Capítulo sexto

La cooperación público-privada en el fomento de la cultura de ciberseguridad

Gregorio Miguel Pulido Alonso
Teniente Coronel del Ejército de Tierra DIM
Jefe de la Sección de Preparación del MCCD

Rafael Rosell Tejada
Director Comercial de S2Grupo

Resumen

En una sociedad avanzada como la nuestra, es capital conseguir una cultura de ciberseguridad global que nos haga más resilientes. La concienciación en esta materia, parte de la cultura de ciberseguridad, es clave en la consecución de este objetivo. Sin embargo, llegar a todos los ciudadanos requiere que los principales actores del sector público y privado en ciberseguridad hagan un esfuerzo en la misma dirección. La consecución de un objetivo como este, unido a la velocidad a la que evolucionan unas amenazas sin precedentes, obliga a todos a alinear sus esfuerzos, puesto que de otra forma no será posible alcanzar un estado de madurez en nuestra cultura de ciberseguridad que garantice un bajo nivel de riesgo.

Para que la cooperación entre ambos sectores sea efectiva esta debe materializarse en forma de «asociación» (*partnership*), con unas normas de constitución y funcionamiento bien establecidas. El instrumento legal, en el caso español, que serviría para articular dicha alianza, podría tomar la forma de convenio. En cualquier caso, será necesario que los asociados principales dediquen, en la forma que se acuerde, suficientes recursos humanos y materiales a este esfuerzo.

Actualmente, nos encontramos en un escenario en el que los diversos actores han puesto diferentes iniciativas en marcha, generalmente orientadas a resolver sus propios problemas y, en muchos casos, divergentes unas de otras.

Palabras clave

concienciación, resiliencia, cultura de ciberseguridad, ciberdefensa, cooperación público privada, incidente, ciberincidentes, programa.

Abstract

In an advanced society like ours, it is capital to achieve a comprenhensive cybersecurity culture which enable us to be more resilient. Cybersecurity awareness, as a part of the cybersecurity culture, is a key element to achieve this goal. In order for this awareness to reach all of the citizens, it is necessarry that both, public and private sectors, join efforts in the same direction. This partnership will benefit, not only the nation, but also the organizations involved.

To be effective, this cooperation shouldn't rest as a simple declaration of intent. On the contrary, this Public Private Partnership should be created with a clear mandate and well defined rules. The legal framework, in the Spanish case, could be on the basis of a formal agreement signed by the partners. In any case, it will be necessary that the stakeholders involved commit enough resources to this common effort.

Nowadays, we find a scenario where different actors have started several initiatives conducting in general terms to resolve their own issues, but in some cases diverging the ones from the others.

Keywords

Awareness, resilience, cybersecurity culture, cyberdefence, public private partnership, incident, cyberincident, program.

Introducción

El mundo en el que vivimos y en el mundo que vamos a vivir marca la creciente e incesante necesidad de la ciberseguridad. Nos enfrentamos a cambios muy rápidos en la sociedad determinados por una serie de «megatendencias» que lo están transformando todo: la hiperconectividad, la aceleración tecnológica y el incremento de población conectada a la Red, impulsada por el crecimiento continuo de la población que habita el planeta.

Cada una de estas megatendencias tiene la capacidad de cambiar el mundo por sí mismas. Juntas tienen una capacidad transformadora sin precedentes en la historia de la humanidad.

Los cambios exponenciales que se están produciendo en las tecnologías de la información y las comunicaciones son la base de ese gran efecto transformador de la sociedad. Gartner habla de un «nexo de fuerzas»[1], una convergencia de lo social, la movilidad, la nube y el acceso a enormes volúmenes de información y su procesamiento mediante técnicas de *Big Data*, impulsado por la aparición de múltiples tipos de dispositivos con precios cada vez menores, que nos permiten un acceso ubicuo y universal a «todo». En definitiva, un nexo de fuerzas que allanan el camino hacia una sociedad completamente digital.

La aceleración tecnológica descrita por el fundador de Intel y conocida como la Ley de Moore tiene un impacto directo en muchos campos de la ciencia y la tecnología, no solo en el campo de las TIC. Campos como la salud, la energía, la industria, la inteligencia artificial, el transporte, la defensa, etcétera, también están experimentando este proceso de transformación exponencial.

La hiperconectividad también está jugando un papel clave en la transformación digital de la sociedad. La conexión de «todo» en red conlleva la aparición de nuevos productos y servicios inimaginables hace tan solo unos años y el desarrollo, en consecuencia, de un modelo económico completamente nuevo y diferente basado en el concepto de *IoT*, *Internet of Things,* o *IoE*, *Internet of Everything*[2].

Hablamos en términos generales de la «caída de las fronteras». Desde el punto de vista de la seguridad la identificación del perímetro de protección ha sido siempre, en todos los ámbitos, la primera fase para determinar el despliegue de defensas en una organización. Hoy por hoy, las fronteras han caído por la hiperconectividad. No sabemos dónde está la frontera digital de una organización y, por tanto, no podemos determinar el perímetro de protección. Se habla en términos generales de que «la frontera somos las personas» y esta es la razón por la que el éxito de los programas de concienciación es esencial y se debe basar en un cambio de cultura de ciberseguridad.

[1] http://www.gartner.com/it-glossary/nexus-of-forces/
[2] https://en.wikipedia.org/wiki/Internet_of_things

La Real Academia Española, entre otras acepciones, define cultura como «el conjunto de conocimientos que permite a alguien desarrollar su juicio crítico». Por extensión, se puede definir la cultura en ciberseguridad como el conjunto de conocimientos y habilidades que permiten a un ser humano desenvolverse en el ciberespacio de una manera segura.

El ciberespacio se define, en la Estrategia de Ciberseguridad Nacional[3], como el dominio global y dinámico compuesto por las infraestructuras de tecnología de la información —incluida internet—, las redes y los sistemas de información y de telecomunicaciones. En otras palabras, el ciberespacio está compuesto por internet y el resto de redes a las que accedemos con nuestros nuevos dispositivos.

Esta cultura de seguridad global es, en esencia, lo que necesitamos madurar para conseguir un estado de ciberriesgo nacional asumible. Sin embargo, no todo el mundo requiere un mismo nivel de seguridad, dependerá, fundamentalmente, de la relación, personal o profesional, que el individuo tenga con el ciberespacio. Así, por ejemplo, una persona que accede de manera ocasional con su *smartphone* a una red social y un directivo de una organización que maneja información sensible con multitud de dispositivos tienen, sin duda, requisitos de seguridad diferentes. Lógicamente, esta situación conlleva niveles de madurez distintos en sus culturas de seguridad.

En cualquier caso, todos los usuarios del ciberespacio deben tener un mínimo conocimiento, claro y reflexivo, del riesgo real que suponen las amenazas a las que se enfrentan en él, así como la manera de hacerles frente. En otras palabras, los ciudadanos digitales deben estar concienciados en esta materia. Para proteger la sociedad es, por tanto, necesario que todo ciudadano o empleado de una organización pública o privada tome conciencia de los riesgos a los que se enfrenta la sociedad en su conjunto.

La Escuela de Altos Estudios de la Defensa, en septiembre de 2013, publicó un completo monográfico que abordaba en profundidad la necesidad de crear una conciencia nacional de ciberseguridad[4]. El objeto del presente artículo es presentar datos, teorías e iniciativas existentes en esta materia, para concluir en cómo la cooperación entre el sector público y privado se constituye, dada la magnitud del problema, en la mejor forma de abordar la concienciación en ciberseguridad a nivel nacional y de situar la cultura global de ciberseguridad en un nivel que minimice el riesgo en esta materia.

El eslabón más débil de la cadena

En este entorno —hiperconectado, hipertecnológico, universal y con acceso ubicuo a todo— se están diseñando los nuevos modelos económicos de la

[3] http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional

[4] Escuela de Altos Estudios de la Defensa, Monografías 137. **«**Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario». 2013.

sociedad digital y nadie se quiere quedar atrás. La Unión Europea, en su documento «Estrategia de Ciberseguridad»[5], afirma que el uso de la tecnología está directamente relacionado con el incremento de la productividad y el incremento del PIB de los países hasta el punto que el Mercado Único Digital supone un incremento de 500.000 millones de euros anuales de su producto interior bruto (en torno a un 5 % del PIB de la zona euro).

Los Gobiernos están impulsando, a través de sus Agendas Digitales, la adopción de las TIC a todos los niveles a través de sus políticas de «tracción» porque son evidentes los efectos positivos que estos avances producen en la sociedad a todos los niveles. No obstante, este desarrollo tecnológico sin precedentes no está exento de riesgos. Uno de ellos es la necesidad de conseguir que esta nueva sociedad digital sea un espacio seguro y de confianza para todos. No en vano, todas las agendas digitales que se están desarrollando tienen en común su apuesta por la seguridad y el desarrollo de la confianza en la Red.

La Agenda Digital Europea es una de las siete iniciativas emblemáticas en la Estrategia Europa 2020 y se diseña en torno a siete campos de actuación principales y dieciséis acciones clave. El tercer campo de acción es «Fomento de la confianza y seguridad en Internet» con la línea de acción AC6, «Conseguir una política de seguridad reforzada y de alto nivel», y la AC7, «Medidas incluyendo legislativas para combatir los ciberataques».

