Nº500 - AÑO 2021

aseguradores

ENTREVISTAS

José Luis Ferré
CEO de Allianz

CECAS

Formación: muy lejos de Europa

REPORTAJE

Transformación digital: ¿todo ventajas?

En el punto de mira de los ciberdelincuentes


Seguro de Salud
Protege tu salud
Desde el primer día cuentas con **programas preventivos** para cuidarte incluso antes de que puedas necesitarlo.
Know You Can
ADOP
Patrocinador del Equipo Paralímpico Español
Entra e infórmate | axa.es
Cobertura otorgada por AXA Seguros Generales.

sumario

Acceda a la revista en **formato digital**

Las empresas, en el punto de mira de los ciberdelincuentes

La pandemia ha sido un auténtico catalizador del proceso de transformación digital que estaba afrontando la sociedad en los últimos años. Esta digitalización tiene numerosas ventajas, pero también supone nuevos riesgos para las empresas.

"El robo de datos es el tipo de ataque que más crece y se convierte en el más peligroso"

La crisis generada por la COVID-19 nos obligó a cambiar todo: trabajo, estudios, compras, ocio, relación con amigos y familiares... De la noche a la mañana, tuvimos que buscar la manera de seguir haciendo todas estas cosas en la distancia. Tras los primeros instantes de desconcierto, nos dimos cuenta de que las herramientas digitales nos permitían dar respuesta a muchas de estas necesidades. Sin embargo, tuvimos que realizar esta transición de forma urgente, dejando la seguridad en un segundo plano en algunas ocasiones. Los ciberdelincuentes, atentos a las debilidades de sus víctimas, han visto su oportunidad. Según CheckPoint, los ciberataques semanales a empresas en España han aumentado un 61% interanual.

Así pues, una vez realizado el esfuerzo para afrontar la transformación digital, es imprescindible revisar las políticas de seguridad y reforzar todos los mecanismos, puesto que un ataque cibernético puede tener un enorme impacto. Y no sólo económico (paralización de actividad, inutilización de equipos, sanciones impuestas por la Agencia de Protección de Datos), ya que un ataque también puede tener otras consecuencias, como la pérdida de información de gran valor y, sobre todo, una crisis reputacional.

Veamos cuáles son los ciberataques más habituales en el ámbito corporativo y algunos ejemplos.

Ransomware

Es el tipo de malware que más está creciendo en los últimos años. Además, es el ciberriesgo más peligroso, debido al impacto que puede tener en la víctima. La infección se suele producir al recibir un correo con un archivo contaminado o hacer clic en una dirección URL comprometida. Esto desencadena el cifrado de los archivos, recibiendo una 'nota de rescate' de los ciberdelincuentes con las instrucciones para recuperar los archivos a cambio de un pago, que normalmente suele ser en bitcóins.

Supone una importante amenaza para las empresas, que tienen una intensa relación a través del correo electrónico con clientes y proveedores, por lo que es fácil que abran e-mails procedentes de personas que no conocen y que hagan clic en archivos camuflados como facturas, presupuestos, fotos, documentación técnica, etc.

El primer gran ejemplo de ransomware a escala planetaria llegó con Wannacry, que en España afectó a empresas como Telefónica, Iberdrola o Gas Natural. En el último año y medio se han producido casos muy notables. Uno de ellos fue el de Colonial Pipeline, operador de un importante oleoducto de Estados Unidos, sufrió un ataque ransomware que detuvo su actividad. La compañía reconoció el pago de 4,4 millones de euros de rescate.

En los últimos meses se está viendo una nueva modalidad de ataques ransomware de doble extorsión. Los ciberdelincuentes ya no sólo cifran la información y piden un rescate, sino que también roban los datos y amenazan con exfiltrarlos si no se paga. Un ejemplo es el ataque a The Phone House en abril, que acabó con la publicación en la 'dark web' de 100 GB de datos —nombre, DNI, datos bancarios, IMEI, correo electrónico, teléfono, dirección, seguros de móviles, etc.— de 13 millones de clientes.

Incluso hay ataques de triple extorsión, en los que se reclama a los clientes de la empresa afectada que paguen una cantidad menor si no quieren que sus datos sean publicados. Éste fue el caso de la clínica de fisioterapia finlandesa Vastaamo. Y otra modalidad de triple extorsión consiste en amenazar a la empresa afectada con realizar un ataque de denegación de servicios que paralice su actividad si no pagan el rescate.

Cabe destacar que el importe medio de los rescates está creciendo desmesuradamente y ya supera los 300.000 dólares (+171% interanual), según el informe '2021 Unit 42 Ransomware Threat Report', elaborado por Palo Alto Networsks

Phishing

Es uno de los malwares más frecuentes. Consiste en la suplantación de la identidad de una persona, marca o empresa conocida con el fin de generar confianza en la víctima para recopilar información confidencial, como credenciales de acceso, claves, etc. Suele llegar a través del correo electrónico, aunque también por SMS o aplicaciones de mensajería instantánea, como WhatsApp.

Se trata de mensajes con un enlace en el que se invita a la víctima a hacer clic, redirigiéndola a una web fraudulenta donde ha de introducir sus datos. Normalmente, se emplea para robar credenciales y acceder a cuentas bancarias, aunque también puede combinarse con ransomware, troyanos bancarios, etc.

BUENAS PRÁCTICAS DE CIBERSEGURIDAD

El "Decálogo de buenas practicas de ciberseguridad para pymes" de Unespa recoge las 10 principales recomendaciones:

1. Definir y aplicar una política de ciberseguridad.
2. Asegurar y proteger los datos e información.
3. Utilizar las redes de forma segura.
4. Protegerse contra el malware.
5. Utilizar el correo electrónico de forma segura.
6. Asegurar el acceso remoto y físico a sistemas y equipos.
7. Proteger los dispositivos móviles y la información que contienen.
8. Mantener las aplicaciones actualizadas.
9. Diseñar y poner en práctica un plan de respuesta a incidentes.
10. Concienciar, informar y formar a todo el personal de la compañía.

Los expertos hacen hincapié en tres aspectos clave. Por un lado, controlar los accesos, empleando sistemas de verificación de la identidad robustos y concediendo únicamente los permisos imprescindibles en función del perfil de cada usuario. Es recomendable evolucionar desde el clásico modelo de autenticación de usuario y contraseña hacia sistemas de doble o múltiple autenticación, por ejemplo. Por otra parte, se aconseja realizar copias de seguridad de forma periódica, con el fin de minimizar el impacto y retomar la actividad lo antes posible en caso de ataque. Por último, es fundamental extremar las precauciones en el correo electrónico, las mayoría de los ataques llegan por este canal.

Por ejemplo, durante los primeros meses de confinamiento se puso en marcha una campaña de phishing dirigida a pymes y autónomos. Los ciberdelincuentes disfrazaban su ataque suplantando a la Agencia Tributaria y reclamaban supuestas facturas no declaradas, aprovechando la confusión en torno a los ERTE vinculados a la pandemia. Dichos mensajes procedían de una dirección terminada en @correo.aeat.es, por lo que era fácil caer en el engaño.

La generalización del comercio electrónico durante el confinamiento también provocó el auge de campañas de phishing que suplantaban a Correos u otros operadores logísticos. Las víctimas recibían un SMS o correo electrónico con el enlace a una web fraudulenta, donde debían aportar los datos de su tarjeta bancaria si querían recibir un supuesto paquete retenido. Muchas entidades bancarias también sufren la suplantación de sus marcas en campañas de phishing que cada vez son más sofisticadas y difíciles de distinguir.

