ESTUDIO SOBRE LAS NECESIDADES DE CERTIFICACIÓN Y ACREDITACIÓN EN MATERIA DE CIBERSEGURIDAD

Madrid, Noviembre 2013

Fundación Empresa, Seguridad y Sociedad
www.fundacionesys.com

ÍNDICE

1. OBJETO DEL ESTUDIO

Las Tecnologías de la Información y la Comunicación, en adelante TIC, están inmersas en todo tipo de actividades de la sociedad actual.

Ya no se trata únicamente de actividades relacionadas con la tecnología, sino que realmente afecta a la vida de los ciudadanos en prácticamente todas sus actividades.

El comercio, los viajes, la atención sanitaria, la educación, los servicios de energía, la telefonía, la justicia, la atención de cualquier tipo desde el Estado, la interrelación con los demás…, es muy difícil encontrar alguna actividad que no dependa en mayor o menor manera de un proceso relacionado con la Informática o las Comunicaciones. En algún lugar hay un proceso informático que determina si el pago que estamos haciendo es correcto en una gasolinera o si hay que rellenar una estantería de café soluble en un supermercado, o si hay plazas en un avión, o si hay que poner en marcha una central térmica para atender una demanda de energía.

La implantación de tecnologías que han afectado a la sociedad tiene importantes hitos: el vapor, la electricidad,… pero la actual dependencia de las TIC parece la influencia mayor de la historia.

Por otra parte las TIC tienen otras características como "oleada" tecnológica diferencial de las anteriores:

- **Su evolución es muy rápida**, cada pocos años surgen aplicaciones de estas tecnologías que realmente afectan fuertemente a la sociedad: la telefonía móvil, internet, las redes sociales, el "internet de las cosas", etc. Cada uno de estos avances se ha extendido a grandísima velocidad y ha afectado a la sociedad, a las relaciones humanas, a la forma de hacer negocios,…

- Esta tecnología **presenta una gran complejidad**, es decir, muchos "grados de libertad" en su diseño, lo que unido a la necesaria urgencia en la "puesta en el

mercado", ha llevado a que se acepte como natural que gran parte de sus productos lleguen al mercado con defectos que han de ser corregidos tras su implantación. Esto es impensable en un automóvil, un electrodoméstico, la construcción de un edificio…, pero en productos TIC es habitual que tras la adquisición de una aplicación informática, por ejemplo, se publiquen errores y fallos de su funcionamiento que se deben corregir con cambios en los programas informáticos.

- **Las TIC son vulnerables a agresiones desde otros lugares u otros países** debido a su propia naturaleza de conectividad. Esta vulnerabilidad está agravada por las otras dos características anteriores: puede producir grandes impactos en la sociedad e incluso importantes beneficios económicos, y además su complejidad intrínseca hace que sea difícil proteger todas sus vulnerabilidades, algunas de las cuales no se conocen hasta que no se sufre una agresión.

Estamos por lo tanto ante una "oleada tecnológica", ya descrita por Alvin Toffler como la "Tercera Ola" en su conocido libro de 1979 [1], en el que describe los efectos de la misma (en comparación con las dos olas anteriores, la agrícola y la industrial) sobre la sociedad, la política, etc. Lo que no mencionó Toffler fue la nueva situación de vulnerabilidad que supone para las sociedades modernas esta "ola".

Hace sólo 30 o 40 años no era fácil detener todo el transporte por ferrocarril de un país, o parar la actividad de miles de oficinas bancarias, y en cuestión de minutos…, hoy es fácil imaginar cómo es posible.

Este estudio propone una reflexión sobre algunas de las necesidades que se están considerando para contribuir a una sociedad más segura en España.

Para ello se ha centrado el foco en la Seguridad frente a agresiones malintencionadas (Security) a las TIC.

1 "La tercera Ola"; Alvin Toffler; año 1979.

En los últimos años, y en ocasiones meses, en España se ha asistido a diferentes esfuerzos en el sentido de dar respuesta a las amenazas, muchas de ellas materializadas, a la Seguridad de las TIC. De entre ellas las más recientes son:

- En Febrero de 2013 la Comisión Europea publica la Estrategia de Ciberseguridad de la Unión Europea (Cybersecurity Strategy of the European Union: An open, safe and secure Cyberspace") [2] y una Propuesta de Directiva Europea para el Parlamento ("Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security accross the Union") [3].