En nuestro caso, la Agenda Digital Española, alineada con la europea, pretende impulsar con acciones concretas la sociedad digital en toda su amplitud. Para conseguirlo se estructura en torno a seis grandes objetivos con sus respectivas líneas de acción. El cuarto es «Reforzar la confianza en el ámbito digital», donde se apuesta claramente, entre otras iniciativas, por la concienciación y sensibilización de la sociedad en esta materia con un enfoque claro hacia las personas. En el ámbito de actuación de la agenda se desarrolla el «Plan de confianza en el ámbito digital» con cinco ejes estratégicos:

- Experiencia digital segura.
- Oportunidad para la industria TIC.
- Nuevo contexto regulatorio.
- Capacidades para la resiliencia.
- Programa de excelencia en ciberseguridad.

Este interés unánime en la seguridad y la confianza en la Red responde al enorme crecimiento que están teniendo cualitativa y cuantitativamente los incidentes de seguridad. El número de amenazas se multiplica y cada vez son más complejas y esto está creando una sensación de inseguridad que puede frenar el desarrollo tecnológico si no se toman cartas en el asunto. En

[5] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

su informe «Global Risk»[6] del año 2014, el World Economic Forum llegaba a plantear un escenario plausible al que llamaba «Cybergedon».

El «Special Eurobarometer 423» sobre ciberseguridad, publicado en 2015, pone cifras a este problema de inseguridad y desconfianza en el mundo digital y, en su introducción, lo cuantifica en miles de millones de euros de pérdidas anuales en Europa, con más de 150.000 tipos de virus en libre circulación y más de un millón de víctimas diarias del cibercrimen. En cuanto a los datos en España, el eurobarómetro refleja el 62 % de los ciudadanos que no se sienten bien informados sobre los ciberdelitos (frente a un 50 % en Europa). Asimismo, el 89 % de los ciudadanos cree que el riesgo de ser víctima de un ciberdelito está aumentando y al 87 % (un 85 % en Europa) le preocupa que las autoridades públicas no mantengan segura su información personal en internet (frente a un 67 % en Europa).

Por lo que la situación en España es, si cabe, incluso peor que en Europa en términos generales de desconfianza.

En 2015, la compañía de seguros británica Lloyd's estimó que el coste anual de los ciberataques rondaba los 400 billones de dólares al año, incluyendo los daños directos producidos más los daños derivados de las tareas de recuperación. El presidente de la compañía, Stephen Catlin, con más de cuarenta y dos años de experiencia, llegó a decir en Londres en febrero de 2015: «los balances de las aseguradoras no son lo suficientemente grandes para cubrir los riesgos de ciberseguridad. Es, sin duda, el mayor y el más sistémico de los riesgos que he afrontado en toda mi carrera»[7].

Para IBM, en 2014, el 95 % de los ciberincidentes fueron causados por errores humanos, entre ellos introducir información sensible o incluso clasificada en sistemas conectados a internet[8]. Solamente el 45 % de los ataques fueron realizados por *outsiders* (personal ajeno a la empresa). Según Kaspersky[9], la cifra es aproximadamente del 80 %. Coincidiendo en el dato, el Gobierno de los Estados Unidos específica que sobre el 80 % de los ciberincidentes suceden por tres factores: pobres prácticas de los usuarios, pobres prácticas en la gestión de las redes y los datos, y pobre implementación de la arquitectura de red[10].

En 2013 el principal objetivo de los ciberdelincuentes eran los sistemas de las empresas. En 2014 pasaron a ser las personas[11]. En esa misma línea, Deloitte afirma que, aunque los ciberdelincuentes reinvierten una parte de

6 http://reports.weforum.org/global-risks-2014/

7 http://internacional.elpais.com/internacional/2015/02/06/actualidad/1423257712_728999.html

8 IBM 2015, Cyber Security Intelligence Index, *Analysis of cyber attack and incident data from IBM's worldwide security services operations.*

9 Kaspersky. Cybersecurity Awareness Brochure.

10 The DoD Cybersecurity Culture and Compliance Initiative.

11 Check Point, 2015 Security Report.

sus beneficios en desarrollar nuevas capacidades técnicas para sobrepasar las barreras de seguridad, el procedimiento que más emplean para acceder al usuario final es la ingeniería social a través de internet[12]. Una muestra, según Symantec[13], es que las campañas de *spear-phising* se incrementaron en un 55 % en 2015 y las técnicas de ingeniería social llegaron a un nivel de sofisticación elevado, dirigido incluso a sobrepasar los sistemas con doble factor de autenticación. También se han observado ataques realizados con *malware* con la finalidad de robar datos personales para su uso posterior.

El perfil profesional de las personas elegidas como objetivo es muy amplio. Por ejemplo, durante la campaña de ataque conocida como «Witchcoven» los adversarios recogieron una ingente cantidad de datos de ejecutivos, diplomáticos, funcionarios gubernamentales y personal militar, especialmente en Europa y Estados Unidos[14]. Sin embargo, en los últimos años se ha observado un crecimiento regular en ciberataques a empresas de menos de doscientos cincuenta empleados, llegando incluso a suponer un 43 % de todos los ataques.

Finalmente, y como muestra de la forma de trabajo de los ciberdelincuentes, Checkpoint insistía en que en 2014, habían observado en los sistemas investigados por ellos, un nivel de ciento seis descargas por hora de ficheros infectados con *malware* desconocido. El 52 % de este *malware* venía dentro de un .pdf mientras que el 3 % eran ficheros correspondientes al paquete Office. En el ciberataque contra el sector energético ucraniano conocido como «Black Energy» el medio empleado para insertar el *malware* fue un fichero de extensión doc[15].

Ante esta situación, que se agrava día a día, es necesario fomentar una cultura de ciberseguridad global adecuada a través de estrategias de concienciación, tal y como se recoge en la «Estrategia de Ciberseguridad para la Unión Europea» que afirma de manera clara que «los usuarios finales contribuyen de forma decisiva a garantizar la seguridad de las redes y los sistemas de información: es preciso que sean conscientes de los riesgos que corren en línea y sean capaces de adoptar medidas sencillas para protegerse de ellos».

Ciberresiliencia y concienciación en ciberseguridad

No existe a nivel nacional o multinacional una definición acordada sobre el término ciberresiliencia. Sin embargo, basándonos en los trabajos de MITRE[16]

[12] Deloitte, Cyber crime: a clear and present danger. Combating the fastest growing cyber security threat.

[13] Symantec, Internet Security Threat Report, volume 21, April 2016.

[14] Special Report FIREEYE Threat Intelligence pinpinting targets: Exploiting Web Analytics to Ensnare Victims, Jonathan Wrolstad Barry Vengerik.

[15] Kaspersky, IT Threat evolution in Q1 2016, Alexander Gostev, Roman Unuchek, Maria Garnaeva, Denis Makrushin, Anton Ivanov.

[16] MITRE Corporation, Cyber Resilience Metrics: Key Observations, Deborah Bodeau, Richard Graubart.

la podemos definir como «la capacidad de anticiparse, resistir, recuperarse y adaptarse a condiciones hostiles consecuencia de condiciones ambientales adversas, estrés de los sistemas por distintas causas o ciberataques».

Symantec ha desarrollado un modelo para mejorar la ciberresiliencia en una empresa basado en cinco pilares[17]. El primero de ellos es la «preparación/identificación», que se basa en gran medida en el conocimiento de los riesgos a los que se enfrenta la empresa y en el que una de las acciones clave es la concienciación de los usuarios. Los otros pilares de este modelo son la protección, detección, respuesta y recuperación.

El modelo de gestión de resiliencia de un equipo de respuesta ante emergencias informáticas (CERT *Resilience Management Model* (CERT-*RMM*))[18], desarrollado bajo los auspicios del Departamento de Defensa de Estados Unidos por el Instituto de Ingeniería del Software (SEI) de la Universidad Carnegie Mellon, contempla como una de las áreas que componen dicho modelo la formación y concienciación de la organización [*Organizational Training and Awareness* (*OTA*)].

Así pues, basados en estos dos modelos dirigidos al ámbito empresarial fundamentalmente, vemos cómo la mejora de los niveles de ciberresiliencia de una organización pasa, indefectiblemente, por impulsar la cultura de ciberseguridad y la concienciación. Este hecho es extrapolable al ámbito nacional como veremos posteriormente, aunque no vamos a profundizar más en la ciberresiliencia, ya que se trata más profundamente por el Instituto de Estudios Estratégicos en un gran artículo de opinión firmado por el profesor Salvador Carrasco[19].

Iniciativas existentes

Vista pues la necesidad de una concienciación en ciberseguridad, de manera sucinta vamos a repasar distintas iniciativas para extraer claves que nos sirvan para acometer esta tarea.

En España

A nivel nacional y dentro del sector público, el objetivo IV de la Estrategia de Ciberseguridad Nacional (ECSN) es «sensibilizar a los ciudadanos, profesionales, empresas y Adminstraciones Públicas españolas de los riesgos derivados del ciberespacio». Asimismo, especifica claramente que «la gestión

[17] SYMANTEC, The Cyber Resilience Blueprint: A New Perspective on Security.

[18] CERT® Resilience Management Model, Version 1.2, Richard A. Caralli, Julia H. Allen, David W. White.
Lisa R. Young, Nader Mehravari, Pamela D. Curtis, February 2016, CERT Program.

