Incentivando la Adopción de la Ciberseguridad

Una iniciativa de:

Copyright y derechos:

Incentivando la Adopción de la Ciberseguridad

Autores:

Gianluca D'Antonio
Adolfo Hernández
Enrique Fojón Chamorro
Manel Medina

Madrid, Noviembre de 2014

Gianluca D'Antonio es CISO del GRUPO FCC. Cofundador y Presidente de la Asociación Española para el Fomento de la Seguridad de la información ISMS Forum Spain. Miembro desde 2009 del Grupo Permanente de Expertos PSG de la Agencia Europea de Seguridad de las Redes y de la Información ENISA. Miembro del Comité de Certificación Internacional del Cloud Security Alliance. Sus competencias profesionales están acreditadas por las siguientes certificaciones: CISM, CISA, CGEIT, L.A. ISO27001, CCSK, CBCI y CDPP.

Adolfo Hernández, es Ingeniero Informático por la Universidad Autonóma de Madrid. Compagina su labor profesional como gerente del área de Governance, Risk & Compliance en Ecix Group, con la colaboración como subdirección de THIBER, the Cyber Security Think tank, siendo también miembro del Spanish Cyber Security Institute y miembro de la junta del capítulo español del (ISC)2.

Enrique Fojón Chamorro es Ingeniero Superior en Informática. Es sub-director de THIBER, the Cyber Security Think tank. y miembro del Spanish Cyber Security Institute.

Manel Medina es catedrático de seguridad informática de la Univ. Polit. de Catalunya (UPC), fundador y director del esCERT (esCERT-inLab-UPC).

Presidente del comité científico del capítulo europeo del AntiPhishing Working Group (APWG.EU). Sub-director del depto. Técnico de ENISA (Agencia de seguridad de la información y las redes de la Unión Europea). Asesor en ciberseguridad de diversas organizaciones.

Contenido

La Sociedad de la Información, como la conocemos hoy en día, presenta una gran dependencia del denominado ´ecosistema digital´

1. Introducción

1.Introducción

Durante la última década, Internet ha pasado de ser una útil herramienta de comunicación para individuos y organizaciones a convertirse en una infraestructura digital esencial para el desarrollo económico y el bienestar de la sociedad en su conjunto. Esta afirmación, incluida en un reciente estudio de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), sobre ciberseguridad[1], pone de manifiesto la imparable transformación de un mundo cada vez más dependiente de las Tecnologías de la Información y las Comunicaciones. Precisamente, esta dependencia constituye un factor de riesgo que no podemos ni debemos obviar, tal y como refleja desde 2011 el Foro Económico Mundial que ha introducido en su Mapa de Riesgos Globales[2] un elenco de incidentes potenciales relacionados con el ciberespacio y el uso de las Tecnologías de la Información y las Comunicaciones.

La Sociedad de la Información, como la conocemos hoy en día, presenta una gran dependencia del denominado ´ecosistema digital´, cuyo acceso y uso se alza como un interés legítimo de la ciudadanía, sin llegar todavía a reconocerle este estatus de pleno derecho. Si nuestra sociedad no puede entenderse sin la disponibilidad y el uso de estas "infraestructuras digitales", la evolución natural de esta situación es hacia el desarrollo de un marco normativo y organizativo de promoción, protección y tutela.

Con este estudio, el **Spanish Cyber Security Institute** (en adelante **SCSI**) y **THIBER**, the Cyber Security Think Tank (en adelante **THIBER**) pretenden propiciar un debate sobre las medidas de carácter legal y organizativo que posibiliten generar un ecosistema digital seguro y resiliente.

1.1 La ciberseguridad, una responsabilidad compartida

Incentivar las acciones y actitudes que permitan mejorar el nivel de resiliencia del tejido empresarial español, cambiar la praxis empresarial en materia de ciberseguridad y aumentar el nivel de concienciación general, constituyen los pilares de la aproximación más eficaz para alcanzar los fines propuestos en el presente documento: el desarrollo de una sociedad capaz de proteger sus intereses, a sus ciudadanos y a sus empresas frente a las amenazas que el uso de las nuevas tecnologías implican.

1. La ciberseguridad, una responsabilidad compartida2. Global Risk 2014. Ninth Edition. World Economic Forum. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf
2. Global Risk 2014.NinthEdition. WorldEconomic Forum. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

Los puntos clave sobre los que se sustenta la aproximación planteada en el presente documento son:

1. Distribución de los costes de la ciberseguridad entre todos los actores involucrados, es decir, ciudadanía, empresas y las propias administraciones públicas.
2. Premiar a las organizaciones comprometidas con la protección de los sistemas de información.
3. Desarrollar el mercado de productos y servicios de ciberseguridad a través del impulso de la oferta.
4. Estimular la demanda de herramientas de seguridad informática por parte de usuarios y organizaciones.
5. Fomentar la investigación y el desarrollo en soluciones y productos de ciberseguridad.
6. Estimular la resiliencia de todo el ecosistema que compone el ciberespacio.

En definitiva, este enfoque impulsa y fomenta la cultura de la seguridad y de la defensa del ciberespacio como una responsabilidad común y compartida entre todos los estamentos de la sociedad.

1.2 Cambio de paradigma

La tradición de la Europa Continental nos ha acostumbrado a un paradigma sancionador y punitivo como método para conseguir los objetivos prefijados. Sin embargo, estas sanciones deberían modularse en función de la capacidad preventiva de la organización afectada, dando soporte a éstas frente a ataques inevitables y castigando solo a aquellas que no hayan actuado con la diligencia debida y sean vulnerables a ciberataques triviales o fácilmente evitables.

Durante la última década, en el ámbito del ciberespacio se ha producido una proliferación de regulaciones comunitarias y nacionales centradas en la parte impositiva y sancionadora más que en la vertiente propositiva y de estímulo.

Las diferencias entre los dos paradigmas no son solo filosóficas, sino determinantes para la eficaz consecución de los objetivos establecidos. Por tanto, es necesario generar las condiciones favorables para que las organizaciones consideren la seguridad y la protección del ciberespacio como un valor y una inversión en lugar de como un coste.

En este sentido, el presente documento propone un programa de incentivos que tiene como objetivo favorecer la adopción de buenas prácticas en ciberseguridad.

1.3 ¿Por qué son necesarias las ayudas?

En el contexto macro y micro económico actual, donde se atisban los primeros síntomas de recuperación en los consumos y en la producción industrial nacional, una política de incentivos permitiría apoyar la iniciativa privada en la misión de proteger a clientes, usuarios y activos de información. La española es una economía basada principalmente en el sector servicios, energía e industria. Estos sectores, que constituyen casi el 90% del Producto Interior Bruto (PIB) nacional[3], presentan una característica común: una fuerte dependencia de las Tecnologías de la Información y las Comunicaciones. Y es precisamente esta dependencia de los nuevos canales telemáticos la que precisa ser tratada como un factor de inversión, bajo la perspectiva de mejorar la experiencia de los consumidores y la confianza de los usuarios en la seguridad de los sistemas que utilizan para contratar servicios y comprar productos.

Según una reciente encuesta realizada por una consultora en varios países desarrollados, la mitad de las empresas españolas encuestadas fue víctima de un ciberdelito en los últimos dos años[4].

Este dato pone de manifiesto la necesidad de un cambio en las políticas públicas sin el cual seguiremos incrementando el déficit de medios y profesionales necesarios para garantizar la seguridad de los sectores anteriormente mencionados.

"la mitad de las empresas españolas encuestadas fue víctima de un ciberdelito en los últimos dos años"

3. http://economy.blogs.ie.edu/archives/2014/02/estructura-de-la-economia-espanola-por-sectores-economicos-y-el-empleo-1970-2013.php
4. http://www.delitosinformaticos.com/06/2014/delitos/fraudes-y-estafas/la-mitad-de-las-empresas-espanolas-sufrieron-ciberdelitos-en-los-ultimos-dos-anos

1.4 El caso español: le necesidad de definir un marco general de ciberseguridad

El 5 de diciembre de 2013, el Consejo de Ministros a instancia del Consejo de Seguridad Nacional, aprobó la Estrategia de Ciberseguridad Nacional (ECN)[5]. Dicho texto, cuya génesis se remonta dos años atrás en el tiempo, desarrolla el punto correspondiente de la Estrategia de Seguridad Nacional presentada en mayo de 2013, que contemplaba la ciberseguridad dentro de sus doce ámbitos de actuación, reflejando futuras situaciones y análisis de situación a partes iguales.

