Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de ATI (Asociación de Técnicos de Informática). _Novática_ edita también _Upgrade_, revista digital de CEPIS (_Council of European Professional Informatics Societies_), en lengua inglesa.

<http://www.ati.es/novatica/>
<http://www.upgrade-cepis.org/>

ATI es miembro de CEPIS (*Council of European Professional Informatics Societies*) y tiene un acuerdo de colaboración con ACM (*Association for Computing Machinery*). Tiene asimismo acuerdos de vinculación o colaboración con AdaSpain, AI2 y ASTIC

CONSEJO EDITORIAL

Antoni Carbonell Nogueras, Francisco López Crespo, Julián Marcelo Cocho, Celestino Martín Alonso, Josep Molas i Bertrán, Roberto Moya Quiles, César Pérez Chirinos, Mario Piattini Velthuis, Fernando Piera Gómez (Presidente del Consejo), Miquel Sarries Griñó, Carmen Ugarte García, Asunción Yturbe Herranz

Coordinación Editorial
Rafael Fernández Calvo <*rfcalvo@ati.es*>

Composición y autoedición
Jorge Llácer

Traducciones
Grupo de Lengua e Informática de ATI
Coordinadas por José A. Accino (Univ. de Málaga) <*jalfonso@ieev.uma.es*>

Administración
Tomás Brunete, María José Fernández, Enric Camarero, Felicidad López

SECCIONES TECNICAS: COORDINADORES
Administración Pública Electrónica
Gumersindo García Arribas, Francisco López Crespo (MAP)
<*gumersindo.garcia@map.es*>, <*flc@ati.es*>
Arquitecturas
Jordi Tubella (DAC-UPC) <*jordit@ac.upc.es*>
Víctor Viñals Yúfera (Univ. de Zaragoza) <*victor@unizar.es*>
Auditoría SITIC
Marina Touriño, Manuel Palao (ASIA)
<*marinatourino@marinatourino.com*>, <*manuel@palao.com*>
Bases de Datos
Coral Calero Muñoz, Mario G. Piattini Velthuis
(Escuela Superior de Informática, UCLM)
<*Coral.Calero@uclm.es*>, <*mpiattin@inf-cr.uclm.es*>
Derecho y Tecnologías
Isabel Hernando Collazos (Fac. Derecho de Donostia, UPV)
<*ihernando@legaltek.net*>
Isabel Davara Fernández de Marcos (Davara & Davara)
<*idavara@davara.com*>
Enseñanza Universitaria de la Informática
Joaquín Ezpeleta Mateo (CPS-UZAR) <*ezpeleta@posta.unizar.es*>
Cristóbal Pareja Flores (DSIP-UCM) <*cpareja@sip.ucm.es*>
Informática y Filosofía
Josep Corco (UIC) <*jcorco@unica.edu*>
Esperanza Marcos (ESCET-URJC) <*cuca@escet.urjc.es*>
Informática Gráfica
Roberto Vivó (Eurographics, sección española) <*rvivo@dsic.upv.es*>
Ingeniería del Software
Javier Dolado Cosín (DLSI-UPV) <*dolado@si.ehu.es*>
Luis Fernández (PRIS-EI-UEM) <*lufern@dpris.esi.uem.es*>
Inteligencia Artificial
Federico Barber, Vicente Botti (DSIC-UPV)
<*{vbotti, fbarber}@dsic.upv.es*>
Interacción Persona-Computador
Julio Abascal González (FI-UPV) <*julio@si.ehu.es*>
Jesús Lorés Vidal (Univ. de Lleida) <*jesus@eup.udl.es*>
Internet
Alonso Álvarez García (TID) <*alonso@ati.es*>
Llorenç Pagés Casas (Indra) <*pages@ati.es*>
Lengua e Informática
M. del Carmen Ugarte (IBM) <*cugarte@ati.es*>
Lenguajes informáticos
Andrés Marín López (Univ. Carlos III) <*amarin@it.uc3m.es*>
J. Angel Velázquez (ESCET-URJC) <*a.velazquez@escet.urjc.es*>
Libertades e Informática
Alfonso Escolano (FIR-Univ. de La Laguna) <*aescolan@ull.es*>
Lingüística computacional
Xavier Gómez Guinovart (Univ. de Vigo) <*xgg@uvigo.es*>
Manuel Palomar (Univ. de Alicante) <*mpalomar@dlsi.ua.es*>
Mundo estudiantil
Adolfo Vázquez Rodríguez
(Rama de Estudiantes del IEEE-UCM) <*a.vazquez@ieee.org*>
Profesión informática
Rafael Fernández Calvo (ATI) <*rfcalvo@ati.es*>
Miquel Sarries Griñó (Ayto. de Barcelona) <*msarries@ati.es*>
Redes y servicios telemáticos
Luis Guijarro Coloma (DCOM-UPV) <*lguijar@dcom.upv.es*>
Josep Solé Pareta (DAC-UPC) <*pareta@ac.upc.es*>
Seguridad
Javier Areitio (Redes y Sistemas, Bilbao) <*jareitio@orion.deusto.es*>
Javier López Muñoz (ETSI Informática-UMA) <*jlm@lcc.uma.es*>
Sistemas de Tiempo Real
Alejandro Alonso, Juan Antonio de la Puente
(DIT-UPM) <*{aalonso,jpuente}@dit.upm.es*>
Software Libre
Jesús M. González Barahona, Pedro de las Heras Quirós
(GSYC-URJC) <*{jgb,pheras}@gsyc.escet.urjc.es*>
Tecnología de Objetos
Jesus García Molina (DIS-UM) <*jmolina@correo.um.es*>
Gustavo Rossi
(LIFIA-UNLP, Argentina) <*gustavo@sol.info.unpl.edu.ae*>
Tecnologías para la Educación
Josep Sales Rufí (ESPIRAL) <*jsales@pie.xtec.es*>
Tecnologías y Empresa
Pablo Hernández Medrano (Bluemat) <*pablohm@bluemat.biz*>
TIC y Turismo
Andrés Aguayo Maldonado, Antonio Guevara Plaza (Univ. de Málaga)
<*{aguayo, guevara}@lcc.uma.es*>
TIC para la Sanidad
Valentín Masero Vargas (DI-UNEX) <*vmasero@unex.es*>