- En Febrero de 2013 el Ministerio de Defensa genera el Mando Conjunto de Ciberdefensa, [4] "para contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa nacional".

- En Marzo de 2013 el Ministerio del Interior y el Ministerio de Industria han firmado un convenio marco de colaboración en materia de Ciberseguridad para conseguir que el ciberespacio sea un entorno seguro para las empresas

[2] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"; Joint Communication to the European Parliament, the Council, the European Economic and Social Committee of the Regions; *European Commission*; JOIN (2013) 1 Final; Bruselas 2013.

[3] "Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union"; *European Comission*; COM (2013) 48 Final; Bruselas 2013.

[4] Creación Mando Conjunto Ciberdefensa. "Orden Ministerial 10/2013, 19 de febrero"; *Boletín Oficial del Ministerio de Defensa;* 2013.
http://www.ieee.es/Galerias/fichero/Varios/BOD_26.02.2013_MandoConjuntoCiberdefensa.pdf

públicas y privadas [5]. El convenio se materializa a través de INTECO y el CNPIC (Centro Nacional de Protección de Infraestructuras Críticas). Se han generado así mismo la Oficina de Coordinación Cibernética y el Centro de Respuesta a Incidentes de Seguridad (CERT) para Infraestructuras Críticas.

- Se prevé para este mismo 2013 la publicación de la Estrategia Española de Ciberseguridad (reclamada desde la propuesta de Directiva Europea)

Además de estas iniciativas desde la Administración, y otras muchas anteriores, como la propia misión del CNI a través del Centro Criptológico Nacional (CCN) de la defensa cibernética de la infraestructura TIC de la Administración, o la propia generación del CNPIC e INTECO, se ha ido generando en España, como en todos los países desarrollados un sector industrial especializado en los equipos y servicios de Ciberseguridad.

Este sector, muy maduro en nuestro país, ha sido objeto de recomendaciones específicas de ordenación en anteriores trabajos de la Fundación [6] y [7].

En el entorno descrito, este estudio concreto pretende analizar el estado y la eficacia de tres herramientas de estructuración de la Ciberseguridad:

[5] Acuerdo del Ministerio de Industria, Energía y Turismo y el Ministerio del Interior para luchar contra la ciberdelincuencia en España"; *Nota de prensa Ministerio del Interior*; Noviembre 2012. http://www.minetur.gob.es/es-es/gabineteprensa/notasprensa/documents/npciberdelincuencia041012.pdf

[6] "Estudio Seguridad Privada en España estado de la cuestión 2012 , (principios , conclusiones y actuaciones propuestas", *Fundación ESYS*; febrero 2012. http://www.fundacionesys.com/index.php?option=com_joomdoc&task=cat_view&gid=9&Itemid=28

[7] "2012 Informe anual de la seguridad en España"; *Fundación ESYS*; 2012. http://www.fundacionesys.com/index.php?option=com_joomdoc&task=cat_view&gid=9&Itemid=28

- Las Certificaciones de Seguridad intrínseca de equipos y aplicaciones informáticas.
- Las Acreditaciones de Seguridad de Sistemas Informáticos en operación.
- Las Acreditaciones de técnicos y directivos de Ciberseguridad.

Estas herramientas, ¿son útiles?, ¿hasta qué punto están implantadas?, ¿cuál es su futuro?.

Para poder responder a estas preguntas, la Fundación ESYS ha recogido la información disponible sobre la normativa que rige a estas herramientas, los organismos que acreditan, los que ensayan, los que certifican, los que evalúan, las empresas usuarias de las TIC, las que prestan servicios de Seguridad en las TIC, etc.

Ha sido de especial relevancia la opinión de algunos expertos consultados:

- **AMETIC** (Asociación de Empresas de Electrónica, Tecnologías de la Información, Telecomunicaciones y Contenidos Digitales), Asociación que agrupa a empresas y asociaciones de empresas representando en total a más 5.000 empresas y a un colectivo de casi 400.000 empleados. Su opinión se ha recogido a través de su Comisión de Seguridad y Confianza.

- Tres grandes empresas usuarias de servicios de Seguridad: **Telefónica, Red Eléctrica y Repsol**.

- Dos empresas punteras y multinacionales en la prestación de servicios de Ciberseguridad: **GMV e Indra.**

El resultado de este esfuerzo se plasma en el presente estudio que, lógicamente, se ha estructurado según los tres aspectos mencionados.