Aprobada en un entorno presupuestario altamente restrictivo, la implementación práctica de las líneas de acción identificadas, cuya consecución y buen término contemplará ciertamente una inversión financiada por el erario público y las empresas, debería pasar por una política de impulso y apoyo a aquellas organizaciones comprometidas con la protección de los sistemas de información e infraestructuras tecnológicas.

Se seguirá, por ende, aprovechando cada oportunidad, como la presente, para reclamar un marco legislativo y reglamentario en esta materia.

5 . Estrategia Nacional de Ciberseguridad Nacional.
http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

2. Principales lineas de acción

2.1 Incentivos legales

2.2 Acceso a financiación

2.3 Incentivos de mercado

2.4 Seguros

2.5 Reconocimiento público

2.6 Facilidad en la contratación con la Administración Pública

2.7 Priorización en la asistencia técnica por parte del Estado

2.1 Incentivos legales

En el prólogo de la Estrategia de Ciberseguridad Nacional, el Presidente del Gobierno se refería a la extrema necesidad de "dedicar todos los medios necesarios" al servicio de la ciberseguridad. La dependencia de nuestra sociedad del bienestar de las nuevas tecnologías requiere un compromiso decidido con "la seguridad del ciberespacio".

Esta aceptación de responsabilidad y liderazgo por parte de las más altas instituciones del Estado, representa un punto de partida determinante para que la ciudadanía, en su conjunto, asuma el coste de este proceso de capacitación. Y es que, tal y como afirma el documento, "...la competitividad de nuestra economía y la prosperidad de España dependen de la inversión que se realice en términos de gestión del talento y recursos para desarrollar las capacidades necesarias para afrontar estos desafíos."

Países como el Reino Unido, India o Estados Unidos han puesto en marcha programas de incentivos fiscales o de financiación privilegiada para dinamizar este mercado y, al mismo tiempo, apoyar a las empresas que apuestan por proteger eficazmente sus sistemas y activos de información. En el caso del Estado de Maryland, en Estados Unidos, estos incentivos fiscales pueden llegar hasta los 250.000 dólares por empresa y año fiscal. Las ayudas están destinadas a las empresas de productos y servicios de ciberseguridad que establezcan sus oficinas en el Estado[6].

En el caso de la India, el marco de incentivos desplegados, en declaraciones de su ministro de comunicaciones, están destinados a aquellas empresas que inviertan en medidas de protección tecnológica[7].

En el plano europeo, en el Reino Unido se ha puesto en marcha un programa de incentivos a la innovación denominado innovation voucher para apoyar a las pequeñas empresas que quieran lanzar nuevos productos y servicios tecnológicos.

En la misma línea, el gobierno irlandés ha impulsado una campaña de apoyo al registro de propiedad intelectual en el ámbito de las nuevas tecnologías con el fin de favorecer el aumento de la riqueza científica y de mercado nacional a través de las patentes[8].

6. http://business.maryland.gov/fund/programs-for-businesses/cyber-tax-credit. http://www.choosemontgomerymd.com/programs-incentives/financial-tax-incentives/local-cybersecurity-investment-incentive-tax-credit-supplement#.VDbA2bF1yn8
7. http://khabarsouthasia.com/en_GB/articles/apwi/articles/features/2013/07/19/feature-01
8. http://www.enterprise-ireland.com/en/Research-Innovation/Companies/Source-licence-new-technologies/

Estas iniciativas demuestran un creciente interés por parte de muchas economías de impulsar la ciberseguridad como un vector de crecimiento económico a través de las siguientes líneas directrices:

1. Desarrollo de un tejido empresarial de proveedores de productos y servicios relacionados con la ciberseguridad.
2. Incremento de las patentes registradas para productos de ciberseguridad.
3. Mejora del nivel de ciberprotección del sector privado.
4. Capacitación de una fuerza de trabajo altamente especializada en ciberseguridad.
5. Aumento de la tasa de empleo con trabajadores altamente especializados.

Tras el análisis de diversas iniciativas internacionales, se resumen los tres bloques principales en los que se agrupan las principales políticas incentivadoras fiscales y legales:

1. Ayudas fiscales en la reducción de tasas. La eficacia de los incentivos fiscales en la promoción de la ciberseguridad dependerá de la capacidad del gobierno para definir las actividades incluidas en esta ayuda de una manera que realmente incentiven los gastos operativos (OPEX) y las inversiones (CAPEX) ya sean en servicios y tecnologías. La definición de "gastos admisibles" o deducibles dentro de este contexto sería determinante. Sin embargo, la disponibilidad de estas líneas de crédito fiscal puede requerir la participación de diversos agentes públicos y el desarrollo de reglamentación así como un posible esquema de certificación de proyectos, servicios y tecnologías deducibles.

Por otra parte, la comercialización en el mercado interior de productos y servicios de ciberseguridad constituirá una actividad comercial que generará unos beneficios en los proveedores, y la recaudación de impuestos por IVA de los productos adquiridos.

Sin embargo, si las empresas no aplican mecanismos de ciberseguridad, las pérdidas potenciales asociadas a los incidentes de cibernéticos pueden producir unas pérdidas económicas que repercutirán en el PIB y en los balances de las empresas, reduciéndose de forma proporcional la recaudación impositiva del Gobierno.

2. Reducción de los costes y tasas administrativas en el registro de patentes nacionales relativas a la ciberprotección, así como una mejora de la protección de patentes tecnológicas.

3. Reglamento y legislación de ciber-seguridad. A pesar de la existencia de muchas normas y estándares que promulgan la adopción de determinados controles de seguridad, se observa una aplicación desigual, poco homogénea e inconsistente. Este hecho genera incertidumbre regulatoria que puede conducir a las empresas a mayores niveles de riesgo financiero, legal y en su reputación. La adhesión de las empresas a programas voluntarios de ciberseguridad o la aplicación total o parcial de sus controles podría proporcionar una mayor seguridad jurídica, actuando como atenuante o incluso eximente en la delimitación de responsabilidades ante un ciberataque[9], sobre todo cuando éstos no estén sujetos a legislación o reglamentos administrativos específicos.

2.2 Acceso a financiación

Para alimentar este ecosistema industrial y convertirlo en una incubadora de iniciativas empresariales capaz de aprovechar las oportunidades de este incipiente mercado es indispensable resolver el acuciante problema del acceso a la financiación.

Comparativamente, las empresas norteamericanas y las asiáticas gozan generalmente de una mejor financiación. Como pone de manifiesto un reciente estudio de A.T.Kearney[10], países como China, Corea del Sur o Japón financian directamente a sus empresas tecnológicas mediante incentivos financieros y fiscales o indirectamente a través de medidas proteccionistas del mercado que facilitan la contratación de los servicios y productos ofrecidos por ellas.

En el caso estadounidense, la presencia de un fuerte mercado de fondos de inversión tipo venture capital ofrece fácil acceso a financiación para las nuevas empresas mientras que en Europa es el sector bancario, fuertemente regulado y con una mayor resistencia a la aceptación de riesgos, es el actor económico principal para obtener apoyo financiero. Sin olvidarnos que, en determinados sectores, como el de defensa, Estados Unidos aplica políticas protectoras que de forma directa apoyan a las empresas nacionales.

Tradicionalmente, los gobiernos europeos han favorecido más la financiación de la investigación científico-teórica más que el desarrollo de productos y mercados. Este factor, que podríamos referenciar como de índole cultural, se suma a una de por sí escasa inversión en I+D+i.

9. http://www.ismsforum.es/ficheros/descargas/la-responsabilidad-legal-de-las-empresas-fente.pdf
10. Thefuture of Europe's Hi-techIndustry, ATKearney , 2013.

Esta óptica basada en el fomento de la cultura de la ciberprotección puede servir como oportunidad para las organizaciones. Por un lado, mediante la adopción de buenas prácticas y medidas de control; y por el otro, impulsando la oferta en el mercado, apoyando la creación de polos industriales orientados al suministro de bienes y servicios que satisfagan la demanda de ciberseguridad.

En el caso español, el Gobierno podría seguir el ejemplo de su homólogo alemán, que recientemente ha constituido un fondo de capital riesgo especializado en tecnologías de la información denominado Hi-Tech Gründerfond, con una dotación presupuestaria que ronda los 400 millones de euros. Del mismo modo, también debería ser tenida en cuenta la implantación de beneficios fiscales para el despliegue de fondos de capital riesgos que invirtieran en proyectos y empresas españolas de ciberseguridad.