Las opiniones expresadas por los autores son responsabilidad exclusiva de losmismos. *Novática* permite la reproducción de todos los artículos, salvo los marcados con© o *copyright*, debiéndose en todo caso citar su procedencia y enviar a *Novática* un ejemplar de la publicación.

Coordinación Editorial y Redacción Central (ATI Madrid)
Padilla 66, 3º, dcha., 28006 Madrid
Tlf.914029391; fax.913093685 <*novatica@ati.es*>
Composición, Edición y Redacción ATI Valencia
Reino de Valencia 23, 46005 Valencia
Tlf./fax 963330392 <*secreval@ati.es*>
Administración y Redacción ATI Cataluña
Via Laietana 41, 1º, 1ª, 08003 Barcelona
Tlf.934125235; fax 934127713 <*secregen@ati.es*>
Redacción ATI Andalucía
Isaac Newton, s/n, Ed. Sadiel, Isla Cartuja 41092 Sevilla
Tlf./fax 954460779 <*secreand@ati.es*>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza
Tlf./fax 976235181 <*secreara@ati.es*>
Redacción ATI Asturias-Cantabria <*gp-astucant@ati.es*>
Redacción ATI Castilla-La Mancha <*gp-clmancha@ati.es*>
Redacción ATI Galicia
Recinto Ferial s/n, 36540 Silleda (Pontevedra)
Tlf.986581413; fax 986580162 <*secregal@ati.es*>
Suscripción y Ventas: <*http://www.ati.es/novatica/interes.html*>, o en ATI Cataluña y ATI Madrid
Publicidad: Padilla 66, 3º, dcha., 28006 Madrid
Tlf.914029391; fax.913093685 <*novatica.publicidad@ati.es*>

Imprenta: 9·Impressió S.A., Juan de Austria 66, 08005 Barcelona.
Depósito Legal: B 15.154-1975
ISSN: 0211-2124; CODEN NOVAEC

Portada: Antonio Crespo Foix / © ATI 2003

novática
UPGRADE
Revista de la Asociación de Técnicos de Informática

MAYO · JUNIO 2003
163

SUMARIO

Monografía del próximo número:
«Ingeniería del Software: estado de un arte»

Seguridad

La confianza y la seguridad aspectos vitales para los servicios electrónicos

José A. Mañas Argemí
Depto. de Ingeniería de Sistemas Telemáticos, Universidad Politécnica de Madrid; socio de ATI

<jmanas@dit.upm.es>

Este artículo fue seleccionado para la monografía «e-AA.PP.» (*Novática* 162, marzo-abril de 2003) pero no pudo publicarse por falta de espacio.

