Arturo Ribagorda

SEGURIDAD Y CERTIFICACIÓN EN EL COMERCIO ELECTRÓNICO

Autor: Andrés Font
Editorial: Biblioteca Fundación Retevisión
Año 2000 - 165 páginas - ISBN: 84-931542-1-0
Sitio: www.retevision.es/fundacion

Desde su nacimiento, esta sección ha saludado con alborozo la aparición de libros escritos en nuestra lengua y versados en la seguridad de la información. Esto siempre ha sido así por lo que ello tenía de consolidación de la materia en nuestro país, pero también porque todas las obras presentaban un magnífico nivel expositivo y denotaban un nivel de competencia de sus autores nada desdeñable, y desde luego equiparable al de especialistas de otros países con más rodaje en las Tecnologías de la Información que el nuestro.

Lamentablemente, el libro que en esta ocasión traemos a colación: **Seguridad y certificación en el comercio electrónico**, de **Andrés Font**, editado por la prestigiosa y respetable **Fundación Retevisión** (que tan encomiables labores de patrocinio y mecenazgo realiza en el ámbito de las tecnologías y que ha publicado otras obras del máximo interés, como "Comercio electrónico: Perspectiva presente y futura en España"), no permite la salutación alborozada a la que aludíamos al inicio.

El libro (mejor opúsculo, aunque antes por su extensión que por su carácter didáctico) no da la talla, al menos en lo que atañe a sus capítulos más técnicos –es decir, la práctica totalidad de la obra–, y no por un fallido intento de hacer descender los conceptos técnicos más inextricables a un nivel comprensible por los lectores más neófitos o ni siquiera iniciados, sino antes bien por una redacción a vuela pluma y, sin duda, por la falta de especialización del autor, abogado y master en gestión –según se apunta en la solapa del manual–.

Avanzando ya en los pormenores de la obra, lo primero que sobresale es el abrumador muestrario de voces inglesas –además de numerosos anglicismos– que la pueblan. Bien es verdad que el autor se excusa por ello en el prólogo (excusatio no petita acusatio manifiesta), pero no parece disculpable la contumaz reiteración con la que se escribe a todo lo largo y ancho del manual "*network*" en vez de red. O "*packets*" por paquetes (de red). O "*worm*" por gusano, "*Trojan Horse*", por caballo de Troya (o incluso troyano, aunque personalmente prefiera la primera), "*logic bomb*" por bomba lógica, y tantas otras voces que de escribir todas llenaríamos el espacio entero dedicado a esta recensión. Evidentemente, ello manifiesta un supino desconocimiento de los textos en castellano editados acerca de la materia –no ya de la seguridad, sino aun de la informática en general–, que hace ya tiempo desterraron los anteriores vocablos reemplazándolos por sus correlatos españoles antedichos.

Pero si lo anterior atañe sólo a la ortografía (y admito que aunque a mi, como docente, me parezca de la mayor importancia muchos lo puedan considerar un tema menor), no para ahí lo cuestionable de la obra. Así, muchas de las definiciones que se deslizan –o explícitamente se proponen como tal en el glosario con que se concluye el trabajo–, sonrojarán a cualquiera mínimamente ilustrado en la disciplina de seguridad. Por ejemplo, se puede leer que: "los *bugs* se infiltran en el software, permitiendo al intruso penetrar...", como si un *bugs* (¿por qué no error?) fuese un programa maligno que cualquier *hacker* introduce deliberadamente en un ordenador. O bien la siguiente afirmación categórica y sin matices: "*Proxy servers*. Se trata de un programa que bloquea la entrada de los virus en las *network*". Tampoco tiene desperdicio la contundente perla que se puede leer en la página 58: "La razón por la que la clave privada puede desencriptar el texto encriptado por la clave pública es que ambas claves están relacionadas matemáticamente a través de una función *hash* o unidireccional.", todo un hallazgo en el cual nadie había caído hasta ahora. Igualmente, en el apartado 4.4 donde se habla de las componentes de una PKI, se afirma con evidente desenvoltura: "Historial de claves. Relación de los datos encriptados por las claves emitidas."(¿?).

Pero si en vez de repasar el texto, acudimos al glosario –que sólo se puede calificar de inefable–, hallamos acepciones del siguiente tenor literal: "Firma digital. Un texto o mensaje encriptado con una clave privada que sirve para autenticar la identidad del remitente.", con ausencia de toda mención a la integridad que tal firma preserva, y que es tan característica de ésta como la autenticación del remitente. Igualmente, nos topamos con que una Autoridad de Registro es: "Una entidad que actúa al servicio de la AC en los procesos registro y verificación de la identidad de un solicitante de una clave privada.", se observará que no de un certificado. También, para el autor, los certificados de clave pública no son digitales, pues un certificado digital es: "Un documento electrónico que verifica la identidad del titular del certificado y sus 'atributos'."

A la vista de lo anterior, el lector disculpará que le sigamos martirizando con despropósitos de semejante cariz –que lejos de concentrarse en algún apartado contaminan todos ellos–, o que nos abstengamos de hacer cualquier juicio crítico de la estructura o disposición de unos capítulos de tan penosa lectura por el cúmulo de disparates que contienen, de los cuales los arriba entresacados no son sino una exigua muestra.

Así pues, se trata de una enorme osadía (no insólita en nuestro país, pero no por ello menos censurable) consistente en pensar que cualquiera puede cultivar cualquier terreno –por lejano que se halle de su formación profesional– tras una breve aproximación. n

Arturo Ribagorda
Catedrático de la Universidad Carlos III de Madrid