"La ciberseguridad se ha colado en las agendas políticas de la gran mayoría de las naciones avanzadas"

La ciberseguridad se ha colado en las agendas políticas de la gran mayoría de las naciones avanzadas, siendo una prioridad en las estrategias nacionales de seguridad y defensa. Sin embargo, la dependencia de proveedores extranjeros para el abastecimiento de los diferentes recursos que componen el sistema de ciberseguridad nacional constituye una debilidad que es necesario mitigar. Las iniciativas que se están llevando a cabo en otros países de nuestro entorno geopolítico ponen de manifiesto la urgencia de afrontar un plan integral, a nivel nacional y europeo, de impulso y apoyo a las iniciativas privadas que inviertan de manera profesional y a largo plazo en el desarrollo de productos y servicios de ciberseguridad.

Para que este objetivo sea realista, es necesario habilitar líneas de crédito empresarial y acceso a fondos de inversión públicos y privados. Los planes quinquenales y decenales desarrollados por el gobierno chino han demostrado ser una herramienta eficaz para conseguir resultados en este ámbito. Las políticas de corto plazo no son capaces de asegurar el suficiente nivel de financiación e inversión en un ámbito que requiere altos niveles de capacitación bajo el perfil de los recursos humanos y largos tiempos de investigación y desarrollo.

Las iniciativas propuestas en las líneas anteriores tienen como condición prioritaria una coordinación por parte del gobierno central y a nivel autonómico y municipal para garantizar la unidad de las actuaciones y fijar los objetivos sin la cual el ecosistema no puede prosperar.

2.3 Incentivos de mercado

Con el objetivo de favorecer la creación de un mercado maduro en servicios y soluciones relativos a la seguridad y defensa del ciberespacio, se propone la creación de polos industriales que englobe la cadena de suministro de ciberseguridad en su totalidad, desde los fabricantes de soluciones o tecnologías a proveedores de servicios especializados.

Para ello, con el objetivo de atraer inversión tanto nacional como extranjera en este sector, el Estado puede incentivar fiscalmente a través de créditos desgravables en el impuesto sobre la renta o sociedades tanto a los inversores privados o corporativos como a las propias empresas receptoras cuyo criterio de elegibilidad se adecue a unas pautas formales, como:

a. Que la empresa receptora esté radicada en territorio nacional.

b. Que esté organizada con ánimo de lucro y que su objeto social sea mayoritariamente la creación de tecnologías y servicios de ciberprotección.

c. Que se mantenga activa durante un mínimo de 5 años y que tenga un número mínimo de empleados.

d. Qué esté al corriente de sus obligaciones tributarias y que no tenga relación contractual con el Estado en el momento de la recepción de la ayuda.

Asimismo, estas empresas, una vez hayan formalizado este incentivo, podrían ser candidatas de programas de ayuda a la internacionalización a través de misiones comerciales patrocinadas por las oficinas de comercio exterior o cámaras de comercio, para apoyar proyectos que permitan avanzar en la comercialización internacional de tecnología de la seguridad.

Del mismo modo, estos dos incentivos deberían ser respaldados a través de programas de acceso a líneas de crédito como facilidad financiera en las etapas iniciales del mercado de ciberseguridad, como ya se menciona en el epígrafe anterior. Incluso se podría optar, como en el caso israelí o norteamericano, a destinar partidas presupuestarias para la creación de un Fondo Nacional de Inversión en Ciberseguridad, actuando como un fondo de capital semilla gubernamental, vehiculizando la creación de start-ups e innovación tecnológica, permitiendo la creación de viveros empresariales especializados.

2.4 Pólizas de ciber riesgo

Hasta el momento, la gran mayoría de las estrategias de reducción de riesgos cibernéticos empresariales pivotan sobre el concepto de reducción de la probabilidad de ocurrencia de una ciberamenaza, tratando así de reducir su superficie de exposición a la misma. En menor medida, se incide en la reducción del riesgo mediante medidas de minimización del impacto del ataque en la organización y sus servicios críticos.

Es en este escenario en el que aparecen los productos aseguradores ante ciberincidentes, como elementos clave para la transferencia del riesgo, mediante los cuales las organizaciones obtienen una póliza para cubrir el riesgo ante amenazas pre-identificadas de forma que el impacto derivado se traslada a la aseguradora a cambio de una prima.

Las ciberpólizas, como también son conocidas, presentan unas coberturas heterogéneas, en las que principalmente se protege ante daños propios (gastos de recuperación de datos, de restauración de imagen pública, de desinfección, de defensa jurídica, de expertos independientes, costes operativos y lucro cesante, etc.) y daños ante terceros (delitos contra el honor, propiedad intelectual de terceros, fallo en el deber de confidencialidad, incumplimientos contractuales, etc.).

Estos productos suponen una línea emergente para promover la adopción de medidas de ciberprotección más robustas, a través de la reducción de la prima como "premio" a su adopción, al estilo de lo que sucede con los seguros de automóviles. Las aseguradoras suelen preocuparse por la percepción de sus asegurados, ya que éstos tienden a relajar la implantación de controles, sabiendo que el riesgo de pérdida se ha transferido a un tercero.

En consecuencia, las aseguradoras pueden jugar un papel clave para mejorar la madurez de ciberseguridad del mercado, ya que:

1. Pueden requerir a sus clientes el cumplimiento de unas cautelas mínimas de ciberseguridad como una condición sine qua non para la aplicación de las coberturas, incluyendo entre éstas, por ejemplo, la adopción de un marco de buenas prácticas.
2. Pueden ofrecer descuentos en las primas a aquellas entidades que demuestren un nivel adecuado de madurez en seguridad de forma que reduzcan los riesgos de pérdidas a transferir a la aseguradora.

3. Las aseguradoras pueden poner en práctica, asesorar o dar soporte a los procedimientos de gestión de ciberincidentes en nombre del asegurado de forma inmediatamente posterior al mismo, mejorando la respuesta coordinada al mismo.

4. Dado que las aseguradoras necesitan datos fiables para que sus departamentos de suscripción cuantifiquen de manera adecuada las coberturas, los riesgos y las políticas de precios, el crecimiento del mercado de los ciberseguros podría conducir a una mejor comprensión de los patrones de las amenazas y la mejora de intercambio de información entre el supervisor designado por el gobierno y las empresas aseguradas.

5. Las propias aseguradoras desplegarán mecanismos de monitorización del estado de ciber-riesgo de los mercados de sus clientes, jugando un papel importante en alerta temprana ante incidentes.

Si bien se recomienda que el mercado de los ciberseguros sea netamente privado, para incentivar la adopción de estos productos se pueden crear unas líneas de acción desde los organismos gubernamentales de forma que:

1. Se reduzca el coste de las primas mediante la asunción de parte de las coberturas de las aseguradoras privadas a través de programas de reaseguro público.

2. Cuando los riesgos sean considerados como “no asegurables” por el mercado asegurador privado, se puede considerar la opción de que sea el Estado el que asuma determinados riesgos para reemplazar o estabilizar el mercado privado, por ejemplo,a través de programas específicos de compensación. En el caso español se podría vehiculizar a través del Consorcio de Compensación de Seguros.

3. Reconocer la adopción de marcos de ciberseguridad con un nivel de madurez determinado como una muestra de control debido, siendo de esta forma su implantación un atenuante ante potenciales ataques y limitando por extensión las responsabilidades civiles e, incluso, penales de las organizaciones atacadas.

2.5 Reconocimiento público

A pesar de la existencia de una abundante normativa en la que se referencia la obligatoriedad para todas las empresas de notificar "hechos relevantes", estos principalmente recaen sobre las sociedades cotizadas. Además dichas normativas se focalizan en el principio de información completa o full disclosure[11] ante hechos relevantes, lo que favorece ciertas reticencias a la hora de cumplir con las mismas. Por este motivo, y dada la dificultad y la falta de recursos para auditar y detectar este tipo de incidentes, la notificación de los mismos se convierte en un compromiso de la corporación con la sociedad en general, y en especial con sus "partes interesadas": clientes, inversores y agentes de mercado.

Por virtud de este principio están obligadas a proporcionar públicamente "información fidedigna, completa, efectiva y actualizada que permita a los inversores formarse un juicio fundado sobre la situación de la empresa y que contribuya al buen funcionamiento y a la transparencia del mercado de valores".

Entendiendo que "cualquier información no conocida por el mercado que pueda influir de forma sensible en la cotización de los valores afectados es susceptible de constituir un hecho relevante"[12], cabría pensar que un incidente cibernético cuyo impacto interno y externo fuese considerable, debería ser considerado un hecho relevante y, por extensión, ser notificado públicamente.

Para ello, el gobierno debería incentivar a las compañías para la comunicación clara y diligente de los ciber-incidentes de especial relevancia para la sociedad, reconociendo de esta forma su responsabilidad social corporativa. Por ejemplo, se podría solicitar como criterio básico de contratación con la Administración Pública o para cotizar en bolsa, el demostrar a través de un procedimiento regulado y en la memoria anual corporativa, la transparencia de la compañía en la comunicación de ciber-incidentes.