[19] «Ciber-resiliencia», Luis de Salvador Carrasco, IEEEs Cuaderno de opinión.

eficaz de los riesgos derivados del ciberespacio debe edificarse sobre una sólida cultura de ciberseguridad. Ello requiere de los usuarios una sensibilización respecto de los riesgos que entraña operar en este medio, así como el conocimiento de las herramientas para la protección de su información, sistemas y servicios».

Derivado directamente de la ECSN, se ha aprobado el Plan de cultura de ciberseguridad, concienciación, sensibilización y educación, cuyo objetivo es «promover la cultura de ciberseguridad entre ciudadanos, profesionales, empresas y Adminstraciones Públicas españolas mediante el desarrollo de actividades y mecanismos para la sensibilización, concienciación, formación y educación que renueven y doten de nuevos conocimientos sobre los riesgos derivados del ciberespacio y el uso seguro y responsable de las TIC».

El Plan se articula en tres ejes de acción: sensibilización, concienciación y conocimiento; normativa y buenas prácticas. Cada eje tiene asignado un organismo de la Administración pública como responsable y otros como colaboradores. Asimismo, se contemplan unos recursos financieros y humanos para poderlo llevar a cabo.

En cuanto a las acciones concretas que se derivan de dicho Plan, algunas de ellas son: desarrollar actividades de sensibilización para asegurar que los ciudadanos, empresas, profesionales, red académica, operadores estratégicos y operadores de infraestructuras críticas tienen acceso a información relativa a vulnerabilidades, ciberamenazas e información para proteger mejor su entorno tecnológico; proponer contenido específico de sensibilización en ciberseguridad para incluirlos en los módulos educativos dirigidos a todos los niveles de la enseñanza en cumplimiento a los establecido en el convenio de Lanzarote[20]; proponer contenido específico de sensibilización en ciberseguridad para incluirlos en los programas de administración de las Adminstraciones Públicas; desarrollar programas de concienciación en ciberseguridad, en colaboración con agentes del sector público y privado potenciando, a través de los organismos con competencias en la materia, la necesaria coordinación y racionalización de esfuerzos; desarrollo de un catálogo de buenas prácticas; detección de necesidades y difusión de herramientas y servicios de ciberseguridad.

En línea con todo lo anterior, los principales actores públicos y privados en el ámbito de la ciberseguridad han ido desarrollando diferentes modelos e iniciativas basadas en el establecimiento de marcos de buenas prácticas.

El Centro Criptológico Nacional CCN-CERT ha sido uno de los pioneros y uno de los más activos y eficientes en definir una fuerte estrategia de generación de información de valor que sirva fundamentalmente a las Adminstraciones

[20] http://www.fapmi.es/imagenes/subsecciones1/1de5_Doc_03_Convenio %20Lanzarote_Parlamentarios.pdf

Públicas —que es su ámbito de actuación— pero también a empresas para protegerse frente a los ciberriesgos.

Dicho centro ha desarrollado una fuerte actividad de generación de Guías[21] que cubren la inmensa mayoría de aspectos relevantes, desde políticas o procedimientos hasta guías técnicas de configuración de entornos. Se trata de guías de enorme valor que sirven de marco de referencia a los equipos técnicos para desarrollar el trabajo de protección de sus perímetros.

Por otro lado, ha realizado una intensa labor en el desarrollo de informes del estado[22] de las amenazas y las previsiones que, desde el CCN-CERT, tienen del desarrollo futuro de las mismas. Así mismo, dicho centro ha organizado diversos cursos de formación.

Por otro lado, también participa en el Mes Europeo de la Ciberseguridad[23], organizado por *ENISA* (Agencia Europea de las Redes y de la Información), cuyo principal objetivo es «concienciar a los ciudadanos de la necesidad de preservar la información y abogar por un cambio en la percepción de las ciberamenazas mediante la promoción de la seguridad de los datos y la información, la educación, el intercambio de buenas prácticas y la competencia».

Otra institución muy activa es el Instituto de Ciberseguridad Nacional (INCIBE) que, por su parte, ha desarrollado diferentes iniciativas orientadas tanto a empresas como ciudadanos. En el ámbito específico del programa de sensibilización, concienciación, educación y formación definido por el Plan de Confianza Digital y la Estrategia de Ciberseguridad Nacional 2013, desde el año 2015 INCIBE lleva a cabo el proyecto Servicio de Creación, mejora y soporte de contenidos de ciberseguridad y confianza digital de INCIBE dirigidos a las empresas y ciudadanos. La Oficina de Seguridad del Internauta (OSI)[24] es una de sus principales iniciativas en este ámbito. Es una oficina que ofrece materiales, herramientas y buenas prácticas. Cabe destacar, por ejemplo, por su interés, el «kit de concienciación»[25] que INCIBE ha desarrollado y ha puesto a disposición de las empresas. Dicho kit propone una serie de prácticas y materiales a distribuir. La primera fase, por ejemplo, consistiría en lanzar un ciberataque dirigido, dentro de la empresa, con un fichero infectado con *malware* inocuo y cuyo vector de infección sería el correo electrónico o una memoria USB. INCIBE incluso propone los mensajes y ficheros a utilizar. Una vez realizada esta primera fase, ya se pasaría una fase formativa en la que se distribuyen materiales como pósteres o trípticos, que también han sido preparados por INCIBE. Se daría continuidad posteriormente a esta tarea mediante consejos de ciberseguridad de periodicidad mensual.

21 https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html
22 https://www.ccn-cert.cni.es/informes.html
23 https://www.enisa.europa.eu/news/enisa-news/ecsm
24 https://www.osi.es
25 INCIBE, Kit de concienciación, manual de implantación.

Por otro lado, los CERT de ámbito autonómico (CSIRT-CV, CESICAT, ANDALUCIA-CERT), en el ámbito de sus funciones, también han desarrollado programas de concienciación basados en portales donde se puede encontrar información relativa a riesgos y buenas prácticas. Merece la pena destacar la gran labor desarrollada por el CSIRT-CV en este ámbito. Es un centro muy activo que cuenta con numerosos cursos[26] e informes[27] que han tenido muy buena aceptación en la Comunidad Valenciana.

En general, las distintas experiencias que se han ido implementando en el panorama nacional se orientan hacia:

- Plan de seguridad, gestión de la seguridad en los procesos de la empresa.
- Cultura de seguridad o todo lo relativo a la sensibilización de ciudadanos y empleados, y de cómo prepararlos.
- Protección de la información, copias de seguridad, protección contra la fuga de información, cifrado, borrado seguro, destrucción de soportes, etcétera.
- Puesto de trabajo, para garantizar la seguridad desde cada puesto.
- Movilidad y conexiones inalámbricas o cómo proteger las comunicaciones en un entorno móvil e inalámbrico.
- Contingencia y continuidad de negocio, para estar preparado para recuperar la actividad del negocio en caso de un incidente.
- Cumplimiento legal, fundamentalmente desde el aspecto de protección de datos personales (LOPD) y de la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI).
- Buenas prácticas de los departamentos de informática. Engloba la seguridad en sistemas y redes, la protección ante intrusiones, las auditorías internas y consideraciones de seguridad en desarrollo del *software* y mantenimiento de sistemas.
- Fraude y gestión de identidad, cómo detectarlo y evitarlo, concienciación sobre técnicas de ingeniería social, timos más frecuentes, etcétera.
- Contratación de servicios, es decir, los aspectos que el empresario ha de considerar cuando contrata servicios en internet o externaliza parte de su actividad.

Otras iniciativas diferentes han sido las que, durante años, han desarrollado la Policía Nacional y la Guardia Civil, tratando de concienciar a los niños en los colegios sobre los peligros que encierra la red.

Por su parte, el Mando Conjunto de Ciberdefensa tiene como misión, entre otros, el definir, dirigir y coordinar la concienciación, la formación y el adiestramiento especializado en materia de ciberdefensa del propio Ministerio de Defensa. En base a ese cometido ha coordinado y puesto en marcha, como veremos posteriormente, el Plan de Concienciación en Ciberdefensa

[26] https://www.csirtcv.gva.es/es/paginas/formación.html
[27] https://www.csirtcv.gva.es/es/paginas/descargas-informes-csirt-cv.html

(CONCIBE) y ha explorado interesantes programas dirigidos a su ámbito de actuación y basados en cursos de sensibilización en la plataforma e-learning del MINISDEF, que incluso incorporan técnicas de *gamificación* orientadas a mejorar los resultados prácticos.

Según Hairol Romero Sandí y Elvin Rojas Ramírez, en su trabajo sobre «La gamificación como participante en el desarrollo del B-learning»[28] definen la *gamificación* como una técnica de aprendizaje basado en las mecánicas y dinámicas de juego para alentar o motivarlo, colaborando en la construcción de nuevas experiencias convirtiendo algunas actividades consideradas aburridas en innovadoras e interesantes para los participantes.

En el ámbito privado hay muchas iniciativas lideradas por las diferentes compañías especializadas en ciberseguridad para implementar planes de concienciación en sus clientes. En general, se han ido diseñando planes de concienciación basados tanto en culturas de procesos con la transmisión de políticas y buenas prácticas a los empleados, como en culturas de *compliance* para el cumplimiento de normativas o legislaciones. Así, se han puesto en práctica numerosas iniciativas basadas en el bombardeo continúo de mensajes relacionados con las políticas o buenas prácticas o con las normativas a cumplir, con un impacto generalmente bajo.