Resumen: *en este artículo se pasa revista a conceptos aparentemente sencillos como "confianza" o "seguridad" y a su significado en un entorno como el actual en el que las personas físicas realizan transacciones a través de la Red, ya sea entre ellas, con empresas o con Administraciones Públicas. Se analiza la caracterización de estos individuos como sujetos activos y como sujetos pasivos que se mueven en este territorio con más o menos confianza y se responde a preguntas tales como ¿podemos fiarnos de la gente?, ¿de quién y de qué se fía la gente?*

Palabras clave: *confianza, firma electrónica, seguridad, servicios electrónicos.*

1. Introducción

El éxito técnico de Internet como medio de comunicación universal ha abierto enormes expectativas empresariales e individuales. Decimos que Internet es universal en el sentido de que es potencialmente capaz de llegar a lugares recónditos, como refleja la simpática frase «tener tono Internet». También es Internet universal en el sentido de ser neutral respecto de lo que se comunica por ella, privado, público, mercantil, administrativo o lúdico. Y esta sensación de tener un medio virgen para explotar ha lanzado atrevidas aventuras empresariales (punto.com) cuya fragilidad hemos apreciado en los últimos años, aunque probablemente el fracaso de las empresas más aventureras no implique la aniquilación del medio. ¿O sí? Porque parece cundir la sensación de que Internet sea territorio apache, zona peligrosa donde cada uno debe velar por su propia seguridad o está muerto. Así pues la pregunta: ¿es Internet digna de confianza?

Hay muchas expectativas en lo que se podría hacer, algunas puro cuento de la lechera y otras con un claro recorrido. Que las relaciones entre empresas se realicen por vía electrónica es un hecho aceptado, con muchos años a sus espaldas, y donde Internet no abre camino, sino que avanza un paso más en una dirección consolidada. Lo que sí es novedad relativamente reciente es la aparición de los individuos como actores de las transacciones electrónicas: el individuo que compra, el individuo que vende, el individuo que se relaciona como ciudadano con su administración pública. Estos individuos pueden ser consumidores de servicios o prestadores de servicios, en un sentido muy general, tanto de compra-venta como de intercambios de opinión o de bienes en formato electrónico (por ejemplo, música). No es cuestión aquí de entrar en las innumerables posibilidades de comportamiento, unas tradicionales, otras imprevisibles, como corresponde a sujetos creativos en terreno inexplorado.

Lo que aquí nos preocupa es la caracterización de estos individuos como sujetos activos y como sujetos pasivos que se mueven en este territorio con más o menos confianza, ofreciendo más o menos confianza a los demás. ¿Podemos fiarnos de la gente? ¿De quién y de qué se fía la gente?

2. ¿Qué es confianza?

Definir «confianza» no es trivial. ¿A qué se refiere la gente cuando habla de confianza? La misma Real Academia Española, punto obligado de partida, abre más puertas que cierra.

confianza. (De confiar).
1. Esperanza firme que se tiene de alguien o algo.
2. Seguridad que alguien tiene en sí mismo.
3. Presunción y vana opinión de sí mismo.
4. Ánimo, aliento, vigor para obrar.
5. Familiaridad (en el trato).
6. Familiaridad o libertad excesiva. Ú. m. en pl.
7. V. Abuso de confianza
8. Pacto o convenio hecho oculta y reservadamente entre dos o más personas, particularmente si son tratantes o del comercio.

de confianza
1. Dicho de una persona: Con quien se tiene trato íntimo o familiar.
2. Dicho de una persona: En quien se puede confiar.
3. Dicho de una cosa: Que posee las cualidades recomendables para el fin a que se destina.

en confianza
1. Confiadamente.
2. Con reserva e intimidad.

La confianza es un sustantivo, es un adjetivo y es parte de numerosas locuciones o formas de hablar. La confianza es un estado subjetivo, con más o menos fundamento, que nos lleva a tomar decisiones de actuación moduladas en su alcance y forma. Si algo no inspira confianza lo evitamos, o nos atrevemos timoratamente y con cautelas; en todo caso cuando no hay confianza no hay velocidad de crucero. Y al revés, cuando hay confianza nos lanzamos en la fe de que no habrá problemas o, si los hubiera, tendrían solución pronta y adecuada. Es en cierta medida la confianza la medida de la carencia de riesgo o, apurando las palabras, la medida del control del riesgo pues los sujetos convivimos con el riesgo bajo control (la conducción de coches) y huimos del riesgo descontrolado (la guerra).

En actividades tradicionales, la confianza es parte de la educación y convivimos inconscientemente con ella, tomando decisiones continuamente sin un análisis cerebral puntual. En territorios inexplorados, sin referentes claros (de confianza, y lamento el círculo vicioso), necesitamos hablar de los procesos de creación y destrucción de la confianza. Y como la confianza tiene un grado, tendremos que saber qué la incrementa y qué la socava.

