Preparándonos para invertir en Ciberseguridad

José Mª de las Heras (cedscad@nauta.es)
*Vocal de la Junta Directiva de **ALI***

El próximo mes de Octubre es un mes importante para iniciar la confección de "presupuestos" en los que las inversiones a realizar siempre ocupan una partida importante. En pleno desarrollo de la Sociedad de la Información, las inversiones TIC siempre están presentes siguiendo las tendencias actuales que afectan directamente a cada sector de actividad, como: Big Data, Cloud Computing, IoT, Smart Cities, Industria 4.0, Redes sociales, Tecnologías cognitivas, Nuevos modelos de pago, etc.

Somos conscientes que puesto que estamos inmersos en una sociedad de la información global en un mundo interconectado a través de Internet[1], hemos añadido el prefijo "ciber"[2] para referirnos a este contexto global en el que utilizamos las TIC. De aquí que nos refiramos a las necesidades de seguridad de las mismas, tanto en su diseño como en su construcción y uso, con la nueva palabra: "ciberseguridad"[3].

Es posible que para 2017 muchas organizaciones, tanto públicas como privadas, estén planificando inversiones en Big Data o Cloud Computing y que las empresas del sector industrial preparen inversiones para evolucionar a la Industria 4.0, o que muchos Ayuntamientos estén preparando inversiones relacionadas con proyectos Smart Cities, pero creo que tales inversiones "quedarían cojas" si con las mismas no consideramos también las necesidades de seguridad que precisan, es decir las inversiones en Ciberseguridad.

Nos engañaríamos si no tenemos en cuenta que para la mayoría de organizaciones resulta complejo planificar, concreta y priorizar las necesarias inversiones en ciberseguridad. Tal

[1] OECD - Organisation for Economic Co-Operation and Development - 35 Member Countries: INTERNET USERS IN 2016 Q2 http://www.internetworldstats.com/stats16.htm

[2] **Ciber**: Elemento prefijal que surge a partir de la palabra 'cibernético' y que entra en la formación de nombres relacionados con la 'cibernética' y más concretamente de 'informática'. Ej. "cibernauta, cibercultura, ciberespacio"

[3] **Ciberseguridad**: La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad."
UIT - Resolución 181 - Recomendación UIT–T X.1205
http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

dificultad emana de la propia definición de ciberseguridad que implica un proceso de seguridad transversal que afecta a toda la organización, que ha de estar bien definido, diseñado e implantado en la misma y siempre teniendo en cuenta que "el eslabón más débil de este proceso" es quien en último término define el nivel de seguridad del mismo.

Los Ingenieros en Informática tenemos la obligación ética y profesional de tener buenos conocimientos actualizados de ciberseguridad y ser interlocutores validos para aportar la luz que necesitan los consejos y comités de administración y de dirección de las organizaciones públicas y privadas para llevar a cabo tales inversiones en ciberseguridad.

Tras esta breve introducción el propósito de este artículo es presentar y dar a conocer dos recientes documentos de gran interés para aquellos ingenieros en informática involucrados en proyectos de seguridad de distinta índole y que bien directa o indirectamente desempeñan el papel de consultores o interlocutores en dichas inversiones

Documento 1: "TENDENCIAS EN EL MERCADO DE LA CIBERSEGURIDAD"[4]

El objetivo principal del Estudio es identificar las grandes tendencias del mercado de la ciberseguridad y describir su potencial oportunidad de negocio para las empresas de la Industria Nacional en Ciberseguridad, configurándose para los integrantes como:

- Mecanismo para la toma de decisiones sobre el modelo de negocio y la estrategia de desarrollo de productos y servicios de ciberseguridad.
- Elemento de promoción de nuevos segmentos y oportunidades de inversión para las empresas.
- Método de estudio sobre la colaboración entre distintos agentes del mercado favoreciendo el establecimiento de sinergias.

Comentarios: Si bien el documento debe considerarse como especializado para el sector de la Ciberseguridad se ha redactado para que su comprensión sea fácil por no especialistas en este ámbito. El documento anuncia la puesta en marcha de un Polo Tecnológico Nacional en Ciberseguridad.

> *"El **Polo Tecnológico Nacional en Ciberseguridad** contará, entre otros, con un objetivo estratégico clave basado en **incrementar la actividad productiva competitiva a nivel internacional de los participantes en materia de ciberseguridad.***

[4] Es un reciente documento publicado por INCIBE que puede bajarse de: https://www.incibe.es/sites/default/files/estudios/tendencias_en_el_mercado_de_la_ciberseguridad.pdf

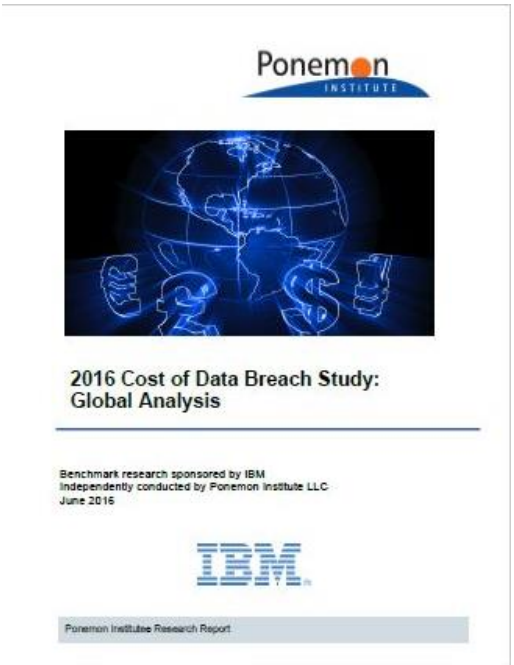
Una vez aprobada la idoneidad y oportunidad de desarrollar y potenciar dicho Polo Tecnológico Nacional en Ciberseguridad, competitivo a nivel internacional y sostenible en el tiempo, ***INCIBE*** *como entidad de referencia y actor neutral en el ámbito de la ciberseguridad nacional, dentro de un marco de colaboración público-privada,* ***pone en marcha una primera fase de medidas encaminadas a aumentar la competitividad del sector, potenciar el mercado interior y promover la internacionalización de la Industria*** *de ciberseguridad española para su desarrollo."*