Suplantación de identidad

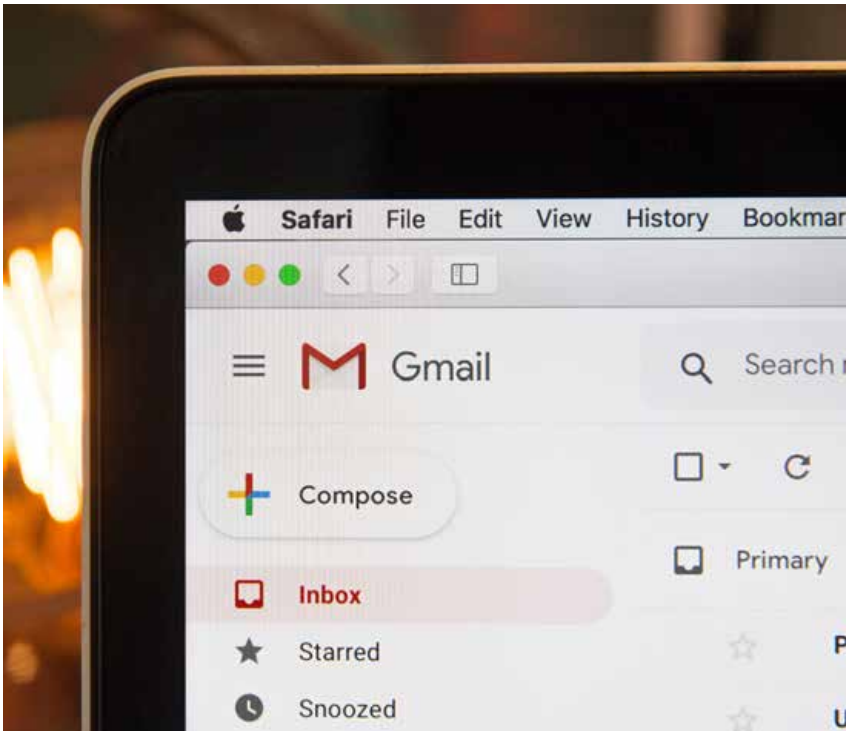
En este tipo de ataques, la víctima recibe un e-mail enviado desde una cuenta de correo de un directivo de la propia empresa o de algún proveedor, suplantando su identidad. Este mensaje suele ir destinado a una persona con capacidad de realizar transferencias o que dispone de información valiosa. El objetivo suele ser conseguir que se realice una transferencia para cerrar una operación ficticia urgentemente, sin que el afectado tenga tiempo de verificar la orden. Este tipo de ataque suele provenir de servidores de correo legítimos o desde un e-mail sustraído previamente, por lo que la víctima no desconfía de ella. En ocasiones, las credenciales de las cuentas de correo empleadas han sido obtenidas en la 'dark web'.

Un paso más allá están los denominados ataques 'deep fake', que emplean inteligencia artificial para suplantar a una persona. Por ejemplo, un grupo de ciberdelincuentes consiguió robar 35 millones de dólares a un banco de Emiratos Árabes Unidos clonando la voz del directivo de una compañía conocido por la entidad. Los atacantes llamaron por teléfono al banco para ordenar la transacción, acompañando la petición con correos electrónicos de la empresa y del abogado que se suponía que iba a ejercer de intermediario en la operación.

Denegación de servicios

Se trata de los denominados ataques DoS y DDoS. Con ellos se busca inhabilitar un servidor, un servicio o una infraestructura. El ataque se puede materializar por la saturación del ancho de banda del servidor de la víctima para dejarlo 'fuera de juego' o agotando los recursos del sistema de la máquina, evitando que pueda responder al tráfico legítimo. La consecuencia es una paralización total de la actividad hasta que se logra restablecer la situación a la normalidad.

Según el informe 'Threat Intelligence Report' de Netscout, en la primera mitad del 2021 se han registrado 5,4 millones de ataques DDoS, con un crecimiento del 11% interanual. Normalmente, este tipo de ataques se dirige a proveedores de servicios de internet, como Google Cloud, Amazon Web Services, Microsoft Azure, GitHub,



"Hay que extremar las precauciones con el correo electrónico pues la mayoría de ataques llegan por este canal"

etc., por lo que perjudican a todos sus clientes si tienen éxito.

Amenaza Avanzada Persistente

Una Amenaza Avanzada Persistente (APT) se dirige a un objetivo específico. Intenta comprometer sistemas que albergan información valiosa, que suelen estar bien protegidos. Para ello, los ciberdelincuentes atacan a objetivos más sencillos, como proveedores en su cadena de suministro o empleados de responsabilidad menor, que tal vez utilicen la misma red. Desde ahí, los hackers se mueven lateralmente hasta llegar al objetivo final.

El ejemplo más conocido es el ataque del año pasado contra SolarWinds, que expuso la información de alrededor de 18.000 organizaciones de todo el mundo, incluyendo a la mayoría de compañías de la lista Fortune 500 y a algunas de agencias del gobierno de Estados Unidos, como la NASA o el Pentágono. Los ciberdelincuentes aprovecharon la vulnerabilidad de una plataforma tecnológica de SolarWinds para infiltrarse en los sistemas de las empresas y entidades públicas que usaban sus servicios. Todavía no se conoce el alcance del ataque y la información que quedó comprometida, puesto que las organizaciones afectadas no se han pronunciado.

Brechas de datos

Son incidentes que ponen al descubierto los datos de los usuarios. No sólo tienen un coste económico, sino que pueden afectar gravemente a la reputación de una empresa y a la privacidad del cliente. Además, hay que recordar que el Reglamento General de Protección de Datos contempla importantes sanciones ante este tipo de situaciones.

No siempre se trata de incidentes protagonizados por ciberdelincuentes, sino que a veces pueden ser denuncias realizadas por hackers éticos. Esto fue lo que sucedió, por ejemplo, el pasado mes de julio, cuando uno de estos grupos advirtió acerca de una brecha detectada en el sistema de autocita de la Generalitat de Cataluña para la vacuna contra la COVID-19. Días antes, la Comunidad de Madrid sufrió un incidente similar en su sistema de autocita, exponiendo datos de sus ciudadanos, como el brazo en el que se vacunaron, cuándo y dónde recibieron sus dosis o qué tipo de vacuna se les inyectó.

Quizá la brecha de datos que más revuelo causó fue la que afectó a la plataforma de relaciones extramatrimoniales Ashley Madison en 2015. Un grupo de hackers exfiltró los datos personales y financieros de sus más de 37 millones de clientes, algunos de ellos muy conocidos. La empresa tuvo que pagar 11,2 millones de dólares para resolver la demanda colectiva presentada por sus clientes en Estados Unidos. Además, sufrió un daño reputacional irreparable.

Autoconfianza

La seguridad de sentirse bien acompañado en cada trayecto.

Con el Seguro de Allianz auto, además de las coberturas que necesitas, te ofrecemos una extensa red de talleres excelentes, la recogida y entrega de tu vehículo a domicilio, la peritación 100% digital y el acompañamiento personalizado de nuestros más de 8.500 agentes y corredores. Esto es... Autoconfianza.

ALLIANZ **auto**. Déjanos apoyarte.

allianz.es

Ciberriesgos, un nuevo escenario

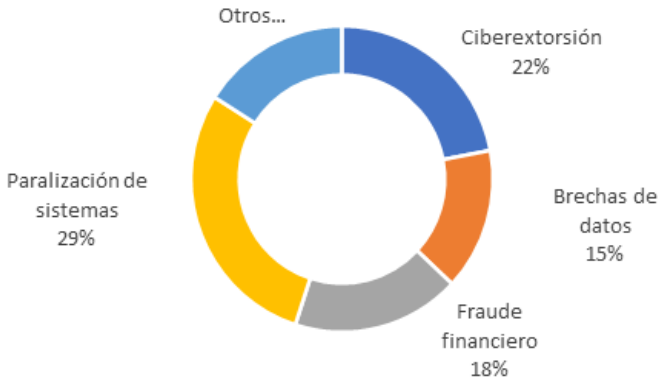
Los ciberriesgos no son una posibilidad, son ya una realidad tanto para los particulares como para las empresas. Afrontamos un nuevo escenario con un número creciente de ciberdelincuentes. ¿Qué se puede hacer ante esta situación? Sin duda, es indispensable establecer medidas de seguridad en los sistemas informáticos y de comunicaciones pero, para los expertos, el Seguro es la única herramienta útil, que se valora sobre todo cuando llega el siniestro.

En una sociedad tan digitalizada, es llamativa la escasa conciencia que hay de los riegos cibernéticos. El ciudadano particular los ve como algo lejano. No es consciente de que dispone de una herramienta enormemente potente, su móvil, que le permite acceder al ciberespacio pero que, a la vez, representa una puerta de entrada a sus propios datos. Y en el ámbito empresarial, a pesar de que hay ya mayor información sobre estos riesgos, ésta no siempre se traslada a una inversión real en seguridad.

A muchos analistas les sorprende comprobar el elevado número de empresas que todavía no han establecido controles de seguridad rigurosos en cuestiones básicas como el acceso al correo electrónico o a las operaciones bancarias. Y es que, a día de hoy, todavía a buena parte de los empresarios les cuesta percibir que prácticamente todos los riesgos del mundo físico tienen su reflejo en el ciberespacio. Para Óscar Sanz, director técnico y responsable de la Actividad de Distribución en la correduría Kalibo, es fácil que el cliente reconozca con total claridad las consecuencias de que su patrimonio desaparezca como resultado de un incendio, "pero aún no ve qué puede ocurrir si sus datos y su información desaparecen o, peor aún, caen en manos inadecuadas. Sin darnos cuenta, gran parte de nuestro patrimonio, el que tiene valor económico y puede afectar a los balances, ha pasado a residir en el ciberespacio: nuestros proyectos, nuestras ideas, la información financiera y contable, los datos de los clientes... el escenario de vulnerabilidades ha cambiado radicalmente".

