H.O.N.G.O.S. y C.H.A.M.P.I.Ñ.O.N.E.S.

Luis G. Fernández
Editor
lfernandez@codasic.com

Quienes conformamos el mundillo de la seguridad de la información hemos de bregar diariamente con una retahíla de acrónimos, mayormente de origen anglosajón, que conforman el escenario de comunicación típico de los profesionales de esta disciplina. La verdad es que es una tarea cansina tener que desentrañar los contenidos de cientos de 'palabrotas' técnicas a las que hemos de aludir para así poder transmitir atinadamente a nuestros interfectos cualesquiera mensaje referidos a la seguridad. Y esto es inevitable e imparable.

En fin, será porque corren tiempos primaverales, pero lo cierto es que la jerga de nuevos h.o.n.g.o.s. y c.h.a.m.p.i.ñ.o.n.e.s. tecnológicos prolifera más que nunca. En forma de abotargantes acrónimos nos vemos en la obligación de entender correctamente el significado de un grupo de letras asociadas a titulaciones, certificaciones, estándares, productos, herramientas y versiones, protocolos, asociaciones..., etc.

De cualquier modo, en las tendencias primavera-verano 2004 tres de estos terminajos tienen visos de incorporarse al acerbo profesional, al menos durante un tiempo. De procedendencia estadodunidense, constituyen tres iniciativas que, sobre el papel, parecen interesantes; se denominan **CSIA** (**Cyber Security Industry Alliance**), **GIAIS** (**Global Infraestructure Alliance for Internet Safety**), y **SecMet** (**Security Metrics Consortium**).

El propósito de la CSIA es claro: ante tanta calamidad telemática los pesos pesados de la industria de seguridad TIC, por fin, desean erigirse en una voz única que ayude a buscar soluciones para afrontar la mejora de la protección en la Red.

Por su parte, la GIAIS la protagonizan **Microsoft** y un importantísimo colectivo de ISPs (incluyendo a la española **Terra**); su pretensión es ayudar a que sus clientes reduzcan el trabajo de gestión de la seguridad de sus sistemas; a los usuarios para lograr la seguridad de su ordenador en línea; a proteger y restaurar a los internautas de las infracciones de seguridad mediante herramientas y guías; y a establecer canales ágiles de comunicación entre los miembros de la alianza para una respuesta rápida en el momento en el que se produzca el ataque de un virus o código malicioso.

Por último, el objetivo de SecMet es definir métricas de riesgos de seguridad cuantitativas estandarizadas para su adopción por parte de la industria, las empresas y los fabricantes, a partir de la experiencia aportada por grandes profesionales de la seguridad del lado usuario. Es curioso constatar que la idea -ciertamente atractiva- coincide en tiempo con las iniciativas de estandarización internacionales cuyo reflejo inmediato es la reciente constitución del grupo de trabajo 'Métricas' del SC27 español adscrito a Aenor.

Son pues todas ellas pretensiones loables. Y tienen visos de oportunidad y sensatez. Por su utilidad, bien vale darles una oportunidad de incorporarse a nuestro zurrón terminológico. ●