2. LAS CERTIFICACIONES DE SEGURIDAD INTRÍNSECA DE EQUIPOS Y APLICACIONES INFORMÁTICAS

2.1 Situación General

En principio sería de gran importancia que los equipos: ordenadores, impresoras, "routers", "firewalls", etc. y las aplicaciones informáticas: de ofimática, de contabilidad, de control de procesos, páginas web, etc. pudieran exhibir un "sello", una certificación, que indicara al consumidor, sea éste un ciudadano, una empresa o un organismo de la Administración, que se trata de un equipo o una aplicación "segura".

Evidentemente, la propia descripción de este deseo suena ingenua. Las amenazas cambian rápidamente, por lo que la seguridad se debe relacionar con un cierto estado de conocimiento de las amenazas a las que se refiere. No obstante, existe una práctica extendida de certificación de Seguridad de equipos y aplicaciones, basada en los denominados Common Criteria (Criterios Comunes, en adelante CC) [8].

Los CC son un conjunto de normas, redactadas como consenso por una serie de organismos nacionales de Australia, Nueva Zelanda, Canadá, Francia, Alemania, Japón, Holanda, Gran Bretaña, Estados Unidos y España (Ministerio de Administraciones Públicas y el Centro Criptológico Nacional).

Estas normas se han recogido en la familia normativa ISO15408 [9] dándoles carácter de normas internacionales generales.

---

[8] http://www.commoncriteriaportal.org/cc/

[9] "ISO/IEC 15408:2009; Information technology- Security techniques-Evaluation criteria for IT security"; *International Organization of Standardization*; 2009. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=50341

La metodología de los CC obliga a definir para cada equipo o aplicación a analizar (en general llamados TOE, Target of evaluation) un objetivo concreto de especificaciones, el llamado ST (Security Target).

A su vez los ST son definidos por cada fabricante, como particularización para un TOE en concreto del cumplimiento de unas necesidades de Seguridad más generales, definidas para ese tipo de productos o aplicaciones. Esas necesidades, objetivos, de Seguridad son los denominados Protection Profile (Perfiles de Protección, PP).

Es decir, los PP son criterios a aplicar para determinados tipos de productos, y se definen por organismos internacionales. Los ST son propuestas de los fabricantes de un determinado ítem (TOE) como objetivo a cumplir, siendo el ST coherente con el PP correspondiente. Complejo, ¿no?

Las cuestiones más importante son: ¿cuál es el PP adecuado para una necesidad en concreto?, ¿el ST definido por el fabricante incluye todo lo que el PP precisa?, ¿el PP evoluciona tan rápido como lo hacen los perfiles de las amenazas?

No obstante los interrogantes anteriores, la realidad es que la certificación frente a los CC es un hecho.

El proceso se basa en España (en otros países es similar) en que la Entidad Nacional de Acreditación (ENAC) acredita a laboratorios de evaluación a quienes se presentan los TOE y los ST para su ensayo. Una vez realizados éstos y obtenidos los resultados (7 niveles de aceptación o calidad), la documentación resultante es evaluada por un organismo de certificación que, a su vez, ha sido acreditado por ENAC.

En España hay tres laboratorios acreditados: INTA, Applus + y Epoche & Espri, y un organismo de certificación (el Centro Criptológico Nacional (CCN)).

El CCN ha definido los PP relacionados con los distintos tipos de cifradores: IP, de datos, voz, fax, productores de PKI, generadores de números aleatorios, centros de gestión, etcétera, y es obligatorio legalmente que los equipos de cifrado utilizados en la Administración Pública estén certificados por el CCN.

INTECO ha redactado los PP correspondientes a los equipos que utilicen el DNI electrónico.

También se pueden certificar otro tipo de equipos en otras funciones de Seguridad para su utilización en España, ya sea a través del esquema de laboratorios y organismo de acreditación descrito o mediante otros de países diferentes.

En el seno de la Unión Europea esta situación se detecta como necesaria de evolución, según se deduce de las últimas publicaciones.

Así, en la mencionada Estrategia Europea de Ciberseguridad [2], dentro de la acción estratégica 4ª: "Desarrollar recursos industriales y tecnológicos para la Ciberseguridad" se establece como estratégica la puesta en marcha de una plataforma público-privada para definir requerimientos de Ciberseguridad a los productos y aplicaciones utilizados en Europa.