No se ha tenido en cuenta, por lo general, que la cultura de seguridad de una compañía y, por tanto, cómo se comporta la misma en términos de seguridad, está fuertemente ligada a las creencias, valores y asunciones de los empleados o personas que la conforman.

Un cambio cultural para adaptar la cultura de seguridad de una organización a las realidades actuales de la ciberseguridad supone una labor increíblemente dura a menos que se empiece desde cero. Normalmente las organizaciones tienen ya establecida su cultura de seguridad e incluso los individuos aportan ya una cultura de ciberseguridad preestablecida.

Hasta principios de 2013, los equipos de IT trataban de imponer estrategias de seguridad ortodoxas. La creación de estrictas reglas y controles que se esperaba que fueran seguidas por todos los empleados. Por ello, se hacía necesario un fuerte apoyo de la dirección y la comunicación era vital para vencer las objeciones de algunos y para mantener la fuerza de la estrategia.

El mundo de la seguridad (de la información) lleva muchos años trabajando en la gestión de riesgos como eje central de estudio para la protección de la información y las infraestructuras de las organizaciones. Sin embargo, en lo que a la implicación del empleado se refiere, el enfoque suele ser «no toques nada». Con el objetivo de proteger aquello que gestiona, se ha metido durante años al empleado en una burbuja de sobreprotección, lo que se traduce en limitar al máximo sus permisos y su capacidad de acción.

[28] http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP118.pdf

Pero es de sobra conocido que la mejora de la seguridad de las organizaciones, tanto cuando hablamos de la información como de los propios medios físicos, no depende «solo» de la implantación de medidas técnicas de seguridad o la definición de procedimientos; es fundamental la implicación de las personas. No se repite suficiente que el factor humano en un pilar fundamental en la seguridad y, por tanto, es necesario desarrollar técnicas efectivas y eficientes para desarrollar al máximo este potencial. Las últimas experiencias más exitosas van en esta línea.

Así, según el NIST (113)[29], existen diferentes niveles de aprendizaje a la hora de aplicarlos a los diferentes miembros de la empresa según los roles y responsabilidades en ciberseguridad que desempeñan dentro de ella, que son:

Concienciación: es un proceso de aprendizaje destinado a todos los miembros de la empresa y se enfoca en cambiar las actitudes individuales y colectivas para comprender la importancia de la seguridad y las consecuencias adversas de su fracaso.

Su objetivo es que los empleados reconozcan y retengan la información que se les proporciona.

Ejemplos de canales para proporcionar este aprendizaje son los folletos, pósteres, videos, comunicados por *email*, *banners*, etcétera. Se busca alcanzar un impacto en un corto espacio de tiempo.

Formación: es un proceso que se centra en trasladar a los empleados de la empresa los conocimientos y habilidades que les permitan realizar su trabajo con mayor eficacia. Se centra en dar a conocer y hacer que se dominen las habilidades necesarias para desempeñar adecuadamente un rol determinado. Ejemplos de canales para proporcionar este aprendizaje son los cursos, las prácticas, las demostraciones, los talleres, etcétera. Se busca alcanzar un impacto temporal a medio plazo.

Educación: es el proceso de formación en ciberseguridad más avanzado y se centra en el desarrollo de la capacidad y la visión para llevar a cabo actividades complejas y multidisciplinares, así como las habilidades necesarias para promover el desarrollo profesional en ciberseguridad. Se centra en hacer que se desarrolle un entendimiento profundo y la capacidad de gestionar el conocimiento en la materia. Las actividades para proporcionar este tipo de aprendizaje incluyen la investigación y desarrollo, los seminarios y grupos de trabajo, los cursos monográficos avanzados, etcétera. Se busca alcanzar un impacto temporal a largo plazo.

Según *ENISA*[30], los programas de concienciación se deben desarrollar en tres fases: planificar, estimar y diseñar. Los programas de formación y concienciación deben ser diseñados teniendo siempre en cuenta la misión,

[29] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf
[30] http://www.enisa.es/

visión y objetivos de cada empresa. Es muy importante que apoyen las necesidades de negocio y que influyan en la cultura de la empresa y, también, en las arquitecturas que soportan sus servicios TI. Los programas más exitosos son aquellos en los que los usuarios consideran que son relevantes para los problemas que se tratan de resolver. En esta etapa se identifican las necesidades de formación y concienciación, se diseña un plan eficaz que cubra dichas necesidades, se busca y se asegura la disponibilidad de los servicios de formación necesarios y se establecen las prioridades para llevarlas a cabo.

Desarrollar y gestionar: en esta fase se incluye cualquier actividad necesaria para implementar el programa de formación y concienciación sobre ciberseguridad. Las acciones del programa, que ejecuta la estrategia establecida para cubrir las necesidades de formación identificadas, solo se podrán gestionar y llevar a cabo una vez haya sido desarrollado el correspondiente material formativo.

Evaluar y ajustar: los mecanismos de evaluación y de retroalimentación son componentes críticos para cualquier programa de concienciación sobre la ciberseguridad. La mejora continua solo se puede alcanzar si podemos conocer cómo está funcionando el programa actual. Es particularmente importante, a nuestro modo de ver, desarrollar sistemas de medición que sean lo más realistas posible, es decir, que nos permitan medir claramente el riesgo que introduce el factor humano. Una vez que se han alcanzado los requisitos iniciales básicos de concienciación, se puede diseñar y empezar a aplicar una estrategia de mejora continua.

Todos los referenciales se hacen eco de la necesidad de considerar el factor humano como un componente esencial de la seguridad.

No obstante, además de todo esto, lo que está claro es que el comportamiento de la organización ante las ciberamenazas depende esencialmente de la cultura de seguridad de la organización. Si queremos cambiar el comportamiento ante ellas, esencialmente, estamos ante un problema de cambio cultural.

De forma general, las culturas de ciberseguridad que nos podemos encontrar en las organizaciones se pueden agrupar bajo cuatro paradigmas diferentes, que, en diferentes momentos, cuentan con aspectos que son beneficiosos para nuestra cultura de seguridad:

- Cultura de Procesos, donde todo es formal y burocrático, el valor central es el control y se crean numerosas políticas y procedimientos formales.
- Cultura de *Compliance*, donde las preocupaciones frente a la legislación vigente establecen las prioridades.
- Cultura de Confianza, en el que trasladamos al empleado los conocimientos y las herramientas adecuadas para gestionar los riesgos a los que, inexorablemente, se tiene que enfrentar.

– Cultura de Autonomía, en el que se fomenta la capacidad de reacción. Es esencial cuando se está materializando un ataque.

A pesar del mencionado plan nacional y de los muchos proyectos de los diferentes organismos, todavía no se ve una acción concertada a nivel global en marcha, probablemente debido a la falta de recursos derivados del momento económico que hemos vivido todos estos años.

Dentro del sector privado

Después de algunos años tratando de implementar estrategias de concienciación corporativas, podríamos decir que nos hemos olvidado de que lo que tenemos que formar y concienciar es a las personas, y por tanto los programas deben ir enfocados a concienciar a las personas para que desarrollen todas sus actividades, tanto en su vida privada como en la profesional, con un nivel adecuado de seguridad. Es decir, se debe fomentar en las personas una cultura de gestión del riesgo adecuada y proporcionarles las herramientas necesarias para realizar estas tareas.

Esta falta de conocimientos y cultura de seguridad no pasa desapercibida para los ciberdelincuentes que aprovechan descuidos, prácticas inseguras de comportamiento y, en general, la falta de formación en materia de seguridad por parte de los empleados para poner en riesgo la seguridad de cualquier organización.

Aunque, en teoría, un modelo basado en impedir al usuario realizar operaciones suena francamente bien, la realidad es que el empleado, nos guste o no, tiene que tocar cosas. Dicho de otra forma, la práctica nos ha demostrado que las paredes de la burbuja en la que intentamos meter al empleado son muy delgadas y este se enfrenta de manera continua a situaciones de riesgo sin tener la información, los conocimientos y las herramientas necesarias para protegerse.

Ante esta situación, no se puede seguir reforzando el papel de la tecnología y los procesos, manteniendo al mínimo imprescindible el de las personas ya que los sistemas de protección y los procedimientos no son infalibles. Hay que apostar, necesariamente, por fortalecer también las capacidades defensivas de las personas en busca de una posición de equilibro y solidez sobre la que implantar una gestión eficaz de la seguridad.

Para conseguir este objetivo es necesario abordar el problema desde su origen, convirtiendo al empleado en parte de la defensa: *human firewall*[31]. De esta forma, el empleado juega un papel activo y relevante en la gestión de la información que maneja, lo que da lugar a una estrategia de seguridad mucho más robusta.

[31] Término acuñado por S2 Grupo en sus sesiones de concienciación.

El primer paso es capacitar al empleado por medio de acciones continuadas de concienciación, formación y prueba en entornos de simulación.

Mediante la concienciación se involucra e implica al empleado en la protección de las tecnologías e información que gestiona, a través del conocimiento y aplicación de las normativas, procedimientos y buenas prácticas en seguridad. Para conseguirlo hay que mostrar al empleado las amenazas a las que se enfrenta y su posible impacto, haciéndole entender por qué debe realizar una gestión adecuada de la seguridad.