"el gobierno debería incentivar a las compañías para la comunicación clara y diligente de los ciber-incidentes"

11. J.E. Cachón Blanco, Derecho del Mercado de Valores, Madrid, 1992, vol. II.
12. Reglamento de Régimen Interior. CNMV. https://www.cnmv.es/docportal/Legislacion/resoluciones/RRI_CNMV.pdf

Las administraciones y organizaciones sin ánimo de lucro pueden actuar como eje vertebrador de una base adecuada de ciber-madurez del tejido empresarial de una nación. Mediante la creación de certificaciones para empresas y profesionales y la constitución de una lista pública de reconocimiento de empresas certificadas, países como el Reino Unido[13] o Australia[14] han dado respuesta a la necesidad de regular un mercado creciente con unas garantías de profesionalidad y calidad. Estas listas centralizadas actuarían como punto de referencia público en el mercado aportando:

1. Un impacto comercial y de reputacion positivo entre las empresas y profesionales listados.
2. Un nivel demostrable de seguridad de los procesos y procedimientos y validación de competencias técnicas de las organizaciones certificadas.
3. Orientación, normas y oportunidades para compartir y mejorar los conocimientos.
4. Medio ágil de inserción en el mercado de competencias, servicios y tecnologías de ciberseguridad.

2.6 Facilidad en la contratación con la Administración Pública

Las Administraciones Públicas (AAPP) tienen una doble función, como proveedores de servicios críticos a la sociedad y como reguladores del mercado y de la economía. Esta doble responsabilidad les ofrece también la capacidad de fijar los requisitos mínimos que deben cumplir no solo sus servicios; sino también aquellos considerados críticos para la sociedad siguiendo el ejemplo de la Directiva Europea de Servicios de Confianza[15].

Esta regulación tiene una doble función:

1. Definir los límites por encima de los cuales deben situarse los planes de seguridad de las organizaciones.
2. Ayudar a los responsables de seguridad a conseguir los recursos necesarios para implantar los mecanismos mínimos de seguridad requeridos en la regulación.

13. Crest.http://www.crest-approved.org/
14. Crest Australia.http://www.crestaustralia.org/
15. http://ec.europa.eu/digital-agenda/en/trust-services

Un ejemplo puede ser la definición normalizada de los criterios para clasificar la información y homologar los sistemas necesarios para gestionarla de forma eficiente y satisfactoria por parte de las AAPP. Esto permitiría, por un lado a los proveedores, unificar los procedimientos de acreditación de productos, dándoles un alcance europeo en lo referente a los requisitos a cumplir. Por otro lado a las AAPP, les permitiría requerir acreditaciones internacionales para optar a la adopción de sistemas clasificados, reduciendo con ello los costes y plazos de validación de los mismos por parte de las mismas, tanto para los proveedores como para la propia administración.

La acreditación de capacidades de las organizaciones que optan a ofrecer servicios a las Administraciones Públicas ha sido siempre objeto de polémica, ya que no siempre son uniformes o están armonizados con los de otras administraciones europeas.

La definición de unos criterios de selección basados en normas y buenas prácticas reconocidas internacionalmente incentivaría su aplicación, ya que facilitaría la acreditación de capacidades para optar a la provisión de servicios a cualquier Administración Pública europea.

De hecho, éste es uno de los objetivos de la Comisión Europea para conseguir el mercado único y eliminar las barreras administrativas.

Estas capacidades se pueden referir tanto a la gestión de procesos de seguridad, como la preservación de datos personales, como a capacidades del personal implicado en los servicios ofertados. En este sentido la Comisión Europea solicitó a la Agencia Europea para la Seguridad de las Redes y la Información (ENISA) en la Estrategia Europea de Ciberseguridad de 2013, la redacción de una hoja de ruta para la implantación de servicios de formación normalizados y homologados en seguridad de redes y sistemas de información (Network and Information Security Driving License), extendiendo así la ya reconocida internacionalmente European Computer Driving License (ECDL).

2.7 Priorización en la asistencia técnica por parte del Estado

La asistencia técnica priorizada es una medida cuya implantación adecuada supondría un claro incentivo para aquellas compañías que, independientemente de su tamaño, adoptasen marcos de buenas prácticas de ciberseguridad reconocidos.

Este incentivo, si bien debe ser conceptuado como un servicio estatal básico, se propone como una prestación con un mayor nivel de servicio y celeridad para aquellas organizaciones que cumplan determinados requisitos. Sin embargo, debe ser interpretado como un complemento, no un sustitutivo, de otros mecanismos de autoprotección cibernética de las propias compañías. Asimismo, deberá funcionar en connivencia con otros mecanismos condicionantes necesarios como el intercambio de información en tiempo real con los órganos estatales.

Esta prestación de asesoramiento técnico adaptado a las circunstancias específicas de cada organización demandante, tanto durante un incidente como de forma periódica, podría realizarse desde los CERTs o CSIRTs nacionales actualmente operativos, así como desde los órganos sectoriales establecidos, si los hubiere, proporcionando una respuesta inmediata y flexible, aumentando la resiliencia ante las ciberamenazas.

Así pues, las actividades de asistencia podrían clasificarse del siguiente modo:

1. Durante un incidente.
    a. Soporte en tiempo real a su resolución.
    b. Coordinación con ISPs, CERTs, FCSE y otros agentes.
2. De forma periódica.
    a. Soporte a la implantación de los mecanismos de protección del marco seleccionado.
    b. Formación y concienciación.
    c. Generación de plantillas documentales de operación y reacción ante incidentes de seguridad.

En cualquier caso, se deberán tomar en consideración determinadas actuaciones a ejecutar por parte del gobierno para una adopción eficaz de este incentivo:

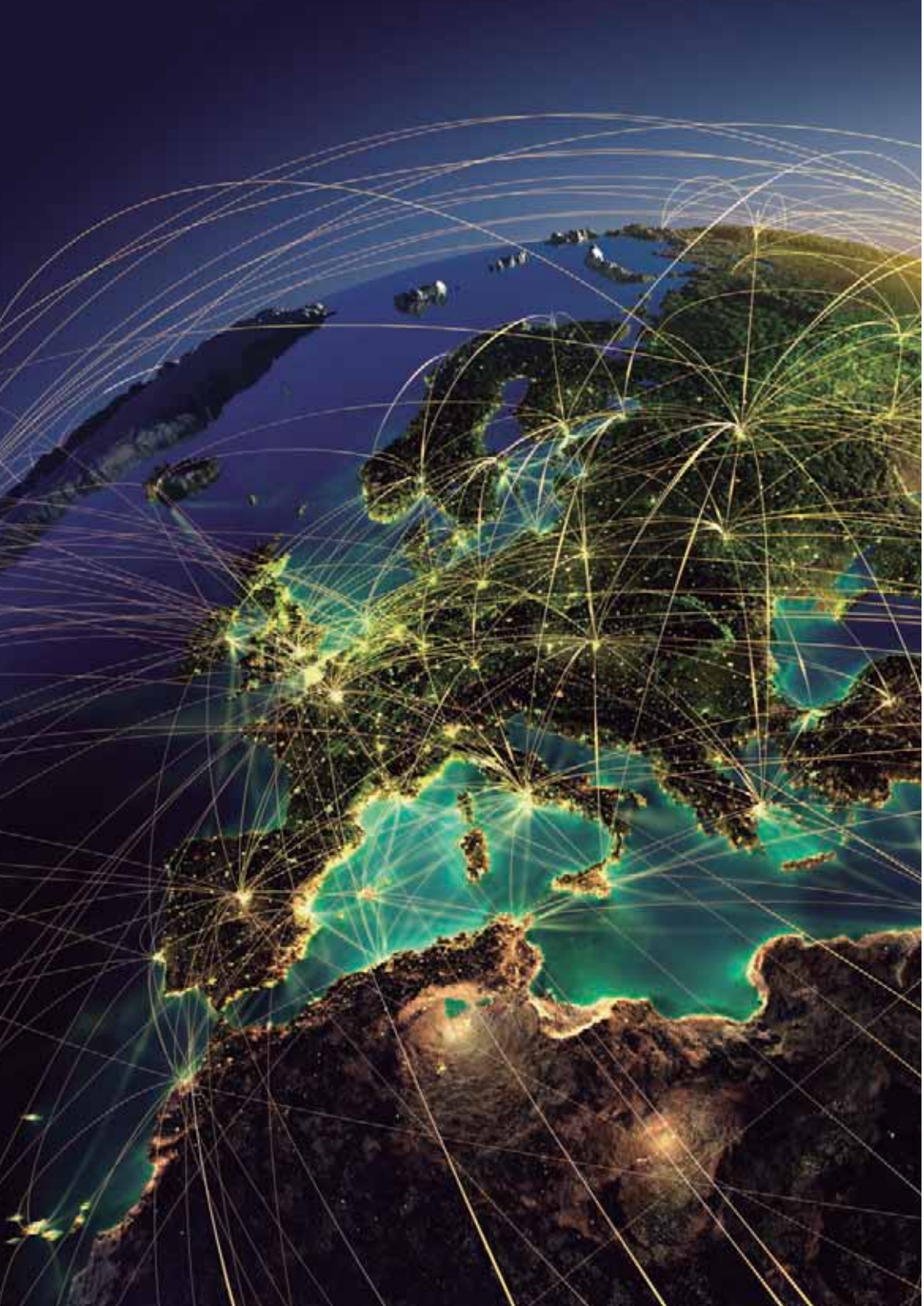
Escalabilidad y costes: el programa, al ser financiado por los órganos públicos centrales, puede presentar un problema de escalabilidad de personal y medidas técnicas para proveer un servicio individualizado conforme sean más las empresas adscritas a este incentivo.