A ese respecto se solicita a ENISA que estimule el desarrollo y la adopción de estándares de Seguridad y el uso de "etiquetas" de Ciberseguridad para identificar equipos y aplicaciones seguros.

2.2 La Opinión de los Expertos

En general los expertos han manifestado la muy necesaria utilidad de contar con un Sistema de Certificación de la Seguridad de los equipos y las aplicaciones, y unánimemente expresan la necesidad de un consenso común europeo.

La certificación basada en los denominados Common Criteria se considera parcialmente útil en España, siendo su limitación la complejidad del proceso y la escasez de empresas acreditadas para la certificación.

2.3 Conclusiones

De todo lo anterior se pueden concluir algunos aspectos relevantes de la situación de la certificación de Seguridad intrínseca de equipos y aplicaciones informáticas:

- **La necesidad de contar con este tipo de certificaciones es alto**, tanto en la opinión de la Administración (Europea, al menos) como de los usuarios profesionales.

- **El estado actual de los mecanismos existentes de certificación no es totalmente satisfactorio**. Se utiliza lo existente, pero su complejidad y su limitación práctica no garantiza realmente la seguridad intrínseca más que ante determinadas circunstancias de difícil comprensión y aplicabilidad.

- **Existe el reto de un posible escenario nuevo**, en función del desarrollo que desde la Unión Europea se promueva al respecto. En cualquier caso, no a corto plazo.

3. LA ACREDITACIÓN DE LA SEGURIDAD DE SISTEMAS INFORMÁTICOS EN OPERACIÓN

3.1 Visión General

También, como en el caso anterior, parece de gran utilidad que los Sistemas Informáticos, que ejecutan funciones diversas para las empresas: contabilidad, facturación, procesos de control, etc. pudieran exhibir un "sello", una acreditación, que indicara al propietario del sistema, o al cliente del servicio que éste presta, sea un ciudadano, una empresa o un organismo de la Administración, que se trata de sistema "seguro", que cumple su funcionalidad con unas garantías mínimas de rechazo de agresiones malintencionadas.

Realmente la complejidad de un Sistema en operación impide garantizar dicho rechazo mediante un conjunto de normas a cumplir que puedan ser comprobadas por una "tercera parte confiable".

Lo que sí existe de forma normalizada es la definición de un modelo de gestión, el denominado Sistema de Gestión de la Seguridad de la Información, SGSI, en el que se definen los procedimientos a seguir para una buena práctica de gestión, todo ello bajo el paraguas de la norma ISO 27001 [10].

Las organizaciones pueden ver certificados sus sistemas de gestión por empresas de certificación externas, acorde con la normativa ISO 27001.

[10] "ISO/IEC 27001:2005; Information technology-Security techniques-Information security management systems-Requirements"; *International Organization of Standardization*; 2005. http://www.iso.org/iso/catalogue_detail?csnumber=42103

Esta normativa establece la metodología a seguir en la gestión, según un proceso de mejora continua que obliga a realizar un análisis de riesgos, a implantar una serie de medidas de Seguridad o salvaguardas, a medir dicha implantación y a gestionar las desviaciones encontradas, de forma que se genere un esquema PDCA (Plan, Do, Check, Act) que cierre continuamente los ciclos de forma periódica, en busca de la mejora continua.

Diversas empresas de certificación realizan auditorias y extienden certificados a las empresas que lo solicitan, para dar confianza a sus clientes o accionistas sobre la Seguridad de los Sistemas de Información. Lógicamente estas auditorías tienen un carácter periódico, para mantener la certificación en vigor tras los cambios que toda organización tiene en el tiempo.

Obviamente, la existencia de dicha certificación, por sí sola, no garantiza que el Sistema esté libre de los riesgos informáticos, pero sí indica que la organización que los ostenta tiene un modelo de gestión adecuado (otra cosa es que lo cumpla adecuadamente).

Es bastante común que cuando una empresa u organismo precise recibir servicios de un proveedor, “acredite” su idoneidad según parámetros propios, pero que en dicha acreditación incluya como requisito indispensable la certificación previa según ISO 27001.

En este sentido se debe resaltar la obligatoriedad de los organismos de las Administraciones Públicas de ser acreditados según el Esquema Nacional de Seguridad (ENS). Esta acreditación la realiza el Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Información (CNI), siguiendo lo estipulado en la Ley 11/2007 y en el Real Decreto 3/2010. La acreditación implica la certificación según ISO 27001, además del seguimiento de unas guías prácticas editadas por el CCN, las CCN-STIC

También, como en el caso anterior, en la Unión Europea esta situación se detecta como una evolución necesaria.

