en marcha del centro	2,0 M€
Eje II: Oportunidad para la industria TIC		**4,1 M€**
6	**Comité Técnico de Coordinación** Constitución de un Comité Técnico de Coordinación entre los distintos agentes competentes para el diseño de un programa integral que cubra el ciclo de vida del emprendimiento y de la I+D+i para el bienio 2014-2015 en materia de ciberseguridad y servicios de confianza, aprovechando los instrumentos de financiación y estímulo ya operativos de la AGE y, en su caso, los de nueva creación que pudieran establecerse. Esta medida se coordinará con el Plan de impulso de la economía digital y de los contenidos digitales y el Plan de desarrollo e innovación del sector TIC. *Fases* • Fase I (2014): Incorporación de líneas y prioridades temáticas en los principales instrumentos de financiación de la AGE y refuerzo de la financiación	-
7	**Soporte especializado a las estructuras de evaluación de proyectos** Incluir a los expertos de INTECO y otros agentes especializados en los Comités de Evaluación de proyectos de los instrumentos de financiación de la AGE. *Fases* • Fase I (2013): Incorporación de INTECO en los procesos de evaluación de los instrumentos de financiación públicos	0,2 M€
8	**Refuerzo de la capacidad de detección de demanda temprana** Incorporación de INTECO a las estructuras público-privadas de detección de demanda temprana de productos y servicios de ciberseguridad y confianza digital. *Fases* • Fase I (2014): Incorporación de INTECO en las estructuras público-privadas de	0,9 M€

	detección de demanda temprana	
9	**Polo tecnológico de ciberseguridad** Estudio de viabilidad para la creación de un Polo Tecnológico de Ciberseguridad en el que participen INTECO y Red.es, empleando las estructuras evaluadas en el Plan de Impulso de la Economía Digital y de los Contenidos Digitales y las oportunidades de cofinanciación de los Fondos Europeos (FEDER). *Fases* • Fase I (2014): Realización estudio de viabilidad	2,5 M€
10	**Foro Nacional para la Confianza Digital** Creación de un Foro Nacional para la Confianza Digital con la participación de todos los agentes más relevantes del sector privado, industria, profesionales, I+D y consumidores junto con el sector público, que actúe como organismo asesor en materia de regulación y estrategia para la ciberseguridad y la confianza. *Fases* • Fase I (2013): Constitución del Foro • Fase II (2013): Aprobación del Plan • Fase III (2014): Inicio de actividades	0,5 M€
Eje III: Nuevo contexto regulatorio		**0,6 M€**
11	**Adopción de la nueva regulación europea** La nueva regulación europea prevista para el periodo 2014-2015 exigirá poner en marcha nuevos instrumentos normativos. Algunos de los instrumentos regulatorios previstos son: la Directiva de Seguridad de las Redes y de la Información, el Reglamento de Identidad Electrónica y Servicios de Confianza y el Reglamento de Protección de Datos Personales. *Fases* • Fase I (2014-2015): Adopción de la nueva regulación europea	-
12	**Esquema de gestión de incidentes de seguridad** La propuesta de modificación de la Ley de Servicios de la Sociedad de la Información (LSSI), que se incorporará en una disposición adicional, tiene por objetivo establecer mecanismos de colaboración entre INTECO y los prestadores de servicios de la Sociedad de la Información, los registros de nombre de dominio y los agentes registradores que estén establecidos en España con el fin mejorar las capacidades de alerta temprana y prevención y de mitigar los incidentes de seguridad que afecten a la red. Esta disposición adicional prevé además el desarrollo de un esquema de conducta en un programa de cooperación público-privada. *Fases* • Fase I (2014): Tramitación de la Disposición Adicional de la LSSI • Fase II (2014-2015): Adopción del código de conducta	-
13	**Esquema de indicadores para la confianza digital** Desarrollo de un nuevo esquema de indicadores para medir los niveles de	0,6 M€