No todos los sujetos parten del mismo punto. Tendremos visionarios, tendremos innovadores, tendremos una masa sin criterio y tendremos tradicionalistas. Y la diferencia es de tiempo, ritmo u oportunidad. Los visionarios aceptan un riesgo elevado, bien por inconsciencia, bien por una esperanza desmedida en el beneficio potencial. Las primeras incursiones en nuevos terrenos las protagonizan estos visionarios que exploran lo desconocido y emiten mensajes para los demás; mensajes en general muy subjetivos, bien ensalzando los éxitos (los padres de los nuevos servicios electrónicos) bien definiendo criterios de valoración (los académicos) bien generando criterio (los intelectuales). El futuro de una tecnología puede verse seriamente afectado por la experiencia y dotes de comunicación de este segmento de visionarios que pueden lanzar cohetes (fenómeno punto.com) o derruir la confianza. Es difícil recuperar la confianza tras una mala experiencia inicial.

Si los visionarios abren brecha, los innovadores están dispuestos a la aventura a poco fundamento que se le vea y pocos mensajes positivos lleguen de los visionarios. Firmes creyentes de que el que da primero tiene una ventaja competitiva, conscientes de que el tiempo es oro y aspirantes cautos a medallas; todos ellos avanzan rápidamente sobre el precario camino abierto por los visionarios que, a estas alturas, probablemente estén en otras aventuras.

No está claro quién escucha a los innovadores, porque la siguiente remesa de usuarios, la masa, se caracteriza por su pasividad (dicho sin ánimo despectivo; simplemente sus intereses inmediatos están en otra parte). Si el mensaje boca a boca animó a los innovadores es porque estaban esperando una excusa; pero la masa lo que necesita son incentivos o, en términos de comunicación, una comercialización de la actividad (o sea, marketing). En cada actividad concreta la masa suele ser mayoría, sus movimientos lentos, para bien o para mal, para mayor o menor confianza (que es lo que nos ocupa). La masa se mancha de aceite lentamente, y también lentamente se lava los fracasos.

Y nos queda el segmento que podríamos llamar tradicional a ultranza que presenta una resistencia activa a la innovación y sólo se apunta a «lo de toda la vida» porque cualquier otra aproximación a la nueva actividad le resulta sospechosa e indigna de confianza. Hay múltiples ejemplos en la historia de la ciencia en la que las nuevas teorías jamás han convencido a los viejos barones, llegando al extremo de requerir cambios generacionales para que triunfe la novedad. Desde Galileo hasta Einstein, por citar personas libres de toda sospecha de irracionalidad. Simplemente, no lo entienden.

La confianza social o sentir popular de la confianza que merece una innovación será la media ponderada (de alguna forma) de la confianza que impera en estos diferentes grupos sociales. Hay un efecto de arrastre (liderazgo) y hay un efecto de empuje (marketing), ambos coloreados por las experiencias buenas o malas que se van conociendo y aireando. Podemos decir que confianza es creer saber lo que va a ocurrir. El punto de partida es diferente para cada uno de los grupos caracterizados en los párrafos anteriores, punto a partir del cual crece o disminuye, al principio con fuertes oscilaciones,
y con el tiempo de forma perezosa.

La confianza crece con la satisfacción de las expectativas. Cuando uno cree que va a ocurrir esto, y es esto justamente lo que ocurre. Cada vez que alguien hace lo que promete, cada vez que funciona un servicio por Internet y, encima, funciona como parecía entenderse en las páginas de anuncio. Cada vez que un producto defectuoso se ve inmediatamente reemplazado por otro impecable. Cada vez que un servicio deficientemente prestado se ve prontamente reparado. Porque la confianza es mayor sin fallos; pero se rehabilita si son pocos y de pronta recuperación. Y la confianza crece cuando otros, desinteresadamente, hablan bien y te cuentan su experiencia positiva y te transmiten confianza. Los visionarios se animan solos, una minoría. Los innovadores se animan con los visionarios. A la masa hay que empujarla poco a poco. Y los recalcitrantes no salen en la foto.

La confianza disminuye con cada sorpresa, sobre todo con las negativas, con los fallos de las expectativas. Cuando uno visita una página web y le desconcierta un anuncio (*pop up)*, cuando un correo infecta con un virus; cuando una factura se sale del tiesto; cuando un proceso de compraventa no lleva a ningún término, o termina en un producto muy por debajo de las promesas, o de imposible reposición; cuando un servicio se presta incorrectamente o simplemente se suspende su ejecución a medio camino, incompleta.