En la Estrategia Europea de Ciberseguridad [2], dentro de la acción estratégica 4ª: “Desarrollar recursos industriales y tecnológicos para la Ciberseguridad” se invita a los “actores públicos y privados” a que, en colaboración con el sector asegurador, se

desarrollen sistemas de medida para que exista el incentivo para las empresas de implementar medidas de Ciberseguridad para abaratar las primas a pagar.

Es decir, se insta a medir la Seguridad de los Sistemas de forma eficaz, lo que invita a deducir que desde la Unión Europea se piensa que la situación actual no permite garantizar con eficacia dicha Seguridad.

El reto de los servicios en la "nube" exige especialmente una forma de garantizar la Seguridad de los Sistemas que permiten esta externalización, al parecer imparable.

También en este aspecto parecen existir dudas importantes sobre la garantía de la resistencia de los servicios así externalizados.

En el trabajo específico de Diciembre de 2012 de ENISA sobre la criticidad de la seguridad en la nube "Critical Cloud Computing. A CIIP (Protección de la Información en las infraestructuras críticas) perspective on Cloud Computing Services" [11] se reconoce la dificultad de determinar las medidas de Seguridad idóneas, dada la velocidad del cambio en las aplicaciones y en las amenazas, y se recomienda generar auditorías periódicas y actualizar las metodologías de forma continua. Un gran reto.

Otra posible forma de analizar la Seguridad de los Sistemas Informáticos en su conjunto es la de centrar el análisis en la protección de los CPDs que, no obstante es una aproximación obviamente parcial al problema.

Para dicho análisis de la protección de los CPDs la normativa más extendida es la del TIER Certification System [12].

Un aspecto importante de este sistema es que declara haber sido diseñado por y para los verdaderos usuarios de los centros de datos (propietarios y técnicos).

---

[11] "Critical Cloud Computing. A CIIP perspective on Cloud Computing Services" *Enisa, European Network and Information Security Agency,* 2012.
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing

[12] http://global.ihs.com/search_res.cfm?RID=TIA&INPUT_DOC_NUMBER=TIA-942

Este sistema es un método que se centra en medir la tolerancia a fallos, la disponibilidad de los recursos, la eficiencia energética y la seguridad de un CPD.

Uptime Institute es el desarrollador de este sistema de clasificación y el único capaz de proveer estos certificados.

Existen cuatro niveles distintos para medir los CPDs: Tier I, Tier II, Tier III y Tier IV. Según esta certificación, cuanto más alto es el nivel, mayor es la robustez y seguridad del centro de datos, y por lo tanto su disponibilidad.

Estos cuatro niveles de los que halamos tienen las siguientes características:

- **Tier I:** Centro de datos Básico. Disponibilidad teórica del 99,671 %.
- **Tier II:** Centro de datos Redundante. Disponibilidad teórica del 99,741%.
- **Tier III:** Centro de datos Concurrentemente Mantenible. Disponibilidad teórica del 99,982%.
- **Tier IV:** Centro de datos Tolerante a fallos. Disponibilidad teórica del 99,995%.

España cuenta con cinco centros con el mayor de los niveles de la certificación (Tier IV), convirtiéndose así en el país europeo con más centros de este nivel, y a nivel mundial, igualando la primera posición con Arabia Saudí.

Estas certificaciones suponen un alto grado de seguridad pero únicamente en lo referente a los centros de proceso de información.

3.2 La opinión de los expertos

Se ha pulsado la opinión principalmente sobre tres aspectos del marco de acreditación:

a) **Su necesidad teórica**.- La opinión general ha sido la de considerar esta necesidad entre alta y muy alta.

b) La **idoneidad del marco de ISO 27001** como referencia a la que ajustar los modelos de gestión.- Ha habido alguna discrepancia, la mayoría de los expertos lo consideran idóneo y algunos creen que es insuficiente.

c) La **situación actual en España** de la aplicación de estas acreditaciones.-Tampoco ha habido unanimidad. Las opiniones se dividen entre los que piensan que es adecuada (la mayoría) y quienes ven la necesidad de un mayor rigor en el control de ENAC, o de un mercado más exigente que no se oriente a conseguir el certificado únicamente.