Como en otro tipo de riesgos, la percepción real del mismo se produce al final de la forma más abrupta: cuando ocurre el siniestro. De esta forma, los empresarios más receptivos al establecimiento de medidas de seguridad son aquellos que han sufrido ya un ataque o que han conocido, de forma muy cercana, a quien lo ha padecido. Afortunadamente, cada vez son más los que confían la elaboración de un entorno de seguridad a profesionales del sector TIC.

DISTRIBUCIÓN DE LOS CIBERSINIESTROS EN EUROPA 1º SEMESTRE 2021



"Sorprende el número de empresas que todavía no han establecido controles de seguridad en algo tan básico como el correo electrónico"

Comunicación fluida

Llama la atención comprobar, en muchas ocasiones, cómo el empresario se escuda en que ya cuenta con un excelente servicio informático para no contratar un seguro. Un sinsentido: sería lo mismo que renunciar al seguro contra el robo porque se dispone de un buen sistema de alarma.

El entorno ideal de la ciberseguridad sería aquel que cuenta con un excelente servicio de consultoría en la materia y, además, con un aseguramiento óptimo en ciberriesgos. Los aseguradores deberían ser exigentes e incluso llevar a cabo una labor didáctica en cuanto al establecimiento de unos estándares mínimos de seguridad cibernética, a la vez que sería deseable que los consultores en materia de seguridad aconsejaran a sus clientes la contratación de seguros de ciberriesgos como la vía óptima de completar su protección. "El establecimiento de medidas de seguridad en los sistemas informáticos y de comunicaciones es absolutamente imprescindible, pero el seguro es la única herramienta útil cuando, pese a todo, el siniestro llega", remarca Sanz.

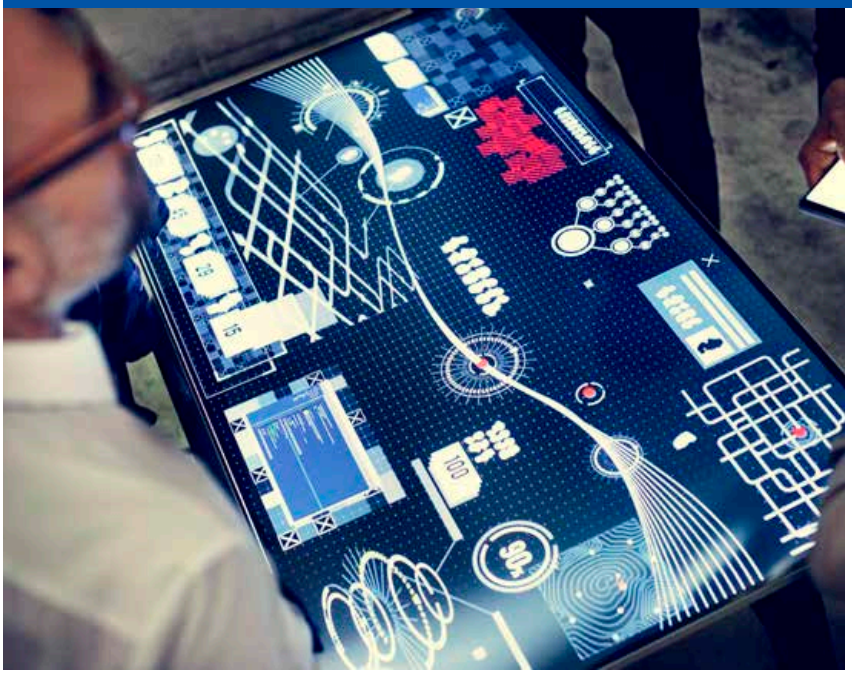
LAS GRANDES NO DUDAN Y LO DEMANDAN

¿Qué suele responder una empresa cuando se le ofrece un seguro de ciber?

- **Las grandes no dudan y lo demandan**. Suelen tener muy claro lo que les preocupa y quieren, aunque no suelen conocer qué les ofrece el seguro. Normalmente, les sorprende positivamente el nivel de madurez de los productos y el amplísimo carácter de la cobertura. En la contratación suelen intervenir departamentos informáticos internos que conocen bien la problemática y con los que es más fácil entenderse.

- **Medianas y pequeñas: ven el riesgo como algo remoto**. Su reacción inicial suele ser de escepticismo y de lejanía. Con ellas suelen funcionar muy bien los ejemplos concretos y reales. En la contratación el mayor problema es obtener la información pues la seguridad cibernética no suele ser una prioridad y suele ser difícil conocer el entorno tecnológico.

- **Un arma comercial muy potente para las empresas más pequeñas son los cuestionarios/solicitudes que dan paso a una contratación casi automática.** Entrañan un evidente peligro: las respuestas no suelen ser consecuencia de un análisis real de cada cuestión planteada. La labor, conocimiento y el sentido común del corredor son clave.



Riesgo real y creciente

El seguro de ciberriesgos está teniendo una lenta penetración en el mundo empresarial, pero esta es muy escasa en el ámbito particular. Y eso que hablamos de un riesgo real y creciente. Las aseguradoras especializadas y muchas generalistas han visto el potencial y se han lanzado a un mercado que, aparentemente, puede ser muy suculento a medio plazo.

Como muestra un botón: las consultas relacionadas con seguros de riesgos cibernéticos se han disparado el último año debido, principalmente, al aumento de ataques contra pymes durante la pandemia.

TRES 'ERRES' QUE SUBEN EL PRECIO

1. El enorme crecimiento del robo de datos, o *ransomware*, un 170% en todo el mundo en los dos últimos años (2019 y 2020). Además, el coste de los rescates también ha subido un 400%.

2. *Rates* o tarifas que no han dejado de subir para que las aseguradoras puedan afrontar esta siniestralidad. Desde 2019 la subida ha sido del 50%

3. Regulación: Cambios constantes cada vez con mayor exigencias que s etraducen en aumento de costes

Solo en España, el año pasado se produjeron 40.000 casos de ciberataques al día, siendo las pymes las más afectadas (recibieron el 70% de los ataques), según datos del Instituto Nacional de Ciberseguridad (INCIBE). El motivo principal es su vulnerabilidad: no suelen contar con buenas infraestructuras digitales y en ellas aumentan los errores humanos por la falta de formación de sus empleados en la materia y la ausencia de medidas de ciberseguridad durante el teletrabajo. El coste medio de los ataques a las pymes asciende a 35.000 euros.

Los ciberseguros generan un volumen de negocio de unos 500 millones de euros en España, con un aumento sostenido de dos dígitos.

No es una 'commodity'

Para el corredor, el seguro de ciberriesgos no es una 'commodity'. Es un producto que exige un conocimiento profundo del cliente, de sus peculiaridades y necesidades. El mercado dispone de opciones que permiten cierta personalización de las coberturas en función de cada caso y la industria debe aprovechar esa flexibilidad. Ahora bien, aunque es cierto que existe un alto grado de madurez en cuanto a coberturas de ciberriesgo para el mundo empresarial, no hay que engañarse: lo que hasta ahora ha hecho la mayoría del sector es trasladar al mundo virtual las soluciones que ya existían en el mundo físico. Para Óscar Sanz el esquema de coberturas de la típica póliza de ciberriesgos reproduce el de una póliza Multirriesgo, "con una garantía sobre el propio patrimonio -que se traduce en la recuperación de datos o en la extorsión cibernética-, una protección de la cuenta de resultados a través de la Pérdida de Beneficios y una potente garantía de Responsabilidad Civil".

Reconoce también que las aseguradoras más avanzadas están empezando a incluir coberturas como el fraude tecnológico o los ataques mediante técnicas de ingeniería social. Eso sí, para acceder a este tipo de garantías, se exige "unos estándares de seguridad medios-altos, algo que es totalmente coherente, y que, de alguna manera, forma parte de la labor didáctica de los aseguradores". En todo caso, concluye, "la clave de estos seguros es contar con un excelente servicio de respuesta a incidentes, algo donde las compañías especialistas han echado el resto y han conseguido contar con las consultoras de más alto nivel para prestar este servicio".