A través de la formación se traslada a la persona el conocimiento necesario para llevar a la práctica una gestión adecuada de la seguridad. Se le forma en cómo hacerlo, dotándole de los conocimientos y herramientas necesarias.

Por último, con el objetivo de mantener actualizados los conocimientos adquiridos dentro de un ciclo de mejora continua, se pone al empleado a prueba mediante ciberejercicios en entornos de simulación.

Una vez capacitado es cuando se puede dotar al empleado de la responsabilidad en la gestión de la seguridad de la información y los medios digitales que maneja, teniendo en cuenta las particularidades de los distintos colectivos que componen una organización, convirtiéndoles en parte activa de la estrategia de defensa.

La creación de una cultura de confianza digital que permita reforzar la protección de los organismos y estimule la implicación de los ciudadanos en el entorno digital, resulta vital para impulsar el pleno desarrollo de la sociedad conectada; para lo cual, el sector de la ciberseguridad se configura como un elemento habilitador clave.

Es esencial, por tanto, promover esta cultura de seguridad en las organizaciones que enfatice todos los aspectos que son esenciales en la gestión de la misma.

La seguridad centrada en las personas es una aproximación estratégica que enfatiza la responsabilidad y la confianza y desenfatiza el control restrictivo y preventivo de la seguridad.

Hay diferentes estadios o niveles en los que hay que avanzar hasta llegar a una cultura de ciberseguridad totalmente centrada en las personas para que el riesgo sea bajo.

Un primer nivel de madurez que podríamos llamar instintivo. En este nivel el riesgo es alto, los comportamientos se memorizan y transmiten informalmente entre empleados y no están documentadas las políticas. Las emociones individuales son los principales criterios de decisión, son intuitivas.

A continuación vendría un nivel más consciente de la necesidad de avanzar en mejorar la cultura de ciberseguridad. Es un nivel de conciencia. En él existe la necesidad de analizar, identificar y cambiar aquellos comportamien-

tos que pueden comportar un riesgo para la organización. Se establecen los primeros intentos para formalizar y estimular comportamientos deseados. Se determinan las políticas y se empiezan a llevar a cabo entrenamientos/formaciones.

Mucho más avanzado, y por ello el factor humano comporta en esta situación un riesgo bastante menor, está el nivel de visibilidad. En este estado los comportamientos y las características culturales se miden y analizan. Se correlacionan los procesos de decisión con los patrones culturales y de comportamiento. Los riesgos culturales que impactan en los objetivos fundamentales son identificados y documentados. Existen ya estrategias formales para bajar el riesgo cultural.

Avanzando en el estado de madurez de la cultura de ciberseguridad subiríamos a un nivel en el que toda la organización está orientada e involucrada en la transformación cultural, es el nivel de conversión. Todos están totalmente orientados, en su conjunto, hacia el esfuerzo global que supone el cambio de los comportamientos y hábitos. La cultura y el comportamiento se miden de forma continua para detectar defectos en los esfuerzos en marcha. Todos los empleados son evaluados y rinden cuentas de las actuaciones culturales.

Por último, un grado de madurez muy alto se corresponde con una conciencia global de la compañía de los diversos ciberriesgos y, por tanto, un grado de riesgo mucho más bajo. La cultura de la organización está formalmente gestionada como un proceso y la medición de todo lo relativo a ella está completamente automatizada. Es el nivel de dominio.

Fuera del entorno laboral

Las estrategias de concienciación pasan, en la práctica, por entender que las personas somos en esencia eso, personas. Todos los planes de concienciación, en general, están orientados a los empleados o a los ciudadanos. No nos damos cuenta que, en realidad, son los mismos. Cualquier persona, en esencia, establece unos parámetros de comportamiento que afectan tanto a su vida personal como a la profesional. En este sentido, es imprescindible hacer que las personas entiendan el problema y adopten unos estándares de comportamiento que mejoren su nivel general de ciberseguridad y, con ello, el de las organizaciones en las que trabajan.

Por otro lado, es necesario que las políticas de seguridad de las organizaciones contemplen que, en realidad, los perímetros de protección hoy en día son completamente difusos y se maneja en muchos casos información corporativa y sensible en equipos que están fuera de ese perímetro, en muchos casos en casa.

La tecnología de los hogares conectados en la actualidad es cada vez más compleja. Las previsiones con el despliegue masivo de *IOT* es que se multi-

pliquen los dispositivos útiles gestionados por cada unidad familiar, llegando incluso según previsiones recientes a tener que manejar cientos de direcciones IP en una red de un hogar avanzado. Las previsiones hablan de 500 IP.

Actualmente, de manera intuitiva y a nivel casero, uno de los miembros de la unidad familiar ejerce labores que ejercería un jefe de la información y un jefe de la seguridad (CIO y CISO), desplegando la tecnología que el hogar necesita y «vigilando» de la forma que puede y sabe la seguridad de su entorno tecnológico. Ese CIO y CISO en funciones no tiene especial formación tecnológica y, si bien puede ser un usuario de la tecnología, actualmente no tiene suficiente formación o conocimiento para ejercer de responsable de seguridad de su hogar. Muchas veces no sabe realmente a lo que se enfrenta.

Si estas personas, con sus unidades familiares, son ejecutivos de compañías que directa o indirectamente trabajan en entornos sensibles el escenario de riesgo se complica.

Por lo tanto, algunas acciones públicas deben ir encaminadas a fomentar el conocimiento y las herramientas que el CISO de la casa puede utilizar para proteger su entorno. Tener un hogar protegido, sin duda, redunda en fortalecer la seguridad del sistema en su conjunto, puesto que es uno de los eslabones más débiles de toda la cadena de seguridad.

A nivel multinacional

La Autoridad Australiana de Telecomunicaciones y Medios de Información[32] publicó un trabajo sobre las diversas campañas de concienciación hechas en diversos países. De este estudio se dedujeron algunos aspectos que dichas campañas tenían en común, entre los cuales destacamos: las herramientas dominantes en la mayoría de las campañas eran páginas web y publicaciones; los juegos y test eran bastante escasos; la mayoría de las campañas no incluían un servicio de asesoramiento; el patrocinador de las campañas era normalmente el Gobierno, aunque en algunos casos se incluía al sector privado; los temas cubiertos eran muy diversos y no se cubrían todos los aspectos que hubieran sido necesarios; las audiencias objetivo en muchas campañas estaban muy diversificadas; la evaluación sobre el éxito de las campañas era bastante; la difusión de folletos, *websites* y otros medios pasivos tienen un impacto limitado si no vienen seguidas de prácticas, y los mensajes difundidos vía televisión han demostrado ser muy efectivos.

Dentro del marco de la OTAN, esta ha desarrollado un Programa de Implementación de Concienciación en Ciberdefensa. Dicho programa está basado en tres principios: la coherencia de los mensajes, la coordinación entre sus

[32] An overview of international cyber-security awareness raising and educational initiatives. Research report commissioned by the Australian Communications and Media Authority, May 2011.

agencias y la sostenibilidad del mismo. Incluye una serie de actividades, incluyendo el *branding* (creación de una imagen corporativa, en este caso para ciberseguridad), objetivos, medidas de los efectos y normas de gobernanza del programa. Dentro de estas actividades el Centro de Excelencia en Ciberdefensa (CCD COE) de Tallin (Estonia) ha lanzado un curso *online* orientado a los usuarios de las redes OTAN y cuya finalidad es ayudarles a familiarizarse con la terminología, los tipos de ciberataque y las técnicas defensivas.

Dentro de la Unión Europea ya hemos visto cómo la propia estrategia contempla la concienciación como un factor necesario a contribuir a la resiliencia. *ENISA* ha desarrollado varios estudios y materiales en este sentido y los ha puesto a disposición de las naciones miembro. Una de estas actividades es el Mes de la Ciberseguridad.

Una iniciativa muy interesante es el acuerdo firmado recientemente por los ministros de Defensa de Letonia, Lituania, Estonia, Holanda, Finlandia, Austria y la Unión Europea[33]. Este documento supone un «compromiso para mitigar los riesgos en el ciberespacio debidos al factor humano mediante una iniciativa en ciberhigiene». Esta iniciativa está abierta a todos los Estados miembros e instituciones de la Unión Europea. Los que se adhieran a ella se comprometen a adoptar unas buenas prácticas y se implementará una plataforma de *e-learning*. Como resultado ya se ha publicado una guía en ciberhigiene[34] dirigida por un grupo de expertos de la Universidad de Tallin y el ministerio letón de Defensa, aunque han contribuido otros expertos.

En este documento se categoriza al personal en grupos (usuarios, directivos y especialistas IT) y los comportamientos que dan origen a ciberincidentes (negligencia, intenciones maliciosas, falta concienciación, falta conocimiento sobre la organización). No todos los comportamientos son aplicables a todos los usuarios

En la Estrategia Internacional para el Ciberespacio de los Estados Unidos[35], y dada la globalidad de este dominio, esta nación asume como finalidad el ayudar a otros Estados para, entre otras acciones, desarrollar e implementar programas dirigidos a elevar el nivel de concienciación y construir así una cultura de ciberseguridad.

Como parte de la ciberdefensa

No existe una definición acordada sobre el término ciberdefensa, pero parece estar claro que entre sus objetivos fundamentales se encuentra la pro-

[33] Pledge of the Cyber Higiene Initiative.