Criterios de priorización: ante la potencial limitación de recursos públicos, se podría priorizar las empresas elegibles también sectorialmente (favoreciendo, por ejemplo, a los operadores de infraestructuras críticas).

Publicidad y competencia con el sector privado: es necesario acompañar el despliegue de este mecanismo con un mensaje de integración y proporcionalidad, ya que se puede percibir que podría beneficiar mayoritariamente a aquellas compañías con menor número de recursos a su disposición. Del mismo modo, se debe hacer hincapié en que estas medidas en ningún caso son sustitutivas de otros mecanismos, por lo que el mercado de la ciberseguridad privado no debe sentirse desplazado. De hecho, el soporte público debería ser proporcional a la inversión privada, de forma que quien no invierta adecuadamente en su propia seguridad, tampoco debería recibir soporte público.

Impacto reputacional: es necesario mitigar, mediante un deber de sigilo estricto, la posibilidad de que el uso por parte de las compañías de la asistencia técnica pueda resultar "estigmatizante" en el mercado si el hecho se hace de conocimiento público. Se debe incentivar a las organizaciones usuarias a solicitar la ayuda de las instituciones del gobierno, garantizando la confidencialidad mediante acuerdos de provisión de servicio, y un impacto mediático nulo o controlado positivamente en su entorno.

Supervisión de la elegibilidad. Esta medida no es un sustituto y, por lo tanto, la elegibilidad de las empresas receptoras debería estar supervisada. Existe cierto riesgo de irresponsabilidad por parte de las empresas, que pueden no actuar de forma diligente y no tomar, por extensión, las precauciones mínimas (control debido) para asegurar sus sistemas, confiando en que las instituciones gubernamentales responderán en última instancia ante un ataque cibernético.



3. Análisis de iniciativas en el ámbito internacional

3.1 Europa

3.2 Estados Unidos

3.3 Israel

3.1 Europa

La ciberseguridad constituye una de las prioridades en la Unión Europea desde la creación en 2004 de su agencia ENISA que tiene por objeto incentivar y asesorar a los gobiernos de los Estados Miembros en la implantación de legislación y regulación en materia de ciberseguridad, intentando que las condiciones e incentivos legales para la aplicación de medidas de seguridad sea uniforme entre los veintiocho.

Posteriormente se crearon otras instituciones europeas:

El Equipo de respuesta a incidentes de las Instituciones Europeas (EU-CERT) en 2012. Éste es el encargado de asesorar y dar soporte en la respuesta a ciberataques recibidos por las instituciones europeas, incentivando la aplicación de medidas preventivas en las mismas, y sirviendo de ejemplo a organizaciones similares a nivel nacional.

El Centro Europeo de Ciber-Crimen de EUROPOL (EC3) en 2013. Heredero de la división de ciber-crimen de EUROPOL, es el encargado de planificar y coordinar todas aquellas actuaciones policiales encaminadas a detectar y perseguir los delitos informáticos de ámbito supranacional, y desarrollar herramientas y metodologías para que las policías nacionales mejoren su calidad y capacidad de respuesta a ciber-crímenes.

El Parlamento y Consejo de la Unión Europea han desarrollado diversas directivas y planes regulatorios para su aplicación directa o indirecta (transposición) en los estados miembros:

a) El Plan Estratégico Europeo de Ciberseguridad , aprobado el 7 de Febrero [16] de 2013, fija cinco prioridades estratégicas:

1. Conseguir la ciber- resiliencia, creando mecanismos de coordinación e incentivando la publicación de datos de ciber-incidentes.
2. Reducir drásticamente el ciber-crimen.
3. Desarrollar una política y capacidades de ciber-defensa relacionadas con la Política Común de Seguridad y Defensa.
4. Desarrollar los recursos tecnológicos e industriales para la ciberseguridad.
5. Establecer una política europea coherente para el ciber-espacio internacional, y promover un núcleo de valores de la Unión Europea.

16. JOIN(2013) 1 final "Cybersecurity Strategy of the European Union: An Open, Safe and SecureCyberspace".

b) Directiva Europea de ciberseguridad[17], cuyo objetivo es uniformizar el nivel mínimo de seguridad informática y de la red en Europa, estableciendo un marco regulador común y mecanismos de cooperación a través de intercambio de información en una red de cooperación y mecanismos de notificación de incidentes, con el objetivo de mejorar la eficiencia en la gestión de los mismos.

Esta cooperación permitirá optimizar recursos, evitando duplicidades y por tanto reduciendo los costes de implantación de mecanismos de seguridad básicos, como el análisis de riesgos, la gobernanza, la concienciación y la prevención e incidentes.

c) Plan de Financiación de Proyectos de Investigación e Innovación del Horizonte 2020. A finales de 2013 se aprobó el octavo programa marco de investigación e innovación de la Comisión Europea, "Horizonte 2020". Con ésta iniciativa se pretende co-financiar sobre todo la innovación en la aplicación de medidas de seguridad, fomentando el uso de desarrollos ya realizados y que necesitan su implantación en casos de uso y demostradores que muestren su eficiencia y ayuden a otras organizaciones a su puesta en marcha, con los recursos imprescindibles, evitando los errores y aprovechando las lecciones aprendidas con la financiación pública.

3.2 Estados Unidos

La Administración Obama, tras los crecientes ataques cibernéticos contra sus sistemas e infraestructuras críticas, ha priorizado la resiliencia de sus servicios públicos, financieros y otros servicios esenciales reforzando las defensas contra las ciberamenazas a través de normas técnicas y orientaciones de respuesta temprana.

El presidente Obama, tras no conseguir que el Congreso exigiese legislativamente a las empresas, en este caso operadores de infraestructuras críticas, una mejora en la protección de sus infraestructuras TIC, ya que requeriría una buen número de reformas jurídicas y un intenso programa financiero, emitió una Orden Ejecutiva extraordinaria, conocida como EO13636, que focalizaba gran parte del esfuerzo en incentivar la industria de la ciberseguridad.

17. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

Dicha orden ejecutiva firmada el 12 de Febrero de 2013, habilitaba a las agencias y gobiernos federales para desarrollar estándares de ciberseguridad para las industrias del sector privado y proponer nuevos mandatos si fuese necesario. Su objetivo primordial es ayudar a los gobiernos federales a proteger las infraestructuras críticas[18].

La orden ejecutiva erige como hubde información sobre ciberamenazas al Departamento de Seguridad Nacional, encargado de compartirla con los diversos estados y empresas del sector privado con responsabilidades sobre la protección de infraestructuras críticas. Dicha orden también requería al NIST la elaboración de un marco de seguridad cibernética de adhesión voluntaria para las empresas responsables de infraestructuras críticas, publicado en febrero de 2014[19].

A fin de acelerar la adopción del marco de buena prácticas, y tratando de mitigar el impacto económico que tendría en las compañías privadas su adopción, lanzó paralelamente un ambicioso plan de incentivos fiscales, de mercado y financieros para los operadores de infraestructuras críticas y para el mercado de la ciberprotección.

Con cierta flexibilidad y autonomía federal, algunos estados como Maryland, han fomentado la creación de polos industriales, similares a sus socios israelís, concentrando empresas tecnológicas y de servicios de ciberseguridad.

3.3 Israel

Los continuos y trascendentes cambios geopolíticos que están aconteciendo en Oriente Medio unidos a la proliferación de actores estatales y no estatales en la zona con capacidades cibernéticas avanzadas sitúan a Israel ante una situación de riesgo permanente.