Quedarse fuera del seguro

Es cierto que la pandemia ha traído un endurecimiento de las políticas de suscripción y de las primas, aunque no hay que olvidar

ASÍ ENTRAN LOS CIBERDELINCUENTES

- A través de ingeniería social (como el phishing)
- Por emails corporativos
- A través de malware
- Por fallos en la configuración de los sistemas
- DDoS (ataques de red distribuidos)
- Por vulnerabilidades en el software
- Mediante credenciales robadas o comprometidas
- Por terceros o cadena de suministro
- A través de protocolos de acceso remoto
- Mediante fuerza bruta

Óscar Sanz (Kalibo): "La clave de estos seguros es contar con un excelente servicio de respuesta a incidentes"

que se partía de una base muy baja, por lo que, sigue existiendo una oferta "asequible". Con todo, se reconoce la creciente dificultad de algunas actividades económicas para poder encontrar cobertura de ciberriesgos y, lo que es preocupante, su posicionamiento fuera del seguro. A actividades que tradicionalmente no gustaban, como la generación de energía, se ha unido recientemente el mundo sanitario. A juicio del directivo de Kalibo, esta situación se está convirtiendo en un problema grave y "como sector asegurador no podemos dejar fuera de cobertura ámbitos de actividad tan críticos como el energético o el sanitario. Creo que tenemos la obligación, incluso moral, de buscar fórmulas de aseguramiento para esa tipología de riesgos".

En lo que se refiere a los ciudadanos particulares, la situación de la oferta aseguradora en ciberriegos es distinta: es escasa en número y limitada en prestaciones. Los tímidos intentos que han aparecido más bien parten de la base de alguna herramienta tecnológica, como antivirus, firewalls... con algún añadido casi anecdótico que no parecen verdaderos productos aseguradores. "No quiero decir que no sean productos válidos; por supuesto que lo son y pueden proporcionar un alto grado de prestaciones a un precio muy competitivo. A lo que me refiero es a que todavía no ha surgido un producto asegurador que sea capaz de trasladar a los particulares un nivel de protección similar al que existe en las empresas. Es una tarea compleja, pero existe un amplísimo campo comercial para quien se atreva a dar el primer paso", afirma Óscar Sanz.

codeoscopic

Creamos tecnología que transforma el sector seguros

- Multitarificación
- ERP
- Analítica de datos
- Gestión de siniestros
- Gerencia de riesgos
- Business intelligence

#lafuerzadelgrupo

www.codeoscopic.com

codeoscopic avant2 SALES MANAGER tesis BROKER MANAGER versus INSURANCE DATA sacs innovaIbérica

Álvaro Satrústegui

presidente y CEO de EXSEL

"Se necesitan unas 20 horas de formación para distribuir bien ciberseguros"

La conciencia sobre la ciberseguridad se ha ido incrementado en nuestro país, pero esto no se ve reflejado en la contratación de ciberseguros. ¿Por qué?: "fundamentalmente, porque falta formación a nivel tanto de mediadores como de clientes", apunta Álvaro Satrústegui, presidente de CEO de Exsel. Por eso, prosigue, "es necesario multiplicar los esfuerzos en formación" y cuantifica en 10 horas la formación básica para "distribuir el ciber seguro" y en 20 horas la formación recomendable "para entender mejor los conceptos de la ciberseguridad y por tanto la gestión de los riesgos implícitos".

¿Cómo percibe la situación de nuestro país en ciberataques? ¿Hay diferencia por CC.AA.?

La situación no es buena y no parece que vaya a mejorar a corto plazo. No creo que existan grandes diferencias entre CC.AA.; pero, sí hay algunas regiones que tienen más sensibilidad al tener más exposición por concentrar más centros de datos de empresas grandes.

¿Hay conciencia de la importancia de la ciberseguridad? ¿Y de contar con un ciberseguro?

Sí hay conciencia al respecto, pero no se traduce en contrataciones de ciberseguros. Esto se debe, fundamentalmente, a que falta formación a nivel tanto de mediadores como de clientes.

¿Y cómo se podría cambiar?

Multiplicando los esfuerzos en formación. Como he indicado, la percepción del riesgo existe, pero, insisto, hace falta mayor formación. El mapa de riesgos ha de incluir a los ciberriesgos de forma natural. Y es ahí donde no se está haciendo suficiente énfasis.

¿Qué daños de los causados por ataques informáticos externos cubren los ciberseguros?

Hay dos tipos. Los daños propios y los daños a terceros. Entre los primeros cabe mencionar: interrupción del negocio, extorsión, hacking telefónico, bricking (daños físicos a los equipos consecuencia de un evento de ciberseguridad) y el más preocupante, y menos ofrecido de todos, el fraude por transferencia de fondos. En daños a terceros tenemos responsabilidades por violaciones de la privacidad (reclamaciones

Mucho cambio

¿Cómo ha evolucionado el mercado español desde que comenzó a ofrecer ciberseguros?

Ha cambiado mucho. Las primeras pólizas estaban centradas casi exclusivamente en Daños a terceros y LOPD. Hoy todas las pólizas incorporan daños propios y además servicios de respuesta rápida de calidad.

y sanciones LOPD), responsabilidad multimedia, responsabilidades por violaciones de seguridad o responsabilidad por vulneración de los derechos de propiedad intelectual.

Importantes pérdidas

¿Cómo perciben este riesgo las aseguradoras? ¿Va apareciendo entre los productos que ofrecen?

Las aseguradoras que han ofrecido este seguro, las especialistas, han sufrido importantes pérdidas. Las demás aseguradoras ofrecen una versión muy limitada del producto, dando a cambio servicios de monitorización o de protección activa. Hay coberturas como el fraude de transferencia de fondos o la extorsión que o no se ofrecen o se ofrecen de forma limitada.

¿Qué riesgos prevé que se podrían dejar de cubrir en ciber?

Como decía, los relacionados con la ingeniería social son los que han visto recortada la cobertura de forma significativa.

"Los riesgos relacionados con la ingeniería social han visto muy recortada la cobertura"

Un ataque de 80.000 euros

¿Cuál ha sido el ataque más costoso y el más complejo que han cubierto?

En nuestro caso un ataque de 80.000 euros. Lo más complejo fue una encriptación de datos con extorsión e interrupción del negocio.

¿Y los mediadores, lo incluyen entre los productos que comercializan?

Sí, pero todavía sin confianza por la falta de formación. Aunque saben que es su obligación al menos proponerlo a sus clientes empresa y profesionales.

¿Qué conocimientos se necesitan para vender coberturas para estos riesgos?

La formación básica apenas supone 10 horas. Con esa formación se puede distribuir el ciber seguro. La recomendable estaría en torno a 20 horas para entender mejor los conceptos de la ciber seguridad y por tanto la gestión de los riesgos implícitos.

Protocolos de formación

¿Cuáles son los 'ataques' más temidos por las empresas? ¿Y por las aseguradoras? ¿Qué consecuencias suelen tener para las 'víctimas?

Los ataques derivados de la ingeniería social. Son los más temidos ya que implican casi siempre suplantaciones de identidad o similar que derivan en encriptación de datos, transferencias de fondos no deseadas, etc. En el mejor de los casos tendríamos el coste de recuperación de datos y cuando se complica se encadenan una serie de reclamaciones, sanciones y pérdidas de fondos que pueden poner en peligro incluso la continuidad de la empresa si es una pyme.

Una parte muy importante de las aseguradoras no ofrecen cobertura de estos eventos o lo hacen de forma muy limitada, exigiendo protocolos de seguridad específicos para ingeniería social.

¿Considera que los ciberataques se podrían incluir entre los riesgos más 'costosos'?

Están empezando a estar entre los más costosos y van a serlo en breve. La razón es la cobertura de la interrupción del negocio derivada de un ciberataque, que es la más costosa. La evolución está en gerenciar estos riesgos de forma adecuada implantando las políticas de seguridad que minimicen esta exposición en las empresas.

España, en buen camino

¿Cuál es su opinión sobre la evolución de ciberriesgos?

En España se están haciendo cada día mejor las cosas y vamos por el buen camino. A nivel global hay más problemas, particularmente en EE.UU., donde la siniestralidad es muy elevada y requiere un replanteamiento que vincule la cobertura con la calidad de las políticas de seguridad de las empresas aseguradas.

Tu salud,
nuestro compromiso

asefa salud

Seguros de Salud adaptados a ti y a los tuyos

Sin copagos en ningún servicio

Unidad de Protonterapia

Extensa cobertura en **medicina preventiva**

Amplio programa de **planificación familiar**

Videoconsulta y receta electrónica

Descuentos familiares

www.asefasalud.es

125 años
Cuidando de tu salud

Transformación digital: ¿todo ventajas?

