DAVID PELÁEZ CHAPADO
DIRECTOR DE TECNOLOGÍA Y ORGANIZACIÓN DE ARTAI

Claves para la digitalización segura de una correduría

Cuando una compañía, independientemente de su volumen de facturación, sector de actividad o modelo de negocio, se plantea la necesidad de avanzar en sus herramientas digitales puede toparse con riesgos y peligros importantes:

1. La urgencia. Este tipo de iniciativas suelen venir condicionadas por necesidades imperiosas de nuestros clientes, partners y en general de los stakeholders con los que nos relacionamos en nuestro negocio. Las prisas son malas consejeras de la innovación.

2. La visión integrada. Se suelen abordar estas iniciativas de forma independiente, según las necesidades concretas de las distintas áreas de la empresa (financiera, RR.HH, comercial, ...), en lugar de establecer un plan coordinado que permita establecer modelos de gestión que, a la vez, favorezcan la interoperabilidad entre los sistemas.

3. La seguridad tecnológica. Es, sin lugar a dudas, el más peligroso, por su impacto (puede acabar literalmente con nuestra compañía) y porque es como esas terribles enfermedades que solo muestran su cara cuando ya es demasiado tarde.

De todas las dificultades y problemas que pueden surgir en un proceso de digitalización el único que puede acabar con nuestra empresa de un plumazo, es la gestión de la seguridad tecnológica, ciber seguridad o seguridad lógica..., que sería el término a mi juicio más acertado.

Ejemplos hay y los vivimos diariamente: basta con leer cualquier diario o ver cualquier noticiario para observar situaciones de altísimo impacto derivadas de ineficiencias en el ámbito de la seguridad lógica. Compañías internacionales de primer nivel, multinacionales con volúmenes de negocio gigantescos, han sufrido situaciones de grave impacto en su actividad, y por tanto en su cuenta de resultados, simplemente por no tener bien estructurada su seguridad lógica, o por no prestarle toda la atención que merece.

Y eso, en mi opinión, y contra lo generalmente considerado, no es tarea únicamente del Área de Tecnología de la empresa sino de todos los que pertenecen a ella.

> "Gestionar adecuadamente la seguridad lógica de nuestros datos es algo inexcusable. Y en ningún caso debe ser visto como un engorro o una cortapisa a la innovación en nuestras organizaciones, sino como una parte más, intrínseca e indisoluble del proceso de evolución"

PRINCIPALES HIGHLIGHTS

Aunque el ámbito ciberseguridad es tan amplio y prolijo, con tantos matices e implicaciones, que hace casi imposible redactar unas líneas

mínimamente explicables en este breve artículo, algunos de los principales highlights que a mi juicio deben resaltarse son:

1 La ciberseguridad o mejor dicho, la gestión de la seguridad lógica, es tarea de TODOS los miembros de la compañía. Y así debe ser entendido por toda la organización. La concienciación, la formación, la implicación de todos, es imprescindible

2 Es importante, casi imprescindible, apoyarse, en partners que nos ayuden, dado el nivel de especificidad y variabilidad constante en este ámbito. En este sentido, la elección de ese tercero que nos ayude es crítica y debe adecuarse sobre todo en filosofía a nuestra compañía.

3 Visión cross. De la misma forma que ante cualquier iniciativa, debemos implicar a las áreas de servicio (RR. HH, compliance, marketing,...), debemos tener en mente siempre la seguridad lógica. Nuestras empresas, corredurías de seguros, son empresas de "conocimiento", en las que "fabricamos y comercializamos información de valor añadido"; por lo tanto, el cuidado de la seguridad de nuestro "producto" debe ser algo a tener en cuenta permanentemente, casi como un mantra.

> "De todas las dificultades y problemas que pueden surgir en un proceso de digitalización el único que puede acabar con nuestra empresa de un plumazo es la gestión de la seguridad tecnológica"

4 Nunca estaremos totalmente seguros. Es imposible. Decía un gran general, que nunca se podrá tener una muralla lo suficientemente alta y gruesa que no pueda ser derribada por un cañón (un tal Napoleón...) y es verdad. Por mucha inversión, sistemas, dispositivos, protocolos y demás medidas que despeguemos, siempre podrá haber alguien que con tiempo y recursos pueda entrar en nuestros sistemas. Pero debemos aplicar siempre el principio de "pérdida asumible". Debemos poner todos los medios a nuestro alcance, dentro de la razonabilidad, que hagan tan complejo y difícil desbordar nuestras defensas que al final "los malos" se planteen si les compensa. Por ello, no debemos dejar de desplegar estas medidas con total rigurosidad. Es imprescindible.

Para finalizar, compartir que la seguridad lógica forma parte, una de las más importantes sin duda, del proceso de digitalización Y este es inexcusable en nuestra industria. Por lo tanto, gestionar adecuadamente la seguridad lógica de nuestros datos, también lo es. Y en ningún caso debe ser vista como un engorro o una cortapisa a la innovación en nuestras organizaciones, sino como una parte más, intrínseca e indisoluble del proceso de evolución, que es ya imparable \