En páginas web todos estamos hartos de anuncios emergentes, de propaganda agresiva, de correos basura, de enlaces engañosos, de enlaces rotos, de contenidos obsoletos, de informaciones no contrastadas, de un largo etcétera que se ve facilitado por la novedad y falta de regulación del medio, así como por la carencia de criterio de los usuarios junto con la ausencia de reglas y leyes que marquen la frontera entre lo correcto y lo incorrecto; es decir, porque no sabemos las reglas del juego y somos víctimas (o creemos serlo, que a efectos de la confianza hay poca diferencia) del medio o de la otra parte (que a efectos de la confianza, tampoco supone gran diferencia).

La confianza es pues subjetiva y hay que cuidarla y mimarla. La confianza es individual y colectiva y el que aspire a merecerla la necesita colectiva e individualmente. La confianza necesita referentes, marcas y saber popular, sobre todo en el segmento de la masa. Pero este es un argumento delicado porque no hacemos sino transferir la confianza en una marca a las cosas que la ostentan y nos lleva a hablar de transferencia de confianza y a hablar de origen de la confianza, lo que nos introduce en el bonito mundo de la lógica matemática y a tecnologías que instrumentan la transferencia fiable de confianza.

Y me gustaría acabar estos intentos de intentar contextualizar la confianza con una mención a la lógica y a las paradojas. La

confianza crece cuando el comportamiento es lógico; pero no en el sentido matemático, sino en el sentido visceral. Una página web que asegure que sólo dice mentiras (lo que es falso porque lo que dice es verdad) sólo encandilará a los matemáticos viciosos; pero seguro que espanta al común de los mortales que busca seguridad, no que le tomen el pelo (por muy meritoria del Nobel que sea la genialidad).

3. ¿Qué es seguridad?

Definir «seguridad» tampoco es trivial. Como en el caso del término «confianza», la misma Real Academia Española, abre más puertas que cierra. ¿A qué se refiere la gente cuando habla de seguridad?

seguridad. (Del lat. securitas, -atis).
1. Cualidad de seguro.
2. Certeza (conocimiento seguro y claro de algo).
3. Fianza u obligación de indemnidad a favor de alguien, regularmente en materia de intereses.

Seguridad jurídica.
1. Cualidad del ordenamiento jurídico, que implica la certeza de sus normas y, consiguientemente, la previsibilidad de su aplicación. En España es un principio constitucional. **Seguridad social.**
1. Organización estatal que se ocupa de atender determinadas necesidades económicas y sanitarias de los ciudadanos.

de seguridad.
1. Dicho de un ramo de la Administración Pública: Cuyo fin es el de velar por la seguridad de los ciudadanos. Agente de seguridad.
2. Dicho de un mecanismo: Que asegura algún buen funcionamiento, precaviendo que este falle, se frustre o se violente. Muelle, cerradura de seguridad.

No está la seguridad lejos de la confianza. De hecho es fácil decir que «seguridad es confianza en lo que va a ocurrir» y «confianza es estar seguro de lo que va a ocurrir», siendo la falta de sorpresa el fundamento común de ambas.

Pero mientras la confianza es terreno de trabajo de sicólogos y sociólogos, la seguridad aparece como «más técnica», afrontada por matemáticos e ingenieros que buscan modelos, tecnologías y soluciones para fundar y medir la seguridad de los productos y los sistemas. En la línea abierta por Sir Isaac Newton de que el tratamiento matemático permite modelar la realidad y por tanto simularla y predecir lo que va a ocurrir. No siempre con lógica cartesiana, sino a veces con razonamientos difusos; pero siempre con una capacidad de tratamiento analítico impersonal.

Un tratamiento analítico de moda es el análisis del riesgo como métrica del estado de seguridad. La idea es simple, cuantifiquemos e interpretemos. El qué es más complicado pues se trata de estimar estados indeseables (de inseguridad o de carencia de seguridad). Un análisis de riesgo parte de una catalogación de activos cuyo valor nos permite comparar, ordenar y priorizar. Catalogar activos es una tarea laboriosa, sobre todo si buscamos una aproximación detallada (en oposición a una aproximación holística). Cualquier proceso humano en general, y de servicios electrónicos en particular, está tan imbricado con otros procesos, actores y componentes que un planteamiento de laboratorio es a la vez imposible y necesario. Imposible porque toda simplificación falsea la realidad; y necesario para poder aprehender la realidad. No quiero perder al lector en disquisiciones; estoy hablando de que hay medios físicos (tan básicos como la electricidad), elementos humanos (tan necesarios de tomar en consideración como los administradores, los gerentes y los piratas informáticos), elementos informáticos (equipamiento, sistemas operativos, aplicativos de consumo, aplicaciones a medida, bases de datos, etc.) y procesos de negocio (relaciones entre empresas y con el cliente final). Y hasta aquí podemos saber lo que nos cuesta reponer un componente defectuoso (incluido despedir a un empleado y formar a otro nuevo), lo que nos cuesta una multa de la Agencia de Protección de Datos y el lucro cesante de una parada en la cadena de producción. Y aún así tendríamos que cuantificar activos intangibles como la credibilidad del mercado y la capacidad de existir tan siquiera. Quizás estamos hablando de cuantificar la confianza de la otra parte, con lo que entramos de nuevo en un círculo vicioso.