La transformación digital se ha acelerado considerablemente en los últimos dos años. Las empresas han aceptado su órdago con contención, sabedoras de que no pueden ignorarlo; pero, muchas veces, no encuentran qué camino han de seguir. Transformarse digitalmente no significa tener una web, utilizar el mail o las videollamadas, implica pasos más complejos, como transformar el modelo de negocio a través de las herramientas tecnológicas. ¿Existen riesgos en este proceso? ¿qué deficiencias encuentran las compañías a la hora de iniciarlo?

Nadie ha dicho que la transformación digital fuera fácil, pero sí necesaria. Muchas son las webinars, ponencias y artículos de expertos que lo recuerdan día a día. El mundo empresarial lo acepta con cierta preocupación porque, a la par que se habla de digitalización, aparecen términos como ciberriesgos, ciberdelincuencia y ciberseguridad. Ejemplo de ello es uno de los casos más sonados en nuestro país, el que protagonizó MAPFRE el 15 de agosto de 2020, cuando fue víctima de un ciberataque tipo ransomware que ralentizó los sistemas de la compañía en un fin de semana clave para la movilidad e incidencias de tráfico.

Gracias a que la aseguradora tenía unos protocolos muy definidos y testados en materia de ciberseguridad, el ataque no puso en riesgo la información propia ni la de sus clientes, pero a lo largo de este último año "se ha visto que muchas empresas no están preparadas todavía para desenvolverse con plenas garantías en estos nuevos entornos y ecosistemas digitales, lo que ha multiplicado su exposición a distintos tipos de ciberataques como malware, spyware, phishing, etc", indica José Luis Mayordomo, director de Desarrollo de Producto de CODEOSCOPIC.

El asunto no es baladí. La inquietud de los directivos de las grandes empresas se refleja en el informe europeo sobre riesgos empresariales, Risk in Focus 2021. Hot Topics for Internal Auditors, del Instituto de Auditores Internos de España. Por tercer año consecutivo la transformación digital se encuentra en el puesto número tres de riesgos a los que tendrán que hacer frente las empresas, creciendo esta preocupación hasta alcanzar la segunda posición para 2025. Por eso, según su presidenta, Sonsoles Rubio, "es tan importante que las compañías estén mejor preparadas tecnológicamente, pues así tendrán mayor capacidad de reacción ante los cambios y la recuperación tras la actual situación de pandemia. Especialmente ahora, la transformación digital debe estar contemplada dentro de la propia estrategia de la compañía, liderada por la Dirección General".

En el caso de las pymes, "las que generen productos y/o incorporen servicios a los mismos serán aquellas que puedan surfear en la ola de la digitalización, mientras que, aquellas donde su actividad principal deriva de la distribución del objeto, son las que más riesgos presentan, fundamentalmente si estos objetos atienden a un mercado generalista", añade Antonio Núñez, Head of Insurance Distribution en NTT DATA Spain.

Desde el Instituto de Auditores Internos de España advierten también de que con la aceleración de la digitalización se han popularizado las plataformas Low Code Development Platform, aquellas que se han desarrollado con poco código concediendo mayor importancia al diseño que a la propia programación. Estas plataformas permiten ir más rápido en la expansión de canales digitales y se estima que, para 2024, el 75% de las grandes empresas utilice al menos cuatro de estas herramientas. "El rápido crecimiento de la digitalización puede hacer que se pierda el control sobre elementos clave, aumentando los riesgos de seguridad y privacidad de los datos", afirma Sonsoles Rubio. Y es que, los riesgos asociados al robo o pérdida de datos personales, si bien no paralizan la actividad, pueden impactar de forma muy negativa en la imagen de la compañía -y sus ventas- así como generar demandas, multas y litigios con costes millonarios.

Formación del personal

En un mundo cada vez más digital, la ciberseguridad es un riesgo permanente para gestionar. Con el fin de prevenir ciberataques, las empresas

Sonsoles Rubio

"El rápido crecimiento de la digitalización puede hacer que se pierda el control sobre elementos clave, aumentando los riesgos de seguridad y privacidad de los datos".

José Luis Mayordomo

"Muchas empresas no están preparadas todavía para desenvolverse con plenas garantías en estos nuevos entornos y ecosistemas digitales, lo que ha multiplicado su exposición a distintos tipos de ciberataques".

LOS PROS...

- **Mayor eficiencia y productividad:** la digitalización permite acelerar los procesos y optimizar las operaciones ahorrando en tiempo y recursos, lo que permite dedicarse a tareas de mayor valor.
- **Aumento de la rentabilidad:** la eficiencia operativa y el aumento de productividad impactan directamente en la cuenta de resultados.
- **Automatización de los procesos:** la tecnología ya se está utilizando en operaciones clave como la administración de pólizas, siniestros, contabilidad, RRHH o en operaciones de atención al cliente, entre otros.
- **Mejora de la experiencia de cliente:** la tecnología permite conocer al detalle al cliente, lo que permite crear y ofrecerle productos, servicios y experiencias a medida, abriendo, además, nuevas oportunidades de negocio.
- **Mayor capacidad de resiliencia:** las empresas que adoptan tecnologías digitales y construyen una cultura digital están en mejores condiciones para adaptarse rápidamente a los cambios.
- **Mejora en la toma de decisiones:** los datos son oro, el activo más valioso de las empresas. Y la tecnología, a través de los datos que brinda, les permite tomar las mejores decisiones para adaptarse rápidamente a la volatilidad del mercado.

deben analizar vulnerabilidades, reforzar protocolos y sistemas y concienciar sobre la ciberseguridad a los empleados, pues las personas son el eslabón más débil de la cadena de seguridad. En este sentido, la falta de personal cualificado es, en opinión de Miguel Ángel Mayordomo, el principal problema al que deben enfrentarse las empresas en su transformación digital. El conocimiento que adquieran los empleados "permite garantizar la integridad y seguridad de los datos manejados que, en muchos casos, constituyen el propio core del negocio". Sonsoles Rubio lo corrobora: "hay escasez de talento con capacidades tecnológicas", por ello, "hay que formar y capacitar a los empleados no técnicos para que puedan desarrollar tareas más tecnológicas y ayuden así a las áreas de TI, cada vez más sobrecargadas de trabajo".

Para Daniel Millet, CEO de MPM Insurance Solutions, "en muchas ocasiones no se invierte el tiempo necesario e infravaloramos su importancia. Prestar atención a la formación de los colaboradores de la correduría, a repensar los procesos de negocio y a una buena implementación de la tecnología para obtener el máximo provecho son aspectos clave que deben tenerse en cuenta".

... LOS CONTRAS

- **Ciberataques tipo ransomware, malware, spyware, phishing...**
- **Proliferación de las Low Code Development Platforms**, que conceden mayor importancia al diseño que a la propia programación.
- **Pérdida del control sobre elementos clave** debido a la aceleración de la digitalización, aumentando los riesgos de seguridad y privacidad de los datos.
- **Falta de personal cualificado.** Se debe formar a los empleados, el eslabón más débil de la cadena de seguridad.
- **Externalización de algunos procesos.** A la hora de externalizar un proceso no se debe externalizar el riesgo.

Antonio Núñez

"Las pymes que generen productos y/o incorporen servicios a los mismos serán aquellas que puedan surfear en la ola de la digitalización".

Daniel Millet

"El reto que tienen las corredurías es cómo abordar un proceso de digitalización escogiendo el compañero de viaje y la plataforma adecuados que les permita integrar las diferentes tecnologías/productos de forma consistente y coherente".

Externalización

Otro riesgo a añadir en la transformación digital es el que va asociado a la posible externalización de determinados procesos. Un ataque a un tercero puede afectar a las redes y sistemas internos de la organización "por lo que es importante que, a la hora de externalizar un proceso, no se externalice el riesgo", señala Sonsoles Rubio.

Por otro lado, Daniel Millet apunta el obstáculo que los mediadores deben afrontar en cuanto a la tecnología en sí misma. "El reto que tienen las corredurías es cómo abordar un proceso de digitalización escogiendo el compañero de viaje y la plataforma adecuados que les permita integrar las diferentes tecnologías/productos de forma consistente y coherente". En su opinión, el riesgo de no escoger la plataforma correcta puede implicar no beneficiarse de las nuevas tecnologías y no avanzar al ritmo necesario en el ámbito digital perdiendo competitividad y oportunidades.