El documento pone de manifiesto los últimos datos económicos relacionados con el crecimiento del sector de la ciberseguridad:

- *"A nivel global, según Gartner, el sector de la ciberseguridad presenta una facturación mundial de 62.540 millones de euros en 2015 y una previsión de aumento de la demanda (partiendo de un gasto en ciberseguridad de 54.082 millones de euros en 2014) que alcanzará los 79.292 millones de euros en 2018".*
- *"A nivel nacional, la facturación total del sector de la ciberseguridad en 2014 fue de 598,2 millones de euros, según datos del ONTSI".*

E identifica un mapa de tendencias de demanda en el que "***se identifican 20 tendencias globales en ciberseguridad catalogadas en torno a 6 sectores de actividad"***. Es un documento muy bien realizado y estructurado en el que también se puede destacar tanto la fiabilidad de las fuentes de información utilizadas como la amplitud de conocimientos en ciberseguridad de los participantes en su realización.

Documento 2: "2016 Cost of Data Breach Study: Impact of Business Continuity Management



Es una investigación realizada por Ponemon Institute LLC con el patrocinio de IBM.

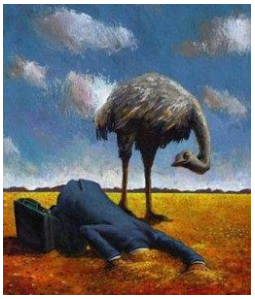
Como resultados de esta investigación están disponibles tres tipos de informes[5]:

- Global report (Learn about the global impact of a data breach)
- Country-specific report (Discover how a data breach affects selected countries. Aunque para España no está, si lo están por ejemplo para Francia e Italia)
- Impact of Business Continuity Management report (Learn how Business Continuity Management can reduce the cost and impact of a data breach)

[5] Estos tres tipos de informe se pueden bajar por separado de: http://www-03.ibm.com/security/data-breach/

Comentarios: Son informes muy actualizados, basados en incidentes reales y con gran nivel de detalle en el cálculo los costes. En su realización han participado organizaciones que han sufrido incidentes de ciberseguridad no muy escandalosos, pero que sin embargo de media suponen daños que sobrepasan los tres millones de euros. En la investigación realizada se informa que los grandes incidentes de seguridad no se han tenido en cuenta para no distorsionar los resultados de dicha investigación, es decir son incidentes de seguridad que afectan a un rango de entre 5.000 y 100.000 registros. La investigación arroja mucha información, como por ejemplo: Los tiempos medios en detectar los incidente y en solucionarlos, los costes directos e indirectos asociados al incidente, o los costes reputacionales traducidos a euros ó dólares. El tercer documento (Impact of Business Continuity Management –BCM- report), entra en detalles sobre cómo disminuyen de dichos costes, y tiempos, cuando la organización dispone de BCM.

Posiblemente el mensaje más contundente de esta investigación es el de que para cualquier organización, sea pública o privada, que lleva a cabo sus actividades en la sociedad de la información **"Invertir en Ciberseguridad es invertir en el Negocio".**



Obviar los riesgos de seguridad, siguiendo la conducta del Avestruz[6], trae malas consecuencias a nivel personal, pero sin duda mucho peores si tal conducta es llevada a cabo por una organización.

Sin el ánimo de ser alarmistas, hemos de ser conscientes de que dichos riesgos son cada día más graves y sin ignorar que "***la ciberdelincuencia se ha convertido en una economía de servicios que está más fuerte que nunca***"[7].

En España tenemos el gran privilegio de contar con publicaciones periódicas, muchas de ellas gratuitas, que permiten a los ingenieros en informática mantenernos al día en temas de Ciberseguridad y, sin obviar los estudios e informes frecuentes que publican organizaciones como INCIBE o CCN, disponemos de buenas revistas especializadas en ciberseguridad como por ejemplo: Revista SIC, Red Seguridad, Revista CIBER elcano, etc.

Pero si en último término afirmamos ***"que la ciberseguridad nos atañe a todos"***, estaremos de acuerdo en que a los ingenieros en informática nos atañe un poco más, por la responsabilidad ética y profesional de estar directamente involucrados en los proyectos que permiten hacerla realidad en nuestras organizaciones.

[6] Eufemismos, o… conducta del avestruz
https://macabal.wordpress.com/2009/08/12/eufemismos-o%e2%80%a6-conducta-del-avestruz/
[7] Cybercrime-as-a-Service Economy: Stronger Than Ever
http://www.bankinfosecurity.com/cybercrime-as-a-service-economy-stronger-than-ever-a-9396