Esta situación ha provocado que desde mediados de los años 1990 los sucesivos gobiernos israelís hayan priorizado el desarrollo y la competitividad de la industria nacional de ciberseguridad, destacando especialmente el programa nacional de incubadoras tecnológicas y la política de internacionalización del sector de las tecnologías del ciberespacio.

18. ExecutiveOrder -- ImprovingCriticalInfrastructureCybersecurity.http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
19. Framework forImprovingCriticalInfrastuctureProtection http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

En 1991, el Ministerio de Industria israelí creó el programa nacional de incubadoras tecnológicas[20] con el objetivo de transformar ideas tecnológicas innovadoras en empresas. Además, estas incubadoras tienen como objetivos secundarios: promover el I+D+i en capacidades estratégicas para la seguridad y defensa del país[21]; crear un ecosistema propicio para que el sector privado pueda invertir en nuevas empresas; y crear una cultura de emprendimiento en el país.

"el Ministerio de Industria israelí creó el programa nacional de incubadoras tecnológicas"

Este año el presupuesto destinado por el gobierno de Jerusalén a su programa de incubadoras tecnológicas asciende a 40 millones de euros. Las empresas que forman parte de alguna de las 22 incubadoras tecnológicas repartidas a lo largo y ancho del país –de las que se estima que un 10% dedican su actividad a la ciberseguridad- recibirán durante los dos años de apadrinamiento en la incubadora una subvención anual que oscila entre 350.000 y 600.000 euros. Del mismo modo, durante estos dos años los emprendedores reciben una sólida formación en aspectos relacionados con la dirección y administración de empresas, así como en aspectos legales y regulatorios. Tras finalizar su estancia en la incubadora, las empresas que se integren exitosamente en los mercados deberán reembolsar al gobierno el 85% de la cantidad percibida durante los siguientes veinticinco años; en caso de cese de actividad los emprendedores verán condonadas sus deudas. Otro aspecto relevante del programa nacional de incubadoras tecnológicas es el hecho de que empresas extranjeras también puedan ser beneficiarias del mismo.

La política de internacionalización de la industria de ciberseguridad israelí ha propiciado que el país se haya convertido en una de las principales potencias mundiales en la materia estimulando las exportaciones y propiciando con políticas fiscales muy ventajosas que empresas extranjeras se instalen en territorio israelí. Se estima que el 7% de la facturación mundial en materia de ciberseguridad[22] es generada por compañías israelís, muchas de ellas provenientes del programa nacional de incubadoras tecnológicas.

En definitiva, Israel es una potencia mundial en materia de ciberseguridad gracias a las políticas inclusivas e incentivadoras de su gobierno.

20. http://www.incubators.org.il/article.aspx?id=1703
21. http://www.moital.gov.il/NR/rdonlyres/5E7A4322-4D0F-4320-953C-83F94024E7AA/0/RDspreads.pdf
22. http://www.asdnews.com/news-53610/Global_Cyber_Security_Market_to_be_Worth_$76.68bn_in_2014.htm

4. Programa de incentivos en ciberseguridad español (PICE)

4.1 Marco de referencia

4.2 Incentivos

4.3 Factores Críticos de Fracaso

4.4 Conclusiones

4. Programa de incentivos en ciberseguridad español (PICE)

La Estrategia de Ciberseguridad Nacional (ECN) aprobada a finales de 2013 reconoce la importancia estratégica de disponer de un ciberespacio fiable, resiliente y seguro para, alineado con las políticas comunitarias y de la OCDE, favorecer un correcto desarrollo centrado en la economía y la sociedad digitales para el crecimiento, el empleo y el bienestar.

Si la ECN fija la hoja de ruta junto con la Agenda Digital para España (ADpE)[23], algunas de las actuaciones específicas en la consecución de los objetivos para la industria española anteriormente indicados se desarrollan en el Plan de Confianza en el ámbito Digital (PCD)[24], que respondiendo a la Estrategia Europea de Ciberseguridad (EUCS)[25],incluye también iniciativas impulsadas por ENISA.

Si bien la meta primordial es mejorar el nivel de resiliencia de la industria española, como ya se refleja en el PCD, una de las directrices colaterales es crear un "[…] eje de oportunidad para la industria TIC, destinado a proporcionar ayudas, incentivos y estímulos financieros a las empresas en todo el ciclo de la I+D+i de productos y servicios de confianza digital, fomentando la normalización técnica, la certificación y la internacionalización".

Así pues, entre otras medidas, se ha puesto en marcha una iniciativa de cooperación industrial denominada Foro Nacional para la Confianza Digital (FNCD)[26], siendo uno de sus objetivos estudiar y proponer medidas de estímulo e incentivos para favorecer las inversiones dela industria TIC y su adopción por la demanda, tanto en el sector público como en elprivado.

Pero junto con el desarrollo de la industria de la ciberseguridad, el sector empresarial nacional –desde las grandes empresas a las pymes– deberá adoptar y desplegar un marco de buenas prácticas de ciberseguridad, cumplir con un creciente marco de normativas en la materia y hacer una gestión dinámica de sus ciber-riesgos; conllevando todas estas acciones una aportación de recursos onerosa.

23. Agenda Digital para España http://www.agendadigital.gob.es/
24. Plan de Confianza en el ámbito digital (PCD) http://www.agendadigital.gob.es/planes-actuaciones/Bibliotecaconfianza/1.%20Plan/Plan-ADpE-5_Confianza.pdf
25. Estrategia Europea de Ciberseguridad (EUCS) http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
26. Foro Nacional para la Confianza Digital (FNCD)http://www.agendadigital.gob.es/FNCD/funciones/Paginas/alcance-fncd.aspx

De esta forma, el marco del Programa de Incentivos en Ciberseguridad Español (PICE) propuesto, tendría como objetivo principal recomendar un primer conjunto de incentivos diseñados para la adopción de un marco de buenas prácticas en ciberseguridad, convergente con las tareas de promoción de la financiación y el I+D+i existentes, como las recogidas en el Plan de impulso de la economía digital y los contenidos digitales[27], y como aquellas que desarrolle el Comité Técnico de Coordinación a instancias de la Medida 6 del PCD.

El esquema de incentivos propuesto, sin ánimo de ser exhaustivo y con una voluntad propositiva, requerirá adicionalmente, de actuaciones específicas que:

1. Evalúen los beneficios, efectividad y eficiencia de los incentivos en la mejora del nivel de madurez en ciberseguridad
2. Determinen las necesidades de financiación pública asociadas a cada tarea.
3. Determinen cuáles de estas acciones incentivadoras requieren esfuerzos legislativos o normativos extraordinarios.
4. Creen un modelo conceptual microeconómico que permita tener en cuenta la probabilidad de adopción del marco de ciberseguridad propuesto en la empresa española así como en la propia Administración Pública, teniendo en cuenta beneficios marginales y costes.

4.1 Marco de referencia

El primer punto decisivo a abordar, al mismo tiempo que se diseña el plan incentivador, es analizar la necesidad de adoptar un marco existente de buenas prácticas en ciberseguridad que actúe como marco de referencia en el mercado, pudiendo estar complementado con normativa sectorial, y que resulte omnicomprensivo, aglutinando tanto el sector industrial, sector servicios y tecnologías para la protección de infraestructuras críticas. Por otra parte, cabe la opción de desarrollar un marco normativo propio amparado por los agentes públicos (tal y como sucedió con el Esquema Nacional de Seguridad regulado en el RD 3/2010 de 8 de enero) y /o por los órganos de normalización habilitados a tal efecto -como AENOR-.

En opinión de los autores del documento y habida cuenta de, por una parte, la existencia de un creciente marco normativo y doctrinal en ciberseguridad y ciberdefensa; y, por otra parte, la pertenencia de España a dos grandes bloques que dibujan nuestro ámbito geopolítico, como son la Unión Europea (UE) y la Organización del Tratado del Atlántico Norte (OTAN), requeriría un esfuerzo elevado alinear un hipotético marco de ciberseguridad nacional con nuestro compromisos asociados a los ejes de la política exterior.

27. http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-impulso-contenidos-digitales.aspx

" se recomienda la adopción de un marco de referencia reconocido"

Es por eso que se recomienda la adopción de un marco de referencia reconocido que permita un reconocimiento cruzado con nuestros socios internacionales, facilitando por extensión la labor interna de las empresas españolas de implantar dichos controles, ya que serían reconocidos en los mercados globales, facilitando los costes asociados a la internacionalización de las mismas. Dicho marco de buenas prácticas en ciberseguridad, sin embargo, podría ser sometido a un proceso de normalización nacional por parte de los órganos nacionales habilitados a tal efecto.