Impulsar iniciativas

Dentro de la Agenda 2030 del Gobierno estatal, aparece el Plan de Digitalización de las Pymes 2021-2025, un conjunto de medidas que pretenden impulsar iniciativas que comercialicen servicios/productos bajo infraestructuras digitales, como el e-commerce, que cuenten con profesionales en el ámbito de las capacidades digitales con capacidades de conectividad de alta velocidad (5G) para utilizar dispositivos conectados (IoT) donde se gestione eficientemente y de forma segura la información (Cloud).

Aquellas pymes que puedan aprovecharse del Plan 2021-2025, tendrán la posibilidad de mejorar su competitividad y pasar de comercializar sus servicios o productos en otros mercados, evitando así ser canibalizadas por sus pares; además, podrán reducir sus costes en base a eficiencia operativa debido al uso de tecnología.

En este sentido, las ventajas de la transformación digital en términos de acceso al mercado, competitividad y flexibilidad son mucho mayores que los riesgos existentes. Según Antonio Núñez, la clave está en combinar la transformación digital con el despliegue de una estrategia adecuada de mitigación y prevención -para evitar que estos riesgos se materialicen-; la transferencia de los costes económicos para el caso de que se produzca algún evento de este tipo -a través de un seguro-; y contar con planes y capacidades que permitan responder y restablecer de forma rápida el negocio reduciendo el impacto. El objetivo es que se minimicen los nuevos riesgos derivados de la digitalización, utilizando herramientas Cloud, Software específico de gestión (ERP), modelos diferentes en la gestión de recursos humanos potenciando el teletrabajo como herramienta de fidelización y captación de talento, buscando el soporte en ámbitos de Ciberseguridad (INCIBE) y/o contratando pólizas que mermen el impacto de un ciberataque, entre otras cosas.

De la digitalización puede depender el futuro de la compañía. Las empresas que vayan por delante tendrán una clara ventaja competitiva. Se calcula que el 75% de las empresas del S&P 500 no existirán en 2027: la edad media de esas empresas ha bajado de 61 a 22 años en apenas 60 años.

Desde un punto de vista operativo, tecnologías como la automatización, el aprendizaje automático y la Inteligencia Artificial aceleran los procesos, aumentan la eficiencia -reducen los procesamientos manuales- y reducen los costes a largo plazo. Y al impulsar la estrategia, permiten subir los ingresos con el desarrollo de nuevos productos o servicios o la irrupción en nuevos mercados que permiten abordar nuevos planteamientos.

Losas en el negocio de las correduría

La gestión de una correduría se está convirtiendo en una auténtica yincana. Requisitos legales, de negocio, cargas administrativas en la relación con las compañías aseguradoras…. Todo un sinfín de trámites y requerimientos burocráticos que alejan el auténtico objetivo de la Mediación en Seguros: conseguir negocio y atender a los clientes, aportándoles un valor añadido y diferencial, adaptado a sus cambiantes necesidades.

Durante los últimos años está quedando patente que la gestión de una correduría de tamaño pequeño, o incluso mediano, que lleva el negocio en solitario, es una labor cada vez más complicada. Los requerimientos normativos, los procesos administrativos y la vorágine del propio mercado, que afectan a todo tipo de empresas de mediación por igual, independientemente de su tamaño, provocan que, en la mayoría de las ocasiones, la propia gestión del negocio acapare el mayor tiempo de dedicación, lastrando los recursos e impidiendo el crecimiento cuando estos son escasos.

Ante ello, existen en el mercado varias soluciones que desbloqueen el crecimiento de las corredurías con menos recursos. Unas pasan por la integración total con otras, perdiendo, eso sí, la propia idiosincrasia que se haya forjado. Otra opción es aunar esfuerzos y compartir recursos mediante la asociación o la agrupación, lo que permite disminuir costes y procesos, pero manteniendo así la esencia del negocio.

Sea como fuere, parece claro que las grandes exigencias que conlleva la gestión de un negocio de Mediación en Seguros suponen un lastre para las pequeñas empresas del sector. Buscar una solución será cuestión de pocos años, dado el proceso de mayor concentración que se va produciendo, día a día, en este segmento.

¿Qué se gana con una fusión o integración?

Con una fusión de corredurías se puede conseguir que la suma de todos los trámites burocráticos y de gestión se queden en la mitad. Una sola DEC, un solo informe del Defensor del Asegurado, impuestos, requisitos laborales....

CARGAS ADMINISTRATIVAS CON LAS COMPAÑÍAS DE SEGUROS

- **Digitalización**
  La llegada de CIMA, tras EIAC, supone un espectacular avance para la relación de gestión entre aseguradoras y corredurías. Su implantación es inminente y facilitará, sin duda, la gestión de éstas. A ello se debe sumar todo el esfuerzo de digitalización de la propia correduría, lo que conlleva una serie de costes y gestiones añadidas.

- **Facturación**
  Las corredurías están obligadas a emitir facturas a las aseguradoras con las que trabajan. No obstante, es práctica habitual que sean éstas las que realicen la "autofactura", es decir, faciliten la factura ya confeccionada a la correduría. Aun así, el cotejo de los datos es necesario.

- **Negociación de condiciones**
  Si bien no es una carga administrativa como tal, negociar todos los años las condiciones económicas con las aseguradoras no deja de ser tarea importante. Gracias a las fusiones de cartera, estas negociaciones pueden resultar más favorables para las corredurías, al contar con mayor volumen de cartera para negociar.

En cuanto a costes, parece obvio que aprovechar las sinergias de varios negocios en uno abaratará los gastos de gestión y permitirá una economía de escala, que siempre ofrece beneficios a sus integrantes.

Pero, además, la fuerte competitividad, cada vez, mayor, de los mercados, los menores márgenes de beneficio a los que se enfrentan las corredurías, y la mayor carga de trabajo administrativo y de burocracia pueden verse beneficiados con la unión de los negocios.

¿Y qué medidas tomar?

El pequeño y mediano corredor se puede llegar a plantear qué modelo de gestión le resulta más interesante a la hora de impulsar su negocio mediante la fusión o alianzas. Parece generalizado el sentimiento de que las pequeñas corredurías (aquellas que no alcancen, por ejemplo, el millón de primas intermediadas) opten por la fusión e integración en grupos más grandes. Sin embargo, su tipología de negocio, que puede ser rentable, basada en la capilaridad, en la cercanía al cliente, en llegar donde las grandes y medianas corredurías no llegan, puede ser un punto a su favor y no siempre ser interesante la integración total o fusión de la cartera.

En el caso de las corredurías de tamaño medio, parece más obvio que la agrupación o asociación, sin perder el control de negocio, puede ser la solución más viable para aprovechar las sinergias.

TEMAS LEGALES QUE DEBEN ABORDAR LAS CORREDURÍAS

Además de todos los requisitos legales que debe cumplir cualquier empresa, las corredurías, reguladas por una muy estricta normativa legal, deben acometer una serie de servicios y obligaciones que incrementan su carga de trabajo y costes, como son:

Protección de datos:
La normativa en materia de protección de datos, cada vez más exigente, obliga a las corredurías a mantener constantemente una serie de controles y vigilancia sobre los datos que manejan de sus clientes. Esto implica mayor trabajo y desembolso cuando se trata de datos especialmente protegidos, como los de salud.

SEPBLAC:
Las corredurías están obligadas a cumplir la normativa sobre prevención del blanqueo de capitales y por ello deben disponer de procedimientos internos adecuados para su cumplimiento, especialmente relativo a los seguros de vida con componente financiero.

Departamento de atención al cliente:
La obligación legal de contar con un departamento de atención al cliente y defensor del asegurado conlleva costes adicionales. La externalización de este servicio es tónica habitual, aunque su coste es exponencial al volumen de cartera manejado.

Formación:
Ni que decir tiene las nuevas obligaciones en materia de formación que han caído como una losa sobre las corredurías de seguros. La nueva Ley de Distribución regula con mayor rigidez esta materia y para las empresas de mediación ha supuesto un lastre añadido para su gestión.

Seguro de responsabilidad civil:
En función del volumen de primas y cartera intermediada se ha de contratar un seguro de responsabilidad civil con una prima acorde al negocio manejado. Sin duda, una integración de carteras logra abaratar este coste.

Aval o seguro de caución:
Requisito legalmente obligatorio cuando se manejan fondos de los clientes, este aval o seguro de caución encarece también la actividad mediadora, y se puede ver proporcionalmente reducido en su coste cuando se fusionan carteras.

SINERGIAS EN ASPECTOS DE GESTIÓN EMPRESARIAL

Entre las obligaciones fiscales y empresariales que tienen las corredurías, como empresas de Mediación que son, se encuentran:

- **Impuesto de sociedades:**
  Obligación de efectuar y presentar un pago fraccionado en los primeros 20 días de los meses de abril, julio, octubre y diciembre.