	confianza digital, prestando especial atención a disponer de métricas para medir fiablemente el nivel de confianza de la ciudadanía y las empresas, así como el mercado potencial para la Industria y las inversiones realizadas por las empresas demandantes. *Fases* • Fase I (2013): Diseño y elaboración del plan de indicadores • Fase II (2014): Obtención de la primera serie	
Eje IV: Capacidades para la resiliencia: INTECO 2.0		**42,3 M€**
14	**Transformación organizativa y refuerzo** Reorientación de la actividad de INTECO, acompañado de un importante refuerzo presupuestario y de plantilla, que le permita desarrollar eficazmente su misión en el mercado interior digital, la industria, las empresas, el mundo académico y la ciudadanía, y con carácter prioritario las empresas de especial trascendencia económica. *Fases* • Fase I (2013): Plan de actividad de INTECO 2.0 • Fase II (2013-2015): Refuerzo y dotación de personal técnico especializado	36,0 M€
15	**Nueva plataforma tecnológica de alerta temprana y servicios de vigilancia tecnológica** Despliegue y operación de nuevos servicios de inteligencia en ciberseguridad, estableciendo acuerdos con las entidades de referencia internacional y desarrollando labores de investigación e innovación que constituyan un núcleo de conocimiento y servicio en permanente evolución, para la detección proactiva de amenazas, la alerta temprana y el apoyo en la toma de decisiones estratégicas relativas a ciberseguridad nacional. *Fases* • Fase I (2013): Nueva plataforma de detección de alerta temprana • Fase II (2014): Modelo de detección y alerta temprano operativo • Fase III (2013-2014): Convenios con entidades de referencia internacional	3,5 M€
16	**Nuevos canales de comunicación para la confianza digital** Mejora de los canales de comunicación con los usuarios mediante una nueva web y sistema de blogs especializados que permitan ofrecer coherencia y homogeneidad a todas sus actuaciones, elaborando mensajes más adaptados a los diferentes públicos objetivos, y logrando con ello un mayor impacto, información de detección y alerta temprana más eficiente, publicación y difusión de conocimiento de relevancia técnica e informes periódicos de situación. *Fases* • Fase I (2013): Puesta en marcha de la nueva web • Fase II (2014): Lanzamiento de blogs especializados	0,9 M€
17	**Cooperación con la seguridad pública y la protección de las infraestructuras críticas** La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la	1,5 M€

	Información y la Secretaría de Estado de Seguridad establecerán un convenio de colaboración para que INTECO-CERT ofrezca su capacidad en ciberseguridad al Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) y a las Fuerzas y Cuerpos de Seguridad del Estado. Por medio de este convenio, INTECO se encargará de poner en marcha un CERT de Infraestructuras Críticas de la Información para el CNPIC y colaborará en las actuaciones de las FCSE. *Fases* • Fase I (2013): Puesta en marcha del CERT de Infraestructuras Críticas	
18	**Colaboración en ciberejercicios** INTECO colaborará con el Departamento de Seguridad Nacional (DSN) en el desarrollo de ciberejercicios nacionales e internacionales y en los que se organicen por el sector industrial y empresarial. *Fases* • Fase I (2013-2015): Participación en los ciberejercicios de ciberseguridad con la industria y empresas de los sectores estratégicos.	0,4 M€
Eje V: Programa de excelencia en ciberseguridad		**6,2 M€**
19	**Equipo de investigación avanzada** Puesta en marcha de un equipo de investigadores expertos que crearán nuevas líneas de investigación relacionadas con la ciberseguridad y desarrollo de proyectos formativos en colaboración. *Fases* • Fase I (2013): Constitución del grupo de trabajo y contratación del equipo de investigación. • Fase II (2014): Desarrollo de actividades y evaluación de resultados.	2,0 M€
20	**Jornadas "Espacio de Ciberseguridad"** Creación de un programa anual de fomento y sensibilización en ciberseguridad para alumnos de institutos y centros de enseñanzas medias. *Fases* • Fase I (2013): Impartición primera jornadas.	0,2 M€
21	**Formación especializada en ciberseguridad** Realización de cursos a distancia para formar a personas que posean interés y conocimientos en seguridad de la información con el objeto de alcanzar elevados niveles de perfeccionamiento y estímulo como profesionales de alta cualificación en el ámbito de la ciberseguridad. Para el desarrollo de estos cursos se evaluará la posibilidad de utilizar plataformas masivas al estilo de los MOOC -Massive Open Online Courses. *Fases* • Fase I (2014): Realización de un piloto de Sistemas Industriales • Fase II (2015): Realización de cursos especializados en ciberseguridad	0,6 M€
22	**Máster Ciberseguridad INTECO**	0,8 M€

	Título universitario propio para estimular la formación de profesionales de alta cualificación. *Fases* • Fase I (2013): Impartición primer master Ciberseguridad	
23	**Programa de becas de INTECO** Programa anual de becas de investigación que permita fortalecer las investigaciones en materia de ciberseguridad. El éxito de esta acción repercutirá en la generación de nuevos expertos que podrán dotar de un conocimiento más especializado al sector público y privado y al mundo académico. *Fases* • Fase I (2014): Asignación becas	0,6 M€
24	**Evento de ciberseguridad** Explorar la viabilidad y oportunidad de organizar un evento de ciberseguridad de gran envergadura en el que participarían los alumnos más destacados de los programas formativos de ciberseguridad en España y los mejores talentos internacionales, para promover la inmersión en tareas y retos avanzados de ciberseguridad diseñados por INTECO y los grupos de investigación colaboradores. Este evento permitirá que la industria pueda participar activamente, tanto en la organización de los eventos, como otorgándoles la posibilidad de presentar casos de éxito. *Fases* • Fase I (2013): Estudio de viabilidad • Fase II (2014): Realización del evento, en su caso	1,0 M€
25	**Estudio de viabilidad de una red de centros de excelencia en ciberseguridad** Evaluación de la oportunidad y viabilidad de crear una red de centros de expertos en ciberseguridad en España. *Fases* • Fase I (2014): Estudio de viabilidad	1,0 M€