La valoración de activos puede ser muy precisa (valor económico) o puramente relativista para centrarnos en lo que percibimos como importante cuando no como crítico. Pero en todo caso no vamos a limitarnos a una visión pasiva, como espectadores, sino que vamos a entrar en un juego de identificación de posibles amenazas que se ciernen sobre aquellos activos y cuya materialización va a suponer un impacto a evaluar. Esta evaluación se suele llamar riesgo, se evalúa en base a estimaciones de la posibilidad de que ocurra y el daño que causaría sobre nuestros preciosos activos, para concluir en una métrica que puede ser económicamente precisa (pérdida estimada) o simplemente relativa (elementos críticos).

El hecho de llegar hasta aquí ya es un gran paso hacia una mayor confianza, en muchos frentes: del inversor en su aventura empresarial, del cliente en su proveedor, del socio en sus interlocutores, del ciudadano en su administración. ¿Por qué? Porque al otro lado tenemos un profesional que sabe lo que tiene entre manos.

Pero tampoco echemos las campanas al vuelo a la primera buena noticia. Ni el responsable de seguridad ni el auditor se van a contentar con tener una foto, salvo que esta fuera idílica. Típicamente habremos detectado una serie de puntos críticos de alto riesgo que requieren un tratamiento inmediato o un plan para afrontarlos. El tratamiento puede suponer la eliminación de la causa, o la suscripción de un seguro que nos ampare por si lo que pudiera ocurrir, ocurre. O bien entraremos en una dinámica de mitigación del riesgo, desplegando contramedidas. Hay contramedidas meramente organizativas (como controles de personal, conciliación de datos parciales,...) y otras de tipo técnico (control de acceso, criptografía,...) Hay contramedidas que dicta el sentido común o la práctica habitual del sector: se supone que las hemos tomado; no haberlo hecho será un serio motivo de desconfianza pues la otra parte se sentirá engañada en sus suposiciones. Hay contramedidas que impone la ley o reglamentos sectoriales; ahora ya no es sólo desconfianza puntual, sino que puede suponer una penalización económica que probablemente busque ser ejemplar pues minar la confianza en un sector o en la Justicia puede suponer un serio quebranto en la confianza colectiva.

En algunos casos las contramedidas no son ni baratas ni evidentes, y habrá que hacer más números hasta ver en que momento el coste de la contramedida se ve adecuadamente recompensado en la reducción del riesgo. Si eso no se consiguiera, más vale cambiar de negocio.

Es habitual que las empresas e instituciones alardeen de sus contramedidas de seguridad, dando por supuesto que han analizado sus riesgos y saben lo que hacen. El mensaje que se transmite es puro marketing: confíe en nosotros por todas estas razones.

Y para terminar esta sección, pongámonos en el otro lado y preguntémonos sobre cómo valorar ese mensaje de seguridad. ¿Cómo y en qué medida convertimos unas garantías de seguridad en una cuantía de confianza? Pues salvo los especialistas con tiempo libre para pensar y calibrarlo todo reposadamente (o sea, salvo nadie), todos los demás recurriremos a referentes sectoriales o generales. Hay sellos de calidad que se emiten tras una auditoría (que es un proceso pautado, reglamentado y ejecutado por expertos) y que reconocen formalmente el valor del estado de riesgo.

Y existen certificaciones emitidas por laboratorios, con el mismo fin. Informalmente podemos decir que se certifican productos y se auditan sistemas u organizaciones; pero no quisiera entrar en un terreno abonado a la polémica. Basta citar el esfuerzo de los Criterios Comunes de Certificación de la Seguridad para destacar la ímproba tarea que supone acordar a nivel mundial unos criterios objetivos de medición y aseguramiento de la calidad con el ánimo, evidentemente, de ser eficaces en un mundo que es cada día más global.

Aunque, digamos lo que digamos, y con todos los sellos y certificados que queramos lanzar al público para alimentar su confianza, esta se demuestra en última instancia andando, pues el tiempo pone a cada uno en su justo lugar y medida; lo que no pretende ser un mensaje derrotista, sino un aviso a navegantes de que hay que estar siempre alerta y que mientras las metodologías de análisis de riesgo y las certificaciones de seguridad consoliden su valor final, deberemos practicarlas de regularmente, incorporando nuevas funciones, amenazas y contramedidas.