3.3 Conclusiones

- **La necesidad de contar con este tipo de acreditaciones es muy alto**, especialmente con la tendencia hacia los servicios en la "nube".

- **El estado actual de los mecanismos existentes de acreditación es parcialmente satisfactorio**. Realmente sólo se acredita la existencia de una organización de la seguridad acorde con la normativa ISO 27001 fundamentalmente. Eso está muy lejos de garantizar la resistencia frente a Ciberataques o mal uso de los Sistemas de Información.

- **La Seguridad de los CPD dispone de una acreditación adecuada,** pero sólo afecta a una parte, importante, de la Seguridad de los Sistemas.

- **No parece fácil mejorar la situación actual,** en el sentido de contar con una metodología que garantice a las empresas, a sus accionistas y clientes, y a las empresas aseguradoras, que un Sistema Informático es razonablemente seguro. Es quizá el problema más importante en el terreno de la Ciberseguridad y, como mínimo, su solución debe ser armonizada a nivel europeo.

4. NECESIDADES DE ACREDITACIÓN DE TÉCNICOS Y DIRECTIVOS DE CIBERSEGURIDAD

4.1 Visión general

La acreditación de personal técnico de Ciberseguridad, es un aspecto totalmente diferente a los anteriores.

El objetivo de la acreditación de personal es el de garantizar la pericia y la fiabilidad de los técnicos que diseñan, o instalan u operan equipos o sistemas informáticos desde la perspectiva de la Seguridad y el acceso a determinada información.

En el Anteproyecto de Ley de Seguridad Privada [13] ni siquiera se menciona a los técnicos o ingenieros como personal de Seguridad, aunque es evidente la importancia de sus actuaciones y la responsabilidad que conllevan (sí se regula en cambio, la selección y formación de los vigilantes de Seguridad).

Independientemente de la Legislación, la necesidad de garantizar la pericia de los técnicos especializados en Ciberseguridad, dada la complejidad tecnológica cambiante de esta disciplina, parece de gran importancia para hacer más claro el mercado de los servicios asociados.

Las acreditaciones que se han detectado en España lo son sin que ninguna legislación o regulación las reclame, y los técnicos que las detentan han accedido a esas acreditaciones a efectos curriculares, en un mercado laboral no regulado al respecto.

Entre las acreditaciones más extendidas en España se cuentan las de ISACA (CISM y CRISC), la de AENOR (S0A S0By S0C), la de ISMS Forum (CDPP) y la de ISC2 (CISSP).

[13] "Anteproyecto de Seguridad Privada"; *Ministerio del Interior*, 16 Abril 2013.

ISACA, International Security Audit and Control Association es una asociación internacional de profesionales, y cuenta en España con tres "capítulos" en Madrid, Barcelona y Valencia. Promueven principalmente dos acreditaciones de personas orientadas a la Ciberseguridad: CISM y CRISC.

CISM, Certified Information Security Manager, está orientado a técnicos y Directivos de Ciberseguridad. Se debe superar un examen y se debe renovar cada tres años mediante formación específica (no exámenes).

CRISC, Certified in Risk and information Systems Control, está principalmente orientado a gestores de Ciberseguridad. Como en el caso anterior es renovable de forma similar.

AENOR, en su actividad docente extiende unos títulos de formación propios, relacionados con la utilización adecuada de la normativa ISO 27001. No son renovables y no son acreditaciones en sentido estricto, aunque se pueden considerar así por el mercado.

S0A, Auditor de Sistema de Gestión de la Información, orientado a Técnicos Auditores de Sistemas según ISO 27001.

S0B, Experto Implantador de Sistemas de Gestión de Seguridad de la Información, orientado a técnicos que han de implantar Sistemas de Gestión según ISO 27001.

S0C, Experto en Sistemas de Gestión de Seguridad de la Información, orientado a gestores de Sistemas según ISO 27001.

ISMS Forum, Asociación Española para el fomento de la Seguridad de la Información, capítulo español del ISMS International User Group. Mantiene un directorio de profesionales españoles (voluntario) y sus acreditaciones. Acredita y forma profesionales en acreditaciones del ISMS.

CDPP, Certified Data Privacy Professional, no renovable y que precisa acreditar 3 años de experiencia además de superar un examen. Orientado a técnicos y gestores.