[34] Guidelines for Responsible IT-related Practices in Modern Organizations (Cyber Hygiene).

[35] International, Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World. May 2011.

tección de las redes y sistemas TIC de los departamentos o ministerios de defensa de las naciones, y que es responsabilidad fundamentalmente de las Fuerzas Armadas.

Puesto que los programas de concienciación deben ser diseñados teniendo siempre presente la misión de la organización y teniendo en cuenta la cultura o idiosincrasia de la misma, la concienciación en ciberdefensa podría ser considerada como un caso particular, si tenemos en cuenta primeramente las misiones de las Fuerzas Armadas (FAS) y consideramos otros factores como: la sensibilidad de la información procesada en las TIC de los ministerios de defensa, la debida seguridad de las operaciones militares (OPSEC) y la dispersión geográfica de las unidades y la movilidad del personal, sometido a frecuentes cambios de destino.

Es necesario definir unos programas diferenciados de los que pueda tener otro organismo nacional o una empresa. La diferencia fundamental se centraría en unos contenidos adicionales destinados a sensibilizar al personal sobre los riesgos que para las operaciones militares pueden tener unas malas prácticas en el ciberespacio. Así, por ejemplo, el militar debe ser muy precavido con los contenidos (fotos, comentarios, etcétera) que cuelga en las redes sociales, puesto que puede dar claves al adversario sobre equipamiento, localización de unidades, movimiento de fuerzas, estado de moral, etcétera.

Otra particularidad debe ser la derivada de la dispersión (despliegues en zonas de operaciones, dispersión de unidades, etcétera) que obligará a contemplar métodos de difusión de mensajes de concienciación que permitan llegar a todo el personal. Un ejemplo sería el uso de aplicaciones para dispositivos móviles (apps).

Finalmente, muy importante, hacer llegar los mensajes a las personas que conforman el entorno personal cercano de los profesionales de las Fuerzas Armadas. Los adversarios pueden utilizar técnicas de ingeniería social para, a través de amigos o familiares, hacerles llegar un *software* malicioso.

En este sentido y como ya habíamos avanzado, desde su creación por la Orden Ministerial 10/2013[36], y en desarrollos sucesivos de la estructura de las Fuerzas Armadas, se ha asignado al Mando Conjunto de Ciberdefensa (MCCD) el cometido de definir, dirigir y coordinar la concienciación en materia de ciberdefensa. El MCCD, en coordinación con los distintos ámbitos del Ministerio de Defensa elaboró un Plan de Concienciación en Ciberdefensa (CONCIBE) que fue aprobado por el jefe del Estado Mayor de la Defensa en diciembre de 2015.

[36] Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

El CONCIBE determina unas audiencias objetivo, niveles a alcanzar, acciones a realizar, recursos, prioridades, cronograma y responsabilidades. Una de las particularidades de este Plan con respecto a otros programas de concienciación es que en la audiencia objetivo se incluye personal que no es usuario de las TIC del Ministerio de Defensa, pero que pertenece a él. No todos los puestos de trabajo de las Fuerzas Armadas acceden a las TIC, sin embargo es muy raro encontrar personal que no tenga un ordenador personal o dispositivo móvil. Incluyendo a este personal, se está reconociendo que el comportamiento privado entraña riesgos cuando se interactúa en el ciberespacio. También y por las razones que hemos expuesto anteriormente, es objeto del CONCIBE el entorno cercano de los militares, como pueden ser familiares o amigos próximos, lo cual no solo contribuye de manera indirecta a la seguridad de las operaciones, sino que además se contribuye al esfuerzo de concienciación de todos los ciudadanos previsto a nivel nacional.

Este Plan está en ejecución desde su aprobación a finales de 2015 y se han desarrollado acciones que han involucrado a diversas unidades y organismos de las Fuerzas Armadas, habiéndose incluso contratado algunos productos a empresas privadas. El CONCIBE contempla unas métricas que deben ayudar en un futuro próximo a hacer una revisión del propio Plan.

Otro ejemplo de plan específico en el ámbito de la defensa es la Iniciativa de Cultura y Cumplimiento de Ciberseguridad (CD3I)[37] del Departamento de Defensa (*DoD*) de los Estados Unidos. Liderada por el Mando Estratégico (USSTRATCOM) y el Mando Cibernético (USCYBERCOM), establece de manera clara la responsabilidad individual de los usuarios y operadores de proteger las redes del *DoD*, así como la de los jefes de unidad de impulsar la cultura de ciberseguridad.

Esta iniciativa establece una serie de principios directores de comportamiento individual (integridad, adecuado nivel de conocimientos, correcta aplicación de los procedimientos, respaldo, y actitud inquisitiva ante los incidentes) y agrupa a los usuarios en cuatro niveles (usuarios, directivos, especialistas IT y ciberguerreros). También especifica que debe haber un sistema de inspecciones, un sistema de comunicación y unos recursos para llevarla a cabo y afirma de manera contundente que «la ciberseguridad debe convertirse en una parte integral de las operaciones, de la misma manera que lo es un esquema de maniobra».

Programas, planes, campañas de concienciación

Aparte de las campañas o planes que ya hemos analizado, existe mucha información y documentación disponible en internet para servir a ayudar a

[37] The DoD Cybersecurity Culture and Compliance Initiative.

definir programas, planes o campañas de concienciación. Vamos a repasar algunos que nos han parecido interesantes.

Entre ellas, de gran valor es la Guía sobre Programas de Formación y Concienciación en ciberseguridad del Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST)[38]. Merece la pena analizar un poco este documento ya que es una completísima guía que no solo sirve para los programas de concienciación, sino también para formación. Esta guía define responsabilidades dentro de una empresa y los pasos críticos a dar para acometer una tarea de concienciación: diseño de un programa, la preparación del material, la implementación del programa y el seguimiento del mismo.

Dentro del diseño del programa, primero especifica acciones a seguir para estructurar la actividad, desarrollar un análisis de necesidades, desarrollar el plan de concienciación, establecer prioridades y definir un nivel a alcanzar. Estructurar la actividad es crítico y propone tres posibles modelos partiendo de la base de que siempre debe existir una autoridad central en formación y concienciación: centralizado, en el que la política, la estrategia a seguir y la implementación son dirigidas por una entidad central; parcialmente distribuido, de manera que la política y la estrategia a seguir están centralizadas y la implementación descentralizada; solo la definición de la política a seguir queda centralizada. La elección de un modelo u otro estará basado en consideraciones como el presupuesto, la organización, el tamaño de la misma y su dispersión geográfica.

La guía también expone cómo hacer métricas de concienciación, cómo puede ser el porcentaje de usuarios que han participado en sesiones de concienciación, los ciberincidentes que sufre la organización a causa del usuario o entrevistas con el personal responsable.

Dado que los recursos siempre serán limitados, será necesario establecer unas prioridades para difundir mensajes. Estas prioridades vendrán dadas fundamentalmente por el nivel de exposición a ciberataques a la que puede estar sometida una parte de la audiencia de adiestramiento.

En cuanto al desarrollo del material de concienciación, el documento propone varias opciones: desarrollado por la propia organización; utilizar alguno desarrollado por alguna organización profesional o contratar a una empresa especializada. También dependerá de la misión y capacidad de la organización definirse por un medio u otro. *A priori* da la impresión que solo las grandes organizaciones pueden ser capaces de desarrollar sus propios materiales.

Con respecto a los temas a incluir en las campañas, el NIST 800-50 propone, por ejemplo: uso y gestión de contraseñas, incluyendo su creación, frecuen-

[38] NIST Special Publication 800-50, «Building an Information Technology Security Awareness and Training Program».

cia de cambios y protección; protección contra código malicioso; políticas; correos electrónicos; seguridad en la web; copia de seguridad de los datos; ingeniería social; *shoulder surfing*; responsabilidades de los usuarios, etcétera.

Otros documentos de utilidad para la redacción de un plan de concienciación son la Guía Suplementaria de Recursos del Modelo de Ciberresiliencia[39] y la Guía de Autoevaluación de Ciberresiliencia[40], ambos derivados del ya mencionado CERT-RMM.

En la primera guía se deja claro que las organizaciones deben dedicar recursos a la concienciación como son: instalaciones, personal, materiales de concienciación, etcétera. También tienen la opción de contratar la concienciación a proveedores ajenos. Ahora bien, en este caso hay que hacer un esfuerzo para definir bien las necesidades de la organización y hacer que el proyecto responda a las mismas. Por otra parte, habrá una parte relacionada con los procedimientos propios de la organización que difícilmente podrá ser subcontratada.

Con respecto la guía de autoevaluación, esta es muy interesante ya que se establecen una serie de aspectos que sirven para evaluar, en general, el nivel de madurez de la resiliencia de una organización. Uno de esos aspectos es la concienciación y en ese particular se pueden sintetizar en dos: que exista un programa dentro de la organización y que este se esté ejecutando.