4. Tecnología

No creo que se pueda escribir nada sobre confianza y seguridad sin mentar la tecnología, aunque el mundo tecnológico es actualmente más fácil que el de las sensaciones personales y sociales. Y no porque sea la tecnología sencilla, sino porque es predecible. Y ¿alguien no confía en las matemáticas?

La tecnología lo impregna todo. Los ordenadores (como activos de producción) cambiaron el mundo hace ya cincuenta años y son actualmente parte vital de los sistemas. Internet ha cambiado el perímetro de las organizaciones, abriendo un amplísimo y aún en exploración universo de amenazas remotas. La misma tecnología cierra muchas posibles amenazas con un buen diseño (componentes, compartimentos estancos, controles de acceso, etc.) y permite el contraataque reactivo para perseguir el delito.

Esta tecnología de comunicaciones y sistemas informáticos es la que constituye los servicios electrónicos en un sentido muy general y es en la que estamos construyendo la confianza. Los visionarios de los centros de investigación ya casi están en otras cosas y los innovadores viven tiempos duros de presupuestos y sorpresas. Estamos transitando hacia las masas que, como miden las encuestas, es cada vez más usuaria de Internet, al tiempo que va renqueando la confianza en el medio y en los compañeros de viaje. Hay, como en todas partes, buenos y malos; buenos (en los sentidos de buena intención y de competencia tecnológica) que van poco a poco contribuyendo a la confianza. Y hay malos (en los sentidos de mala intención e incompetentes tecnológicos) que la minan de forma espectacular.

El medio, Internet, es demasiado prometedor como para admitir que vaya a fracasar; pero el camino va a ser duro pues si el medio es débil a la hora de imponer calidades (todo es intercambiable por medio de bits), entonces necesitaremos construir la confianza en niveles superiores de servicio. Esto no es novedad para los ingenieros: hace siglos que se construye en el agua, en terrenos inconsistentes y en zonas de actividad sísmica. Simplemente hay que saber hacerlo.

5. Transferencia de confianza

Por esto, buscando seguridad sobre bases inseguras, no es de sorprender que la criptografía como tecnología y los servicios web como organización, busquen aunarse para ofrecer servicios de fiables donde la confianza que nos ofrecen algunos actores (pongamos el Banco de España) se pueda aplicar con garantías en los servicios (pongamos transferencias económicas).

Hay cosas sencillas como garantizar por medio de cifrado el secreto de las comunicaciones, lo que ya es un pilar importante pues crea una red (virtual) entre puntos de confianza. Los desarrollos de la criptografía en este terreno han sido no sólo espectaculares, sino además efectivos y estamos en la situación idílica del viejo Arquímedes: «*Dadme un punto de apoyo y moveré la Tierra*» que en criptografía se lee: «*dadme una clave segura y nadie interceptará vuestras comunicaciones*». El talón de Aquiles se llama ahora gestión de las claves.

Quizás la tecnología más inquietante, por su potencia, novedad y dificultad de uso práctico, sea la firma electrónica basada en la famosa criptografía de clave pública. La capacidad individual de crear firmas que protejan la integridad de los datos y sean imputables al signatario, es fácilmente asimilable al invento de los contratos por escrito que revolucionó el comercio hace miles de años. Alguno dirá, y no le falta razón, que consolidar el valor probatorio de un contrato escrito ha costado unos miles de años y aún es motivo diario de controversia judicial entre sujetos, empresas, instituciones e incluso estados. Habrá que tener paciencia y cuidar el crecimiento de tan potente herramienta. A veces el término «contrato» hay que entenderlo en un sentido muy general: documentos firmados, declaraciones, acuses de recibo, etc. Todo aquello que permita imputar al signatario a través de una fácil verificación de firma.

Porque la firma electrónica se puede verificar con cierta facilidad; facilidad que no es tanta si trabajamos fuera de línea (*off line signature verification*); pero sí es realmente fácil si contamos con la disponibilidad de las comunicaciones. La verificación puede ser humana (en relaciones interpersonales, comerciales o administrativas) o automática (en sistemas robotizados y procesos de negocio), lo que permiten diseñar procesos distribuidos (o sea, relaciones entre dos o más participantes).

El talón de Aquiles de la firma electrónica probablemente esté en su valoración: ¿qué valor tiene? o, en términos de riesgo ¿qué riesgo mitiga? ¿cuánto mitiga los riesgos que mitiga? ¿qué nuevos activos y nuevas amenazas introduce? ¿cuánto riesgo introduce? Son todas preguntas que se prestan a respuestas gloriosas (cuentos de la lechera o afirmaciones de escaso fundamento) por visionarios; pero que los innovadores han descubierto que cuesta lograr que esta tecnología valga efectivamente lo que promete teóricamente.