CCSK, Certificate of Cloud Security Knowledge, orientado a técnicos que gestionen la seguridad de servicios en la "nube".

ISC2, International Information System Security Certification Consortium, organización internacional. Promueve varias acreditaciones, la más conocida es la que se expone.

CISSP, Certified Information Systems Security Professional, orientado a técnicos y homologado en USA como certificado según ISO 27024.

Otras también extendidas son las de IRCA (LA ISO 27001), SANS (GIAC), CSA (CCSK), EC Council (CEH), IAPP (CIPP),...

Como se pone de manifiesto, todas estas acreditaciones en realidad lo que exponen es que la persona que las detente ha superado con éxito un examen correspondiente, que responde a un cuerpo de contenidos técnicos determinado, y diverso según cada acreditación y, en algunos casos, que acredita una experiencia profesional en la actividad determinada.

Evidentemente el personal que disponga de una de estas acreditaciones reconocidas, en el mejor de los casos garantiza, a quien le contrate o a quien reciba servicios de una empresa que le emplee, que ese técnico o gestor tiene una formación técnica adecuada para las tareas que realiza, pero en ningún caso da indicaciones sobre la honradez de la persona.

Este último aspecto sólo podría abordarse desde una legislación específica (inexistente) como la que permite seleccionar a los vigilantes de Seguridad Física e, incluso, penalizar de forma especial los delitos que pueda cometer.

Por otra parte, es interesante estudiar la existencia de las titulaciones universitarias y de formación profesional que afectan a estos conocimientos, lo que se recoge en el estudio de ESYS "Necesidades de Formación en el sector de la Seguridad" de 2013 [14].

También atendiendo a lo que desde la Unión Europea se plantea, y a partir de lo que se menciona en la citada Estrategia Europea de Ciberseguridad [2], dentro de la acción estratégica 1ª: "Promover la resiliencia cibernética" se le insta a ENISA a que proponga un plan ("roadmap") para conseguir un programa de certificación voluntario ("driving licence") que permita mejorar (y garantizar) las capacidades de los profesionales de la Seguridad Informática. Es decir, una vez más inconformismo europeo ante la situación actual.

Por todo lo anterior hay interrogantes interesantes a plantear.

> ¿**Son fiables las acreditaciones** para garantizar los conocimientos de los profesionales?
>
> ¿**Es razonable este sistema de múltiples acreditaciones** frente a la licenciatura universitaria específica?

4.2 La Opinión de los Expertos

Los expertos han opinado sobre dos sujetos posibles de acreditación: Los Directivos con responsabilidad sobre la Ciberseguridad de sus empresas y los Técnicos Especialistas que proveen de servicios de Ciberseguridad.

[14] "Necesidades de formación en el sector de la seguridad"; *Fundación ESYS* 2013.

En cuanto a los **Directivos de Seguridad** ha habido casi unanimidad en considerar necesaria su acreditación en alguna de sus formas, y también que afecte a los conocimientos específicos como a su honestidad.

Mayoritariamente se opina que la formación debiera ser universitaria (grado) y complementada con un master especializado.

En lo que respecta a los **Técnicos de Ciberseguridad,** también se opina mayoritariamente que se precisa su acreditación, y que afecte a los aspectos técnicos y morales, pero donde no hay unanimidad, incluso importante dispersión de opiniones es en los aspectos de la formación, en cuanto si ésta ha de ser académica o de entidades privadas y asociaciones internacionales.

4.3 Conclusiones

- **Parece importante contar con acreditaciones profesionales de Ciberseguridad**, tanto desde el aspecto de capacidad técnica como de honestidad.

- **Actualmente sólo existen acreditaciones profesionales en los aspectos de capacidad técnica,** y son de tipo voluntario y radicadas en organizaciones internacionales, no sujetas a legislación europea ni española específica.

- **La situación actual es insatisfactoria**, en cuanto a que el reconocimiento legal de estas acreditaciones es nulo y a que no garantiza la ética, ni su responsabilidad legal, de las personas acreditadas.

- **Sería deseable contar con un sistema de acreditación español, armonizado con Europa,** centrado en las características técnicas y apoyado en estudios universitarios.

- **Sería deseable contar con que la Administración española regulara la responsabilidad legal de los técnicos de Ciberseguridad,** mediante la incorporación de este aspecto a la Legislación específica necesaria de la Ciberseguridad dentro de la Seguridad Privada.