Para alcanzar la estandarización del nivel de ciberseguridad en nuestro territorio, a través de la adopción de este marco de buenas prácticas, el Gobierno deberá respaldar este reto mediante el establecimiento un conjunto de incentivos con una visión multisectorial que posibiliten que las empresas puedan implementar aquellas medidas que les permitan disponer de un ciberespacio seguro y poder así dar respuesta a uno de los principios rectores de la ESN, la responsabilidad compartida.

4.2 Incentivos

El Programa de Incentivos en Ciberseguridad Español (PICE) ha comenzado por la realización de un examen inicial de las propuestas de incentivos públicas a tal efecto para definir la gama de incentivos a ser incluidos en el presente estudio.

En el presente estudio conjunto entre **THIBER** e **ISMS Forum Spain** se propone un plan de incentivos vertebrado sobre 7 líneas de acción, agrupando un total de 23 acciones incentivadoras, en los siguientes términos:

1. Marco de incentivos legales

1.1. Programa de ayudas fiscales, reduciendo las tasas impositivas para empresas en la adquisición de tecnologías y servicios que soporten la adopción del marco de ciberseguridad establecido. Dichas soluciones y servicios deberán ser debidamente justificados a través un proceso de homologación y/o certificación por parte de un agente público que además deberá definir el concepto de “gastos admisibles” o “desgravables” tanto en costes operativos (OPEX) como en inversiones (CAPEX).

1.2. Reducción de los costes y tasas administrativas en el registro de patentes nacionales relativas a la ciberprotección, así como una mejora de la protección de patentes tecnológicas en ciberprotección.

1.3. Elaboración de un reglamento y legislación específico en materia de ciberseguridad para la industria española y las AAPP, unificando el cumplimiento así como las potenciales superposiciones de requisitos existentes y complementando la Directiva de Seguridad de las Redes y de la Información (SRI)[28], el futuro Reglamento Europeo de Protección de Datos Personales y el Reglamento de Identidad Electrónica y Servicios de Confianza. Este reglamento deberá reflejar un análisis de las iniciativas internacionales, reconociendo reglamentos normativos extranjeros equivalentes (tipo Safe Harbor), reduciendo la carga de auditoría y validación de cumplimiento.

1.4. Limitación de responsabilidades civiles y penales mediante la demostración de una implementación del marco de control de ciberseguridad mencionado, demostrando una gestión diligente y el debido control sobre los procesos empresariales en lo relativo a sus medidas de protección cibernéticas.

2. Acceso a financiación y fondos de inversión

2.1. Inclusión dentro de los instrumentos de financiación de la Administración General del Estado ya existentes y del Instituto de Crédito Oficial, de nuevas variables en la concesión de programas de líneas de crédito y financiación estatales con condiciones ventajosas por cumplimiento y adopción del marco de buenas prácticas de ciberseguridad establecido a tal efecto.

2.2. Ayudas fiscales y financiación de actividades asociadas al I+D+i en materia de ciberseguridad, ya mencionado en el Plan de desarrollo e innovación del Sector TIC[29], con especial énfasis en aquellos programas investigadores ligados al fomento de la investigación técnica (PROFIT), ampliando la política industrial (AVANZA) y creando más proyectos tractores dentro del Plan Nacional de I+D+I relacionados con la ciberprotección, acercando la oferta y la demanda.

2.3. Ayudas gubernamentales a la inversión en empresas de ciberseguridad nacionales y start-ups en todo el ciclo de inversión, ya sea capital semilla o capital riesgo, para su internacionalización, sustentado y asesorado por grupos de interés y sectoriales específicos, pudiéndose otorgar créditos desgravables sobre el impuesto sobre la renta tanto a los inversores como a las propias empresas receptoras cuyo criterio de elegibilidad se adecue a unas pautas formales definidas, aprovechando el ecosistema e iniciativas público-privadas actuales.

28. http://europa.eu/rapid/press-release_IP-13-94_es.htm
29. http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-sector-tic.aspx

3. Impulso del mercado de ciberseguridad

3.1. Ayudas específicas en el acceso a nuevos mercados y proyectos de internacionalización, mediante campañas comerciales y diplomáticas específicas, con especial énfasis en LATAM y Oriente Medio, aprovechando los medios existentes en la Administración General del Estado así como el Plan de Internacionalización de Empresas Tecnológicas[30] de laADpE.

3.2. Creación de un polo industrial, que actúe como una incubadora y aceleradora empresarial enfocadas en las tecnologías de ciberprotección. Ésta deberá ser el embrión de un ecosistema propicio para que el sector privado pueda invertir en nuevas empresas. El presente incentivo será la prolongación lógica de la medida PDC-9 del Plan de Confianza Digital, así como una línea más a incluir en las políticas del Ministerio de Economía y Competitividad a través de la Secretaría de Estado de Economía y Apoyo a la Empresa.

3.3. Desarrollo de un Fondo Nacional de Inversión de Ciberseguridad (FNIC), permitiendo la inversión pública en este sector, de forma que permita balancear la necesidad de existencia de empresas de nicho en este sector, pero también pueda contemplar reducir la fragmentación actualmente existente actuando como socio inversor público de una empresa robusta (denominada "campeón") que pueda competir en los mercados internacionales.

4. Desarrollo del mercado de los ciberseguros

4.1. Estimular la demanda del mercado de servicios de ciberseguros, trasladándolos como una obligatoriedad en la contratación con la Administración Pública.

4.2. Campañas de reducción de costes en la contratación de pólizas de seguro, a través de mecanismos como:

El reconocimiento de la adopción de marcos de ciberseguridad con un nivel de madurez determinado como un mecanismo de reducción de daños propios y a terceros derivados de un ciber incidente.

La reducción del coste de las primas mediante la asunción de parte de las coberturas de las aseguradoras privadas a través de programas de reaseguro.

4.3. Creación de fondos de garantía ante ciberamenazas de alto impacto, considerados riesgos "no asegurables", con el objetivo de reemplazar o estabilizar el mercado privado, habilitado a través del Consorcio de Compensación de Seguros, adscrito al Ministerio de Economía y Competitividad, y a través de la Dirección General de Seguros y Fondos de Pensiones.

30. http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-empresas-tecnologicas.aspx

4.4. Habilitar la capacidad del Consorcio de Compensación de Seguros, actuando como asegurador directo en el caso de que el mercado privado falle en la provisión de las ciberpólizas (por ejemplo por de falta de seguro o insolvencia del asegurador), pero sin entrar en competencia con el sector privado.

5. Reconocimiento público

5.1. Elaboración de un catálogo de empresas habilitadas para la prestación de servicios de ciberseguridad.

5.2. Obligación de prácticas full-disclosureen la Memoria Anual Corporativa de las empresas privadas, mostrando sus actividades e hitos más relevantes en materia de ciberseguridad así como la necesidad de comunicar incidentes de seguridad a los organismos públicos y al propio mercado.

5.3. Profesionalización del sector de la ciberseguridad, mediante la creación de esquemas de certificación y capacitación de profesionales y empresas. De esta forma se aumentará la tasa de empleo con trabajadores altamente especializados.

6. Optimización de los procesos de contratación con la Administración Pública

6.1. Reducción de los plazos de contratación con la Administración Pública para aquellas empresas que acrediten la adopción del marco de control.

6.2. Reducción de los plazos administrativos asociados a la acreditación de sistemas clasificados y a la homologación de sistemas TIC.

6.3. Reducción de la carga burocrática y de trámites en la acreditación de capacidades en concursos públicos.

7. Priorización en la asistencia técnica por parte del Estado

7.1. Soporte consultivo en la implantación del marco de referencia de ciberseguridadseleccionado.

7.2. Mejora en el nivel de soporte técnico ante ciberincidentes, siempre que de forma previa la empresa receptora haya activado mecanismos de compartición de información y demostrado diligencia en la adopción del marco de control, priorizando la prestación de capacidades de INCIBE como punto neutro de gestión de incidentes.

7.3. Definición de guías concisas relativas a cómo implementar las medidas de seguridad necesarias en el seno de la empresa.