De nuevo hay que pedir paciencia y experiencia hasta que calibremos la aportación de la firma electrónica a la confianza. En esta línea se sitúa la legislación relativa a firma electrónica, buscando un terreno de juego fiable (seguridad jurídica) con fundamentos técnicos en el origen (prestadores acreditados de servicios de certificación) y en los medios (dispositivos seguros de firma).

6. Origen de confianza

La firma electrónica es un instrumento de transferencia de confianza. ¿En qué?

La primera aplicación que se ha anunciado con oropeles ha sido la certificación de identidad que se debe leer como que alguien conocedor de la identidad física o jurídica de otro, reconoce y firma para que así conste un certificado que podrá ser usado por el portador donde le convenga; es decir donde haya confianza y se lo admitan. Confianza en la tecnología y en el signatario.

Una segunda aplicación, aún en estado incipiente, es el aval de potestades. Lo mismo que una llave habilita al portador a abrir una puerta, o un cheque personal habilita a una persona a su cobro, o un poder habilita la firma de un apoderado para firmar por la empresa, los llamados certificados de atributos permiten al beneficiario alguna actividad electrónica. Hay certificados nominales que requieren el concurso de un certificado de identidad (por ejemplo el reconocimiento como médico colegiado) y hay certificados al portador (como una tarjeta de control de acceso al edificio). Todo tipo de variantes que en realidad no imponen limitaciones a la creatividad de los que diseñan procesos de negocio e imponen reglas de avance (la firma de tres miembros de los veinte miembros del consejo de seguridad; un millón de firmas de ciudadanos mayores de edad; ...).

La confianza en el signatario es muy interesante por cuanto un signatario ampliamente conocido puede avalar a un colectivo amplio de usuarios. Así Verisign certifica a millones de personas y servidores web en Internet, y el Estado Español planea certificar a todos los ciudadanos con el llamado DNI electrónico. Los colegios profesionales, las cámaras de comercio, las asociaciones internacionales, etc. etc. son posibles generadores de certificados de identidad o de capacidad. Y los ejemplos están elegidos para destacar la colisión que va a aparecer entre la certificación pública y la iniciativa privada, cuyo desarrollo ya veremos con el tiempo; pero de momento podemos centrarnos en la confianza que inspira el emisor del certificado (o proveedor de servicios de certificación si queremos reconocer que esto de los certificados es un conjunto de servicios y no un producto). La firma es mero vehículo.

Lo malo es que la firma del certificador es también electrónica y entramos en un círculo vicioso de aquellos de quien verifica al verificador. Pregunta que es tan básica y elemental como la de por qué nos fiamos de las conclusiones de las matemáticas: porque llevan años acertando prácticamente siempre. Es decir, confianza ganada día a día durante siglos. Lo malo es que ahora tendremos que fiarnos de los ordenadores, con un penoso historial: llevan decenas de años fallando“ todos los días.

No es por ser catastrofista; sólo destacar que la calidad de los sistemas, necesaria para confiar en la firma, aún es claramente mejorable y, probablemente, jamás llegue a la difícilmente superable cota alcanzada por las matemáticas; pero seguro que aprendemos a vivir en un mundo razonablemente seguro, simplemente cuando no haya sorpresas, los fallos no sean catástrofes, el riesgo esté bajo control y equilibremos el riesgo con el beneficio. Esta cuantificación justa de la confianza que nos merece la tecnología de firma electrónica es la que aún ignoramos.

7. Para concluir

Hemos intentado en los párrafos anteriores entender qué es la confianza, que es un valor percibido por los participantes y que modula la disponibilidad de las partes para involucrarse en un servicio electrónico. Sin confianza no hay servicios; pero la confianza depende de las personas y de los colectivos, hay que crearla, mimarla y empujarla.

Desde un planteamiento más técnico hemos visto cómo medir y certificar la seguridad y hemos divagado sobre algunas tecnologías que prometen sustentar una elevada confianza. Son tecnologías que se proponen a sí mismas como habilitadoras de los servicios electrónicos, y sin duda lo son; pero aún necesitan otro hervor. Hablamos de la prometedora firma electrónica y los difusos servicios de certificación de identidad y de capacidades.

Todo junto podemos resumirlo en que estamos viviendo unos tiempos interesantes y que con Internet muchas cosas ya no serán igual; siempre y cuando haya confianza en la seguridad que ofrece.