Por otra parte, el Consejo de Estándares de Seguridad de Tarjetas de Pago (PCI SCC), que es un foro responsable del desarrollo, educación y concienciación de los estándares para incrementar la seguridad de los pagos electrónicos, hace algunas propuestas interesantes en materia de concienciación en ciberseguridad[41]. Entre ellas destacamos: la necesidad de crear un equipo para concienciación compuesto de personal con diversos perfiles; definir el mínimo nivel de conocimientos a alcanzar por todo el personal de la organización; incluir diversos modos de difundir los conocimientos, como pueden ser la formación clásica, aprendizaje basado en el ordenador, *emails*, circulares, boletines; difundir los materiales adecuados en los momentos oportunos y de manera eficiente; ajustarse a la idiosincrasia de la organización y definir unas métricas que sirvan para medir el éxito de las campañas.

Asimismo el Instituto SANS en noviembre de 2015 llevó a cabo una encuesta[42] sobre este tema. Este estudio ha puesto en relieve dos hechos clave: en general los equipos de concienciación no tienen el apoyo, tiempo y recursos

[39] Carnegie Mellon University, Cyber Resilience Review (CRR) Supplemental Resource Guide, volume 9,Training and Awareness,Version 1.1.

[40] Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide February 2016.

[41] PCI Security Standards Council. Best Practices for Implementing a Security Awareness Program, October 2014.

[42] SANS, Awareness is hard: a tale of two challenges, 2016.

que necesitarían para tener éxito; y segundo, los equipos de concienciación suelen tener buenas habilidades técnicas pero les suelen faltar habilidades de comunicación interpersonales.

Basados en las propuestas del PCI SCC y SANS podemos llegar a la conclusión de que los equipos de concienciación ideales deberían estar compuestos por un buen comunicador y un buen técnico. El primero para hacer llegar los mensajes clave y el segundo para apoyarle y poder realizar demostraciones técnicas que tengan el impacto necesario.

En la misma línea y según Kaspersky hay empresas que gastan millones en campañas de concienciación pero realmente pocos responsables de la seguridad de las TIC (CISO) están contentos con los resultados. El motivo aparentemente es que la mayor parte de los programas llevan mucho tiempo, son muy técnicos y esencialmente basados en mensajes negativos. Por tanto, propone aproximarse al problema con una visión más sofisticada con técnicas de *gamificación*, ataques simulados e instrucción interactiva en profundidad de las destrezas en ciberseguridad[43].

Cooperación público-privada para la concienciación en ciberseguridad

A la vista de todo lo comentado hasta el momento podemos ver que definir un plan de concienciación para una organización o empresa nunca es sencillo, pues aunque existen guías disponibles y muchas experiencias y buenas prácticas, en muchos casos lo verdaderamente difícil para acometer con éxito y garantías un proyecto de concienciación reside en el cambio cultural que es necesario realizar. Asimismo, es necesario dedicar recursos materiales, humanos y financieros, y para ello hay que convencer de la necesidad a la dirección de las organizaciones.

La tarea se complica aún más si la concienciación la queremos llevar a un ámbito superior, como es el nacional. En este caso la audiencia objetivo es muy amplia: afecta a todos los ciudadanos de la nación. Sin duda, para la consecución de un objetivo de esta naturaleza la Administración debe jugar un papel clave a la hora de dinamizar este trabajo, aportando los recursos necesarios. Sin embargo, los organismos públicos con responsabilidades en la materia son diversos, cada uno con diferente organización, responsabilidades y recursos.

Teniendo en cuenta que el concienciar a los ciudadanos redunda en beneficio de ambos, nación y empresas, quizá la solución esté en abordar este tema de una manera global mediante la creación de una asociación de cooperación entre ambos sectores [*Public-Private-Partenership* (*PPP*)]. *ENISA* ha estudia-

[43] Kaspersky. Cybersecurity Awareness Brochure.

do cómo articular una *PPP*[44] en ciberseguridad y ofrece algunas recomendaciones que pueden ser de utilidad y que pasamos a analizar.

Participar en una *PPP* trae beneficios para ambos sectores. El Gobierno de la nación cumple con lo expresado en la ECSN relativo a la mejora de la resiliencia, que a su vez es un mandato expresado en la Estrategia de Ciberseguridad de la Unión Europea, que indica que «para impulsar la ciberresiliencia en la Unión Europea, tanto las Adminstraciones Públicas como el sector privado deben desarrollar capacidades y cooperar efectivamente».

Para los socios del sector privado el pertenecer a una asociación de este tipo les reporta también otros beneficios. Entre ellos se pueden destacar los siguientes: acceso a información privilegiada y especializada, acceso al conocimiento no disponible en ningún sitio más, oportunidad de contribuir a una dirección estratégica y a políticas nacionales, y la posibilidad de intercambiar lecciones aprendidas, buenas prácticas y ver distintos puntos de vista sobre cómo afrontar el problema.

Pero si hay un beneficio importante para que una empresa participe en un *PPP* este es el prestigio que supone participar en una iniciativa de estas dimensiones. Para otras compañías el prestigio viene dado por la confiabilidad que ofrecen a sus clientes de que sus transacciones electrónicas y privacidad quedan protegidas por su compromiso con la ciberseguridad.

Una *PPP*, según *ENISA*, queda definida como una relación organizada entre organizaciones públicas y privadas, en la que se establece un ámbito y objetivos en común y define unos cometidos y metodología de trabajo para alcanzar la finalidad compartida.

Esta definición es muy interesante pues supone que una asociación de este tipo no debe ser una entelequia, un simple deseo político de armonía entre ambos sectores. Una *PPP* debe estar perfectamente estructurada y definida y por supuesto esta asociación debe ir más allá de la mera contratación de servicios a empresas. Debe suponer una aportación común de esfuerzos a un fin común que redunde en beneficio de todos los participantes en ella.

En primer lugar, debe existir un organismo de coordinación o regulador. Dicho organismo puede ser el que impulse la iniciativa y, en general, debe ser visto como un socio más en disposición de apoyar. En ningún caso debe dar la impresión de que se establece una relación de mando y subordinación entre los asociados en la *PPP*. A esta *PPP* en este documento nos referiremos también como consorcio o asociación.

Es fundamental definir con claridad las relaciones entre miembros de la asociación y los procesos que se van a desarrollar en el marco de la asociación y entre esta y el exterior. Entre ellos es vital la definición de la gobernanza

[44] Cooperative Models for Effective Public Private Partnerships food Practice Guide.

de la *PPP,* así como una clara definición de los cometidos a desempeñar por cada socio participante.

Es importante animar a los socios a compartir información y a que tengan en cuenta la información que reciben. Como mecanismos de relación dentro del grupo, estos deben quedar claramente establecidos en los estatutos y deberían basarse en reuniones regulares presenciales, reuniones por videoconferencia, difusión electrónica (*email*, portales web, etcétera) o una combinación de todas ellas.

Habrá también que definir el tipo de asociación que se quiere crear teniendo en cuenta la misión y que puede ser de varios tipos: comunidades a largo plazo, cuya razón fundamental es el intercambio de información; grupos de trabajo, son aquellos que se constituyen con un fin muy concreto; grupos de repuesta rápida, se constituyen por un corto periodo de tiempo y para ocuparse de algún asunto urgente; o grupo de actividad combinada, es una comunidad a largo plazo que puede reunirse para planear y practicar estrategias y, si hay una emergencia, un pequeño comité constituye un grupo de respuesta rápida o equipo de trabajo.

Este tipo de asociación debe canalizar la inversión pública necesaria en esta materia. El punto de partida para que se pueda dar una cooperación público-privada efectiva es la necesidad de orientar la inversión para conseguir una serie de objetivos. En este sentido en la *PPP* estarán representados todos los estamentos implicados en la resolución de estos problemas: Administración, empresas y ciudadanos.

De cualquier manera, al definir una asociación de este tipo, será fundamental considerar el marco legal. En el caso español este es la Ley 40/2015 que regula el régimen jurídico del sector público. En dicha ley se definen los convenios como aquellos «acuerdos con efectos jurídicos adoptados por las Adminstraciones Públicas, los organismos públicos y entidades de derecho público vinculados o dependientes o las universidades públicas entre sí o con sujetos de derecho privado para un fin común» (artículo 47, apartado 1, de la Ley 40/2015). Esta definición incluye tanto los convenios interadministrativos (artículo 6 de la Ley 30/1992) como los convenios suscritos entre Adminstraciones Públicas y particulares.

En dicha ley se establecen los requisitos para la celebración de convenios. Por ser de especial aplicación a la definición de una *PPP* destacamos los siguientes: «La suscripción de convenios deberá mejorar la eficiencia de la gestión pública, facilitar la utilización conjunta de medios y servicios públicos, contribuir a la realización de actividades de utilidad pública y cumplir con la legislación de estabilidad presupuestaria y sostenibilidad financiera. Los convenios que incluyan compromisos financieros deberán ser financieramente sostenibles, debiendo quienes los suscriban tener capacidad para financiar los asumidos durante la vigencia del convenio, y las aportaciones financieras que se comprometan a realizar los firmantes no podrán ser superiores a los gastos derivados de la ejecución del convenio».