INCENTIVO	PRIORIDAD
1. Marco de incentivos legales	
1.1. Programa de ayudas fiscales	Media
1.2. Reducción de los costes y tasas administrativas en el registro de patentes	Baja
1.3. Elaboración de un reglamento y legislación específico en materia de ciberseguridad	Alta
1.4. Limitación de responsabilidades civiles y penales	Baja
2. Acceso a financiación y fondos de inversión	
2.1. Creación de un programa de líneas de crédito y financiación	Media
2.2. Ayudas al I+D+i en materia de ciberseguridad	Media
2.3. Ayudas gubernamentales a la inversión en empresas de ciberseguridad nacionales y startups	Alta
3. Impulso del mercado de ciberseguridad	
3.1. Ayudas específicas en el acceso a nuevos mercados y proyectos de internacionalización	Media
3.2. Creación de polos industriales, incubadoras y aceleradoras empresariales	Media
3.3. Desarrollo de un Fondo Nacional de Inversión de Ciberseguridad	Baja
4. Desarrollo del mercado de los ciberseguros	
4.1. Estimular la demanda del mercado de servicios de ciberseguros	Alta
4.2. Campañas de reducción de costes en la contratación de pólizas de seguro	Media
4.3. Creación de fondos de garantía ante ciberamenazas de alto impacto.	Alta
4.4. Habilitar la capacidad del Consorcio de Compensación de Seguros, actuando como asegurador directo en el caso de que el mercado privado falle en el seguro.	Media
5. Reconocimiento público	
5.1. Elaboración de un catálogo de empresas habilitadas para la prestación de servicios de ciberseguridad.	Media
5.2. Obligación de prácticas full-disclosureen la Memoria Anual Corporativa de las empresas	Media
5.3. Profesionalización del sector de la ciberseguridad, mediante la creación de esquemas de certificación y capacitación de profesionales y empresas	Alta
6. Optimización de los procesos de contratación con la Administración Pública	
6.1. Reducción de los plazos de contratación con la administración publica	Media
6.2. Reducción de los plazos administrativos asociados a la acreditación de sistemas clasificados y a la homologación de sistemas TIC.	Baja
6.3. Reducción de trámites en la acreditación de capacidades en concursos públicos.	Baja
7. Priorización en la asistencia técnica por parte del Estado	
7.1. Soporte en la implantación del marco de referencia seleccionado	Alta
7.2. Mejora en el nivel de soporte técnico ante ciberincidente	Alta
7.3. Definición de guías concisas relativas a cómo implementar las medidas necesarias en el seno de la empresa	Media

4.3 Factores Críticos de Fracaso

En la implementación práctica del programa de Incentivos propuesto, tras el análisis de las estrategias similares abordadas por otras naciones así como la propia idiosincrasia nacional, y habida cuenta de que el éxito de otras iniciativas analizadas no será fácilmente replicable y trasladable de una realidad nacional a otra, se han identificado tres Factores Críticos de Fracaso (FCFs) asociados al programa. La identificación de los mismos suponen un primer paso primordial que fijará el camino hacia la consecución de los objetivos marcados.

1. Primer FCF: Campaña de promoción insuficiente.

El Programa debe venir acompañado de una política de promoción, comunicación y difusión pública clara y concisa del marco de incentivos, creando diversos prototipos de caso de negocio que muestren el escenario de retorno de inversión derivado de la mejora de la ciberseguridad en las organizaciones. Esta campaña de medios debe tener alcance internacional a través de las embajadas, de forma que actúen como un atractor de capital de inversión extranjero.

2. Segundo FCF: Marco de aplicación cortoplacista.

El marco de incentivos propuesto debería manejar un horizonte temporal quinquenal o incluso decenal, rompiendo así los periodos de cuatrienales de las legislaturas, ya que el enfoque de la estrategia a seguir debe ser a medio y largo plazo, si bien se contemplan algunas líneas de incentivos a corto, como las que referencian al mercado de los ciberseguros. Las políticas de corto plazo no son capaces de asegurar el suficiente nivel de financiación e inversión en un ámbito que requiere altos niveles de capacitación bajo el perfil de los recursos humanos y largos tiempos de investigación y desarrollo.

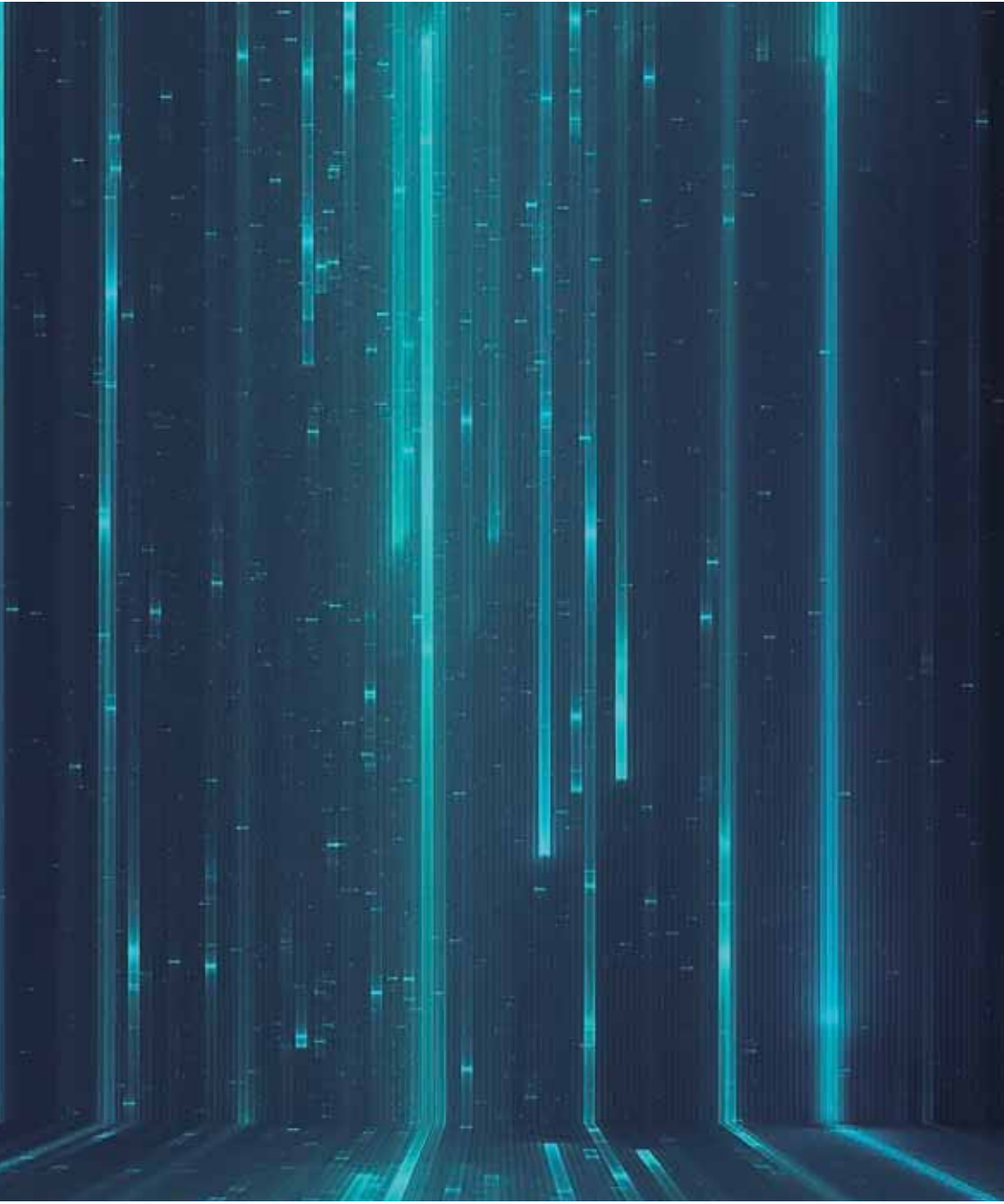
3. Tercer FCF: Ámbito de aplicación del marco de control

El marco de control debería ser de aplicación exclusiva al sector privado. Para que toda la cadena de valor de ciberseguridad empresarial e industrial sea realmente resiliente, la aplicación del marco de buenas prácticas debería ser equitativa y, por extensión, de aplicación también en la Administración Pública.

4.4 Conclusiones

El Gobierno necesita como complemento a las políticas anteriormente mencionadas, que entre los planes a diseñar se encuentre el desarrollo de un plan de incentivos empresariales realista, que permita garantizar una correcta y masiva aplicación de medidas de ciberprotección en el tejido empresarial en un plazo razonablemente corto, sustentado sobre la premisa de la distribución de los costes de la ciberseguridad entre todos los actores involucrados

Así pues, la adopción del marco del Programa de Incentivos en Ciberseguridad Español (PICE) propuesto, supondría la primera aproximación inclusiva de esta naturaleza, orientada a mejorar el nivel de ciber-resilencia de la industria española así como a potenciar un mercado emergente de productos y servicios de ciberprotección, amparado bajo estrategias de cooperación y de compartición de la responsabilidad y conocimientos.



UNA INICIATIVA DE:

ISMS Forum Spain

THIBER
The cybersecurity think tank