- **IVA:**
  Aunque la actividad aseguradora está exenta de IVA, como tal, las corredurías que cobren honorarios o tengan colaboradores que, por sus funciones, las obliguen a facturar IVA, están obligadas a presentar este modelo trimestralmente.

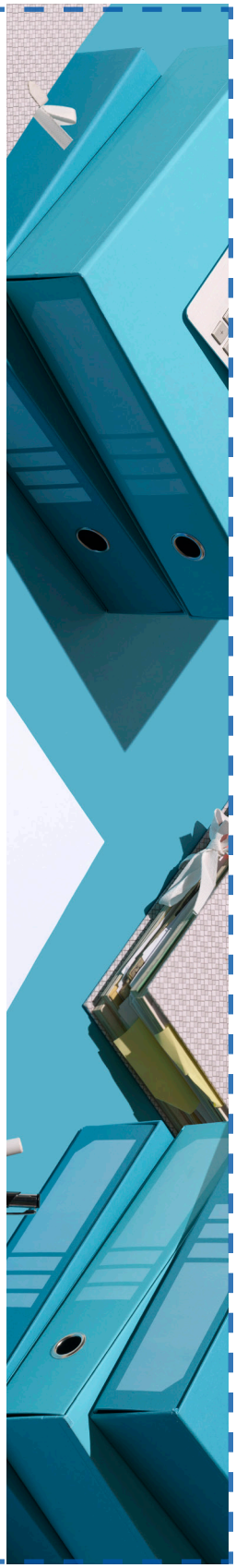
- **Declaración anual de operaciones con terceros:**
  Las corredurías, como cualquier otra empresa, han de presentar el modelo 347, cuando respecto a otra persona o entidad hayan realizado operaciones que en su conjunto hayan superado la cifra de 3.005,06 euros en el año natural.

- **Seguridad Social:**
  Han de asumir, también, toda la carga administrativa derivada de la tenencia de trabajadores por cuenta ajena que tengan contratados.

- **Nóminas:**
  La correcta gestión de las nóminas de los empleados es otro punto que requiere especial atención y dedicación en el día a día.

- **Prevención de riesgos laborales:**
  El mero hecho de tener trabajadores a su cargo obliga a las corredurías a cumplir la normativa de prevención de riesgos laborales, que incluye entre otras cosas, adoptar medidas de seguridad e higiene en el trabajo, o llevar a cabo acciones formativas para el personal.

- **Contabilidad:**
  Como cualquier empresa, las corredurías han de llevar sus libros de contabilidad y una gestión adecuada a la normativa legal. Además, están obligadas a separar las cuentas empresariales de aquellas otras en las que se gestionan fondos de clientes.



FORMACIÓN EXPERTO

Cursos Experto Universitario diseñados para satisfacer las necesidades profesionales del sector asegurador. Impartidos por la Universidad CEU San Pablo.

EXPERTO
VIDA Y SALUD

NUEVA FORMACIÓN CONTINUA

VENTA CONSULTIVA Y FIDELIZACIÓN DEL CLIENTE

IBIPS PRODUCTOS FINANCIEROS

NUEVO ENTORNO EN LA VENTA DE SEGUROS

LOPD

CIBERRIESGOS

Para más información contactar con CECAS:
cecas@cibercecas.com
www.cibercecas.com

CECAS
Escuela de negocios de seguros

José Luis Ferré

Consejero delegado de Allianz España

"Queremos ser un jugador relevante en la gestión del ahorro"

Allianz apuesta por ser "un jugador relevante en toda la gestión del ahorro de los españoles". Por eso, lleva tiempo animando a su red de mediadores a ampliar su ámbito de conocimiento y formación, "en aras de ofrecer a los clientes el mejor servicio y asesoría en el ámbito de los seguros y los productos financieros". De hecho, destaca su CEO, José Luis Ferré, ya cuentan con más de 1.000 mediadores certificados en MiFID. Otra de las grandes apuestas es la innovación: "Procuramos incorporar todas las innovaciones tecnológicas que puedan ayudar tanto al mediador como al cliente y lo hacemos siempre de la mano de la Mediación. Son nuestros agentes los que primero testean todo y nos dan inputs para seguir mejorando".

¿Cómo definiría la actual situación de Allianz?

A pesar de que la Covid-19 supuso un shock, al que hubo que hacer frente prácticamente de la noche a la mañana, también fue la "prueba de fuego" para el trabajo previo de digitalización realizado por las empresas. Nosotros nos sentimos muy satisfechos de nuestra capacidad para, no sólo dar servicio a los clientes (incluso en los momentos más complicados del confinamiento) sino para acompañar y apoyar a la red de Mediación en unas circunstancias tan complejas como inesperadas. 2021 ha sido para nosotros un año de despegue, con muchos proyectos cristalizados. En Vida hemos consolidado nuestro Plan Estratégico de Vida y Asset Management. En un año tan complejo, hemos fortalecido nuestra oferta con Allianz Perspektive y comenzamos a operar con la agencia de valores Allianz Soluciones de Inversión. Nuestra Mediación se ha sumado a este proyecto y ya contamos con más de 1.000 mediadores certificados en MiFID.

En No Vida hemos lanzado un nuevo producto de automóviles que está disponible, para todos los agentes, en la nueva plataforma global del Grupo. Es un producto renovado que creemos es el mejor del mercado. Permite mayor agilidad en la emisión y cotización: en solo 19 segundos podemos dar un precio al cliente. Además, incluye servicios de valor añadido como la cobertura RC de patinetes eléctricos, de hasta 300.000 euros, o cuestiones como la posibilidad de guardar la póliza en el wallet.

¿Cómo prevén cerrar 2021?

No solemos hacer previsiones de negocio concretas, pero sí puedo adelantar que somos optimistas. Ha sido un año de retos y de muchos lanzamientos, como los citados. Es difícil quedarse con un solo proyecto. Pero tengo claro que todos estos retos no hubieran sido posibles sin el apoyo y el compromiso de nuestra Mediación. Su avanzada digitalización le ha permitido no solo seguir dando un exce-

¿Qué riesgos son más complicados de colocar?

Sin duda, los que todavía se están desarrollando, ligados a las nuevas tecnologías y a la falta de legislación. El paradigma de la movilidad, así como el aseguramiento a las personas y a los vehículos, hacen que se abra una incertidumbre sobre cómo evolucionará el seguro de autos. Los nuevos vehículos de movilidad personal y su regulación serán clave para 2022. En particulares, la inquietud sobre la evolución del cambio climático y los eventos meteorológicos hacen que en el futuro se replanteen los Multirriesgos, tal y como los conocemos.

En riesgos industriales, las actividades muy expuestas a grandes incendios, como reciclaje y tratamiento de residuos, así como gran empresa química y de alimentación, también son complejas de asegurar. Ocurre igual con las coberturas de ataques cibernéticos, cada vez más frecuentes y donde los siniestros se han disparado de manera generalizada.

Un proyecto pionero

"La digitalización se ha instalado ya en nuestros hábitos y forma parte de nuestro día a día. Ahora incluso los baby boomers han adoptado las prácticas de los millennials o centennials y utilizan con normalidad las nuevas tecnologías para transacciones y compras. Por eso hay que intensificar la adaptación de la oferta y la gestión de los negocios a un consumidor cada vez más conectado, que consulta varios canales antes de comprar y que exige agilidad, eficiencia y una buena experiencia de cliente. Por otra parte, no podemos dejar de anticiparnos a las necesidades del mañana: los jóvenes representan el futuro y hemos de comenzar a estar cerca de ellos, interactuando en aquellas plataformas que forman parte de su día a día. A modo de ejemplo, hemos incorporado Whatsapp a nuestros canales de comunicación, un proyecto pionero que presta servicio las 24 horas, los 7 días de la semana. Nos permite la gestión de trámites de manera clara, rápida y sencilla".

lente servicio a los clientes, sino seguir desarrollándose y ayudándonos a seguir mejorando como compañía.

¿Qué objetivos destaca de 2022?

Será un año de consolidar proyectos y de seguir haciendo nuevos lanzamientos. Nuestro foco estará en el crecimiento rentable, la excelencia técnica y la centralidad en el cliente, con especial foco en poner en valor nuestra marca.

¿Cuáles son las claves de su apuesta por la Mediación? ¿Y por otros canales?