5. DATOS DEL ESTUDIO

5.1 Redacción

El equipo de redacción se ha formado por los miembros de la Comisión Delegada Técnica de la Fundación (de las empresas Telefónica, Indra, Gas Natural Fenosa y Securitas), coordinados por el Presidente de la Comisión.

La Edición se ha realizado desde la Dirección y la Secretaría de la Fundación.

5.2 Los Derechos del Estudio

La presente publicación pertenece a la Fundación Empresa, Seguridad y Sociedad (ESYS) y está bajo una licencia Reconocimiento-No comercial-SinObraDerivada 3.0 Unported España de Creative Commons, y por ello está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento:** El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a Fundación ESYS como a su sitio Web: *www.fundacionesys.com*. Dicho reconocimiento no podrá en ningún caso sugerir que ESYS presta apoyo a dicho tercero o apoya el uso que hace de su obra.

- **Uso No Comercial**: El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

- **Sin Obra Derivada**: La autorización para explotar la obra no incluye la transformación para crear una obra derivada.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de ESYS como titular de los derechos de autor. Nada en esta licencia menoscaba o restringe los derechos morales de ESYS.

5.3 Referencias

5.3.1 Textos

[1]- "La tercera Ola"; *Alvin Toffler*; año 1979.

[2]- "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace"; Joint Communication to the European Parliament, the Council, the European Economic and Social Committee of the Regions; *European Commission*; JOIN (2013) 1 Final; Bruselas 2013.

[3]- "Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union"; *European Comission*; COM (2013) 48 Final; Bruselas 2013.

[4]- Creación Mando Conjunto Ciberdefensa. "Orden Ministerial 10/2013, 19 de febrero"; *Boletín Oficial del Ministerio de Defensa;* 2013. http://www.ieee.es/Galerias/fichero/Varios/BOD_26.02.2013_MandoConjuntoCiberdefensa.pdf

[5]- "Acuerdo del Ministerio de Industria, Energía y Turismo y el Ministerio del Interior para luchar contra la ciberdelincuencia en España"; *Nota de prensa Ministerio del Interior*; Noviembre 2012. http://www.minetur.gob.es/es-es/gabineteprensa/notasprensa/documents/npciberdelincuencia041012.pdf

[6]- "Estudio Seguridad Privada en España estado de la cuestión 2012 , (principios , conclusiones y actuaciones propuestas", *Fundación ESYS*; febrero 2012.

http://www.fundacionesys.com/index.php?option=com_joomdoc&task=cat_view&gid=9&Itemid=28

[7]- "2012 Informe anual de la seguridad en España"; *Fundación ESYS*; 2012. http://www.fundacionesys.com/index.php?option=com_joomdoc&task=cat_view&gid=9&Itemid=28

[8]- http://www.commoncriteriaportal.org/cc/

[9]- "ISO/IEC 15408:2009; Information technology- Security techniques-Evaluation criteria for IT security"; *International Organization of Standardization*; 2009. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=50341

[10]- "ISO/IEC 27001:2005; Information technology-Security techniques-Information security management systems-Requirements"; *International Organization of Standardization*; 2005. http://www.iso.org/iso/catalogue_detail?csnumber=42103

[11]- "Critical Cloud Computing. A CIIP perspective on Cloud Computing Services" *Enisa, European Network and Information Security Agency,* 2012. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing

[12]- http://global.ihs.com/search_res.cfm?RID=TIA&INPUT_DOC_NUMBER=TIA-942

[13]- "Anteproyecto de Seguridad Privada"; *Ministerio del Interior*, 16 Abril 2013.

[14]- "Necesidades de formación en el sector de la seguridad"; *Fundación ESYS* 2013.

5.3.2 Referencias Web

- www.ccn.cni.es
- www.cnpic-es.es
- www.inteco.es
- www.ametic.es
- www.fundacionesys.com
- www.gasnaturalfenosa.com
- www.indracompany.com
- www.securitas.com/es
- www.santander.com
- www.telefonica.es
- www.minhap.gob.es
- www.enac.es
- www.inta.es
- www.applus.com
- www.epoche.es
- http://europa.eu/index_es.htm
- www.enisa.es
- www.isaca.org/spanish
- www.aenor.es/aenor
- www.ismsforum.es
- www.isc2.org

- http://www.cni.es

- Esquema nacional de Seguridad (ENS): http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=146

- Guías CCN-STIC: https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=188&lang=es