La seguridad vale más

Si hacemos un chequeo de salud en el ámbito de la seguridad de los sistemas de información y protección de datos personales, se puede comprobar claramente, teniendo presente lo cambiante y dinámico que es este sector, que existe una situación de madurez. Encontramos un despliegue de soluciones de seguridad extenso, un futuro visible en una orientación hacia la seguridad gestionada, una presencia permanente de las autoridades de protección de datos. A ello se suman nuevos retos en el horizonte como el Esquema Nacional de Seguridad, o la computación en "Cloud".

POR JOSÉ MANUEL LAPERAL

Todo ello es muy positivo y confirma el estado de movimiento continuo que vivimos y en el que debemos estar en el sector. Mucho ha cambiado desde aquel mensaje que se oía hace más de una década: "la LOPD no se puede cumplir".

Sí, hay madurez, pero sigamos atentos y reflexionemos. Hay más regulaciones que nunca, más medidas que nunca. Pero hagámonos dos preguntas:

¿En cuántas organizaciones conseguimos que se llegue a percibir además una aportación de valor por parte de la inversión en seguridad?

¿Sabemos salirnos de rol de inspección, control, fiscalización con el que es lógico partir en los inicios?

Porque parece razonable pensar que si vamos madurando y nos orientamos hacia una mejora continua, esa percepción debería cambiar. Estamos en un sector en el que el mercado aporta cada vez más nuevas soluciones, por tanto, es lógico esperar de ellas un valor adicional al de ser meras herramientas de inspección.

Suena bien, pero además, debemos observar que si no evolucionamos en el mensaje y nos mantenemos en el primer estadio, siempre nos costará (y cada vez más) obtener inversiones en nuevos recursos que si evolucionamos hacia un nuevo enfoque en el que destacar el valor. Pero es que además es cierto, hay valor en la seguridad.

Intentemos trabajar, en mensajes que deberían estar más presentes: "Puedo enseñarte qué ganas", frente a recalcar insistentemente lo que pierdes por su ausencia, que ya está muy oído.

Pensemos en algunos posibles ejemplos de puntos de apoyo, sobre los que crear nuevas líneas de mejora en relación a lo que la organización está ganando o debe ganar al invertir en seguridad:

La legislación ha resultado una valiosa palanca de activación. Reconozcamos que muchos logros aún no se habrían conseguido sin una presión regulatoria y la labor de las autoridades de protección de datos. Pero una vez puestos a ello ¿realmente necesito un legislador para que me indique que tengo que proteger un activo tan valioso como son mis datos? La experiencia demuestra que es bien posible que unos datos que la legislación identifica como de nivel básico, finalmente queden protegidos por las más altas medidas de seguridad al analizar que la continuidad saludable de mi organización depende de su buena conservación.

La seguridad arrastra inversión TIC, que a su vez se traduce en el despliegue de nuevos servicios. Por ejemplo, si nos fijamos en la protección de los datos de las personas en situaciones difíciles, razonamos con facilidad que este colectivo es probablemente uno de los receptores más necesitados de nuevos servicios, de los que no deberían quedar excluidos, pese a que inicialmente pudieran no manifestar un interés inicial

en esta materia. Por ejemplo, un dispositivo de radiofrecuencia que se utilice para el control del paciente, puede posteriormente utilizarse para servicios de localización o de actividades de entretenimiento para una persona de edad avanzada. Obviamente, la inversión en TIC, para la que la seguridad y protección es una palanca perfecta, permite abrir nuevas posibilidades de mejora de la calidad, asistencial, y nuevos servicios que mejoren la calidad de vida de las personas dependientes. Esa es la aportación de valor, orientarse hacia este objetivo es fundamental, ya que si no lo hacemos nos encontraremos que no estamos sino cumpliendo una normativa, no pensando en dar un servicio cada vez mejor a la persona que, probablemente, lo necesite más que ninguna otra.

Auditamos y al hacerlo conocemos. Este aspecto es de especial importancia. Al auditar el funcionamiento de un sistema de información obtenemos un conocimiento adicional que nunca nos dan los propios datos, aunque éstos sean explotados con técnicas de Inteligencia de Negocio (Business Intelligence). Los datos que almacenamos nos proporcionan información sobre una materia en concreto, pero es muy posible, que realmente sólo estemos obteniendo conocimiento de unos pocos. Al auditar los accesos a nuestro sistema, conseguimos saber cómo y en qué situaciones son realmente útiles los datos que almacenamos. Sabremos qué conjuntos de información son más frecuentemente consultados, en qué periodos de tiempo se hace, si hay estacionalidades en tipos de consultas, si éstas se corresponden con lo que cabía esperar. Tendremos la evidencia de qué datos no se consultan nunca (quizá no sean necesarios) y pueden ser identificados como de escaso interés. Hay un enorme potencial en la auditoría de los sistemas de información.

Mejora de la calidad de la prestación del servicio. En ocasiones ocurren desafortunadas situaciones en las que un proceso de investigación se ve invalidado porque se descubre que se ha producido una invención de pacientes para completar un ensayo clínico. Está claro que la protección de los datos tiene mucho que decir en esto, puesto que situaciones de tal naturaleza pueden evitarse si adoptamos medidas de seguridad en torno a la calidad de los mismos (trazabilidad del origen, prevención de alteraciones y no repudio). Ello redundará en beneficios tales como fármacos mucho más probados y de mayor calidad. Además, también podemos encontrar una ventaja que ofrecer al investigador, asegurando la protección de datos de su trabajo. Dando respuesta a esta lógica y humana preocupación ¿acaso no estamos potenciando con ello su celo investigador? Hay muchos ejemplos aplicables.

Estos nuevos enfoques estarán cada vez más presentes en nuevos retos y soluciones que surgirán en el ámbito de la seguridad, y especialmente, cuando miramos hacia el entorno sanitario.

No siendo algo del todo nuevo, últimamente se habla cada vez más de la necesidad y los beneficios de la creación de un espacio socio-sanitario. En la realidad actual, la primera lectura que hacemos de esto es la apertura de los sistemas de información sanitarios hacia el ámbito social, lo que supone, un tremendo impacto en el control del acceso a la información. Nos vuelve de nuevo el mensaje de control, de auditor de regulador, de enormes costes. Un nuevo embrollo con el que lidiar.

Pero, ¿es esto todo? Démosle la vuelta más a ver si mejora. Pensemos si los beneficios que podemos recoger de la Libre Elección de Médico, por poner un ejemplo, en términos de ahorro costes, mejora la prestación asistencial, nuevos servicios y otros muchos, se pueden alcanzar sin un gran soporte en materia de seguridad, que garantice que, no sólo se mantiene la protección de los derechos del ciudadano, sino que los servicios se presten con adecuada solvencia (leamos autenticación y control de acceso) y efectividad (leamos disponibilidad, etc.)

Una vez más, estamos en la situación económica de feroz competencia de recursos en la que las nuevas iniciativas son tremendamente difíciles de llevar adelante, como todos conocemos. Pero si contamos con el activador de la necesaria inversión en seguridad como ya hemos comentado, y su capacidad tractora, tenemos un puente con el que empezar a avanzar hacia nuestro objetivos de mejora asistencial.

Ya tenemos un nuevo lema sobre el que trabajar: “La seguridad vale mucho, la seguridad vale más”.

José Manuel Laperal González
Responsable de Seguridad
Sanidad - Agencia ICM -
Comunidad de Madrid