En cuanto al contenido mínimo de un convenio, la Ley 40/2015 expresa que este será el siguiente: «a) Sujetos que suscriben el convenio y la capacidad jurídica con que actúa cada una de las partes. b) La competencia en la que se fundamenta la actuación de la Administración pública, de los organismos públicos y las entidades de derecho público vinculados o dependientes de ella o de las universidades públicas. c) Objeto del convenio y actuaciones a realizar por cada sujeto para su cumplimiento, indicando, en su caso, la titularidad de los resultados obtenidos. d) Obligaciones y compromisos económicos asumidos por cada una de las partes, si los hubiera, indicando su distribución temporal por anualidades y su imputación concreta al presupuesto correspondiente de acuerdo con lo previsto en la legislación presupuestaria. e) Consecuencias aplicables en caso de incumplimiento de las obligaciones y compromisos asumidos por cada una de las partes y, en su caso, los criterios para determinar la posible indemnización por el incumplimiento. f) Mecanismos de seguimiento, vigilancia y control de la ejecución del convenio y de los compromisos adquiridos por los firmantes. Este mecanismo resolverá los problemas de interpretación y cumplimiento que puedan plantearse respecto de los convenios. g) El régimen de modificación del convenio. A falta de regulación expresa la modificación el contenido del convenio requerirá acuerdo unánime de los firmantes. h) Plazo de vigencia del convenio».

Vemos, pues, cómo un convenio puede ser el mecanismo ideal para definir una *PPP*.

Experiencias y buenas prácticas

En junio de 2012, cuarenta y cinco representantes de la Unión Europea y de los Estados Unidos, del sector público y privado, se reunieron en Bruselas para discutir cómo involucrar intermediarios para «elevar la concienciación en ciberseguridad»[45]. Los participantes expusieron algunas ideas y compartieron experiencias y buenas prácticas. Algunas de las conclusiones de dicha reunión son las siguientes:

- Para las empresas el cooperar en campañas de concienciación crea una buena imagen de la marca, generando así buenas oportunidades de negocio. Sin embargo, convencer a los directivos de la importancia de participar en un proyecto de este tipo es una gran dificultad, a pesar de que merece la pena a largo plazo el financiarlo.
- La ciberseguridad supone un reto cultural pues debe ir encaminada a ciertos cambios en el comportamiento de los usuarios.
- Los ciudadanos son conscientes de alguna manera de que hay medios técnicos para protegerse, pero en muchos casos no saben cómo aplicarlos.

[45] Involving Intermediaries in Cyber-security Awareness Raising.

- Es importante no asustar a los usuarios pero sí animarlos a conectarse y estar seguros al mismo tiempo.
- Para concienciar no es necesario dar excesiva información técnica.
- Los mensajes de concienciación deben estar cuidadosamente estudiados para que vayan dirigidos a una audiencia concreta.
- Los usuarios de las TIC más jóvenes puede ser buenos promotores y llegando a ellos se puede llegar a los padres. Cuanto antes comience la educación, mayores serán los efectos en el comportamiento adecuado de los usuarios en el ciberespacio.

Los medios de comunicación social deberían ser considerados como el principal canal para difundir los mensajes clave. Así, por ejemplo, la televisión tiene un papel clave. También debe tenerse en cuenta la popularidad de las redes sociales.

Los participantes en una *PPP* deben estar involucrados en todas las etapas del proceso.

También la OTAN ha definido una Asociación Industria-OTAN en Ciberdefensa (*NATO Industry Cyber Partnership, NCIP*). Este agrupa a distintas entidades de la OTAN, equipos de respuesta ante incidentes de ciberseguridad y un amplio espectro de representantes de las industrias de los países, incluyendo también representantes de las universidades y centros de enseñanza[46].

Un ejemplo concreto

En Estados Unidos se han lanzado algunas iniciativas interesantes en cuanto a concienciación en ciberseguridad, como son: el mes de la concienciación en ciberseguridad, la campaña *Stop. Think. Connect*, el día de la privacidad de los datos (*Data Privacy Day*) y la campaña Re: Cyber para directivos.

En 2001 se fundó la Alianza Nacional de Ciberseguridad (*National Cyber Security Alliance, NCSA*). Fue conformada por un grupo de líderes visionarios de la industria que se dieron cuenta de que no se había hecho lo suficiente para formar al público sobre cómo protegerse en las redes. Desde el principio los principios reguladores incluían que, aunque en algunas esferas los socios miembros podían competir, sin embargo, todos tenían un interés compartido en un internet más seguro y confiable y el éxito final vendría garantizado si trabajaban juntos y próximos al Gobierno, quien también compartía este interés.

Hoy en día la misión de la *NCSA* es educar una sociedad digital de tal manera que puedan utilizar internet de manera segura en la casa, el trabajo y la escuela, protegiendo la tecnología que utilizan las personas, las redes a las que se conectan y los medios compartidos. Sus actividades están financiadas por los miembros asociados y por el Departamento de Seguridad.

[46] http://www.nicp.nato.int/news/index.html

Algunas empresas asociadas a esta inciativa son: ADP, AT & T, Bank of America, Comcast, EMC, ESET, Facebook, Google, Intel, Leidos, McAfee, Microsoft, Symantec, Verizon and VISA.

En el año 2009 la política del ciberespacio del presidente Obama recomendaba que «El Gobierno Federal, en cooperación con educadores e industria, debería conducir un esfuerzo común de concienciación pública en ciberseguiridad y esfuerzo en educación». Como respuesta, en una iniciativa sin precedentes, la *NCSA* junto con el grupo de trabajo Anti Phising trajeron consigo veinticinco empresas y siete agencias gubernamentales para explorar la posibilidad de una campaña nacional de concienciación. El grupo rápidamente tomó la tarea y en los siguientes catorce meses trabajando en estrecha cooperación y por consenso investigó y desarrolló un conjunto de mensajes que deberían estar disponibles y ser usados por todos.

Este es el origen del programa clave desarrollado por la *NCSA* y conocido como *Stop.Think.Connect* (Para. Piensa. Conecta). El trabajo desarrollado ha sido reconocido al proclamar el presidente Obama *Stop. Think.Connect* como la campaña nacional de concienciación durante su anuncio del Mes Nacional de Ciberseguridad en 2010.

Algunos de los beneficios de esta campaña incluyen:

- Más de ciento cincuenta socios firmaron la campaña para utilizar el mensaje de la campaña. Grandes y pequeñas empresas, departamentos de policía e instituciones educativas y del Gobierno entre ellas.
- La campaña se ha expuesto en transportes públicos de importantes ciudades de Estados Unidos como Washington, Boston y Chicago.
- Se han desarrollado pequeñas campañas en torno a mensajes clave de la campaña.
- Muchas empresas lo han utilizado para demostrar al público su política interna de seguridad en las redes.
- Mucho material ha sido desarrollado para escuelas.

Aunque esta campaña inicialmente solo iba dirigida a los Estados Unidos, esta campaña creció internacionalmente y se ha expandido hacia otras organizaciones regionales e incluso otros países.

Conclusiones

La concienciación en ciberseguridad es una actividad permanente que debe empezar desde las etapas iniciales de la enseñanza y que debe alcanzar a todos los ciudadanos. Sin duda, supone un claro beneficio para el individuo y su ámbito laboral, lo que redunda finalmente en una nación más resiliente en el ciberespacio.

El Gobierno de España a través del Plan de Cultura de Ciberseguridad, Concienciación, Sensibilización y Educación intenta que se alcance el objetivo

último de garantizar la resiliencia nacional en la primera etapa del proceso. Y esto lo hace involucrando a los diversos actores del sector público.

Sin embargo, las dimensiones de dicho proyecto son muy amplias y echamos de menos a empresas y organizaciones que también pueden participar y cuya contribución es significativa. Esta cooperación público-privada no debería ser una simple postura política o declaración de intenciones. Debería ir más allá utilizando el marco legal disponible, mediante la celebración en un convenio que diera cabida a diversos actores del sector público como del sector privado, que oriente la necesaria inversión por parte del sector público.

A nadie se le escapa la dificultad de la creación de un ente de estas características. En primer lugar para la Administración dedicar recursos especialistas con experiencia en diversas materias (comunicación pública, ciberseguridad, asesores legales, etcétera). En segundo lugar, el llegar a un acuerdo y materializarlo. Finalmente, destinar la inversión necesaria para tener éxito en esta tarea.

A pesar del esfuerzo a realizar, creemos que a nadie se le escapan tampoco los beneficios a largo plazo. Un ejemplo en esta línea es la fórmula seguida por la Unión Europea para enfocar la inversión en I+D+i que se va a realizar en el marco del Horizonte 2020. Se han definido diversas *PPP*; en particular en el ámbito de la ciberseguridad, con el objeto de canalizar la inversión hacia los intereses y necesidades de los sectores productivos.

En cualquier caso, no basta con que el individuo esté concienciado en ciberseguridad. Hay que conseguir que la persona tenga un compromiso real con su empresa y con su nación. Para ello, a nivel laboral, las empresas y organizaciones deben ofrecer a los trabajadores un plan de vida, una seguridad, un sentimiento de grupo, en algunos casos un ideal, y proporcionar una serie de valores añadidos que vayan más allá del estímulo económico directo. A nivel nacional es importante hacer saber al ciudadano que con su ciberseguridad personal contribuye a la de la nación.

En definitiva, para tener éxito y mejorar nuestra cultura global de ciberseguridad hay que (1) pensar que trabajamos con personas (2), disponer del apoyo institucional y los recursos para desarrollar todos los planes que son necesarios y alinearlos con los intereses del Estado y (3) Aglutinar en una *PPP* a todos los interesados (empresas, Administración, empresas de ciberseguridad) para definir las líneas de trabajo más apropiadas para garantizar el éxito.