En Allianz tenemos una clara apuesta por la Mediación: es nuestro principal canal. Creemos firmemente en el valor añadido que la asesoría y la cercanía al cliente aportan a la hora de tomar cualquier decisión y más si se trata de decisiones financieras, donde tenemos importantes lanzamientos previstos. Mantenemos con toda nuestra red una frecuente y fluida comunicación que nos permite un enriquecedor intercambio de ideas e impresiones. Además, seguiremos apostando por la formación para conseguir profesionales todavía más expertos en todos los ámbitos que puedan ser de utilidad para el cliente y sus propias organizaciones.

Como empresa global, creemos que el cliente debe poder elegir el canal por el cual quiere interactuar. Apostamos por la Mediación, pero también desarrollamos otros canales, en este caso bancaseguros, junto a BBVA. Creemos que las innovaciones de la *joint venture* pueden aportar beneficios también a nuestra Mediación.

Soluciones integrales

¿Cómo deben evolucionar los mediadores de seguros?

Somos muy conscientes del valor añadido que la asesoría y la cercanía al cliente aportan al tomar cualquier decisión y más si son decisiones financieras. Creemos que los mediadores pueden evolucionar hacia una oferta de soluciones integrales a los clientes, protegiéndoles en todos los ámbitos de su vida, no solo en los clásicos Autos o Hogar, sino también con soluciones financieras completas. Por eso, llevamos mucho tiempo animando a la red de mediadores a ampliar su ámbito de conocimiento y formación e incorporarse a nuestros programas formativos enfocados a mejorar las competencias, en aras de ofrecer a los clientes el mejor servicio y asesoría en seguros y productos financieros. El objetivo es acompañar al cliente para que conozca y comprenda los productos y tome la mejor decisión de compra. Además, la apuesta de la Mediación debe ser la digitalización y poder atender al asegurado en cualquier momento y desde cualquier lugar. En esta línea, nosotros procuramos incorporar todas las innovaciones tecnológicas que puedan ayudarle en su labor.

¿Cuál es su opinión sobre la evolución de los productos de ahorro/inversión en España?

El prolongado entorno de bajos tipos de interés está lastrando la evolución de los seguros de Vida Ahorro. Especialmente acusado ha sido el compor-

CIMA es un paso adelante

"Cima es gran avance en el compromiso sectorial para la implantación de los estándares de intercambio de información; lo estamos llevando a cabo compañías y corredurías a través de la Plataforma de Conectividad y Servicios que está desarrollando Tirea.

Hará posible unificar y simplificar los canales de comunicación, tanto si utilizan software de mercado en su gestión, software propio o para quienes acceden individualmente a los portales de cada entidad con la que opera. Es un paso imprescindible para percibir el valor que proporciona la digitalización aplicada a la distribución y nos permitirá avanzar hacia la excelencia que exige el cliente actual".

tamiento registrado en 2020 debido a que, al impacto de los bajos tipos, ha habido que sumar el de la crisis provocada por la Covid-19. Por eso, en este entorno, es tan importante ofrecer una gama de productos amplia y el asesoramiento de agentes y corredores, para tomar las mejores decisiones de inversión, es importante. Nosotros tenemos claro que queremos ser un jugador relevante en toda la gestión del ahorro de los españoles.

¿Cuáles son los principales retos sociológicos y económicos que tendrá que enfrentar nuestro país y cómo influirán en el sector?

Los cambios regulatorios están teniendo un impacto muy relevante. La digitalización y la incorporación de las nuevas tecnologías han de ser una prioridad estratégica de las aseguradoras, junto con la centralidad en el cliente y el desarrollo de productos y servicios que respondan a sus nuevas necesidades y prioridades. Además, a nivel de país, debemos hacer frente al envejecimiento de la población.
Con todo, la dimensión y relevancia del cambio climático y la repercusión que ya está teniendo en el negocio asegurador lo posiciona como una de las mayores prioridades tanto para el sector como para la sociedad.

Nuestro propósito no es solo brindar seguridad financiera: 'Protegemos tu futuro' también significa que la sostenibilidad en todas sus dimensiones es nuestra prioridad. La sostenibilidad y la inclusión son la mejor manera de realizar nuestro potencial de crecimiento y creación de valor. Y al mismo tiempo, contribuir a un futuro más sostenible para el mundo y las sociedades en las que vivimos y trabajamos. Nuestra ambición es pasar de ser una empresa responsable por derecho propio a ser líder en la industria de servicios financieros y más allá. No en vano, somos la aseguradora número 1 en el Dow Jones Sustainability Index.

Formación: muy lejos de Europa

La importancia y complejidad de una actividad se mide por la preparación que se requiere para su ejercicio. Esta máxima podemos aplicarla a los profesionales de los seguros. Tradicionalmente el foco se ha puesto en la formación legalmente establecida para acceder a la profesión que, en la actualidad, recoge la Resolución de Formación de 3 de junio de 2021 de la Dirección General de Seguros y Fondos de Pensiones (DGSFP), pero ¿qué pasa con el resto de la regulación que afecta al sector?

CECAS Insurance Business School

En España, como en el resto de la UE, existe un Catálogo Nacional de Cualificaciones Profesionales (CNCP), que facilita la adecuación de la formación profesional a los requerimientos del sistema productivo. Incluye las 'Cualificaciones Profesionales' más significativas del sistema productivo, organizadas en familias profesionales (26) y 5 niveles. Cada cualificación (687) está formada por un bloque coherente de unidades de competencia. Y cada unidad de competencia (2.290) lleva asociado un 'Módulo' con especificaciones de la formación.

Al Seguro pertenecen dos cualificaciones profesionales de la familia 'Administración y Gestión', en cuya actualización ha participado este año el CECAS, junto a profesionales y expertos del sector: ADG649_3 'Gestión técnica de seguros privados' y ADG545_3 'Distribución de seguros y reaseguros privados'. Ambas tienen una duración de 720 horas lectivas y pertenecen al nivel 3, el más alto no universitario.

"Esperamos que esta última actualización, conforme a los requisitos de la Ley Distribución y legislación que la desarrolla, pueda ser una vía más de formación para los distribuidores pues hasta ahora la incoherencia con lo establecido por la antigua Ley de Mediación condenó, en la práctica, a que estos certificados fuesen 'papel mojado'", apunta Marta Rodríguez Varona, senior sales manager del CECAS.

Certificados de Profesionalidad

Para acreditar una cualificación es necesario el correspondiente 'Certificado de Profesionalidad', que acredita el conjunto de competencias profesionales que capacitan para el desarrollo de una actividad laboral, "sin que ello constituya regulación del ejercicio profesional. Esto es importante en el caso de seguros y aclara la relación de estos certificados con lo establecido en la Resolución de la DGSFP", aclara la experta del Centro de Estudios.

Cada certificado se corresponde a un perfil profesional estructurado en unidades de competencia e incluye la formación asociada a dicho perfil. Por otro lado, el Servicio Público de Empleo Estatal (SEPE) y los órganos competentes de las Comunidades Autónomas son los encargados de expedir los certificados con validez nacional.

Formación Profesional Dual... en Seguros

Hasta aquí la estructura de la Formación Profesional en el ámbito laboral, que se complementa con la establecida en la llamada Formación Profesional Educativa'. En septiembre, el Consejo de Ministros remitió a las Cortes el Proyecto de Ley Orgánica de Ordenación e Integración de la Formación Profesional, que pretende la integración en el ámbito laboral de la FP Educativa y la FP para el Empleo. "Con ello se persigue contar con una oferta de formación profesional flexible y progresiva que acompañe al profesional a lo largo de toda su carrera, consciente de que la formación constante será imprescindible para garantizar la empleabilidad de las personas, hecho que recoge de manera taxativa la Resolución de la DGSFP de 3 de junio de 2021", resume Rodríguez Varona.

UNA 'FOTO' QUE NO NOS FAVORECE

- El 35% de la población activa española tiene una cualificación baja y un 25% intermedia.
- Sólo el 12% de los jóvenes españoles está matriculado en FP frente al 25% de la UE y el 29% de los países de la OCDE.
- El 46% de la población activa carece de una acreditación profesional.
- España dedica unas 17 horas de formación al año por persona trabajadora, frente a las 50 horas de Alemania y las 80-85 de las empresas líderes en el mundo, según el Foro Económico Mundial.

También pone de relieve la importancia de la Formación Profesional Dual, que combina la formación con prácticas obligatorias en empresas. "En seguros somos pioneros en FP Dual, al contar ya con dos exitosas ediciones en Cataluña y una primera 'piloto' en la Comunidad de Madrid, en las que el Consejo, CECAS, los Colegios junto a Unespa y otras instituciones y fundaciones del sector, así como aseguradoras, han participado y lo harán más en el futuro para hacerlo extensivo a otros territorios".

Para la experta del CECAS, en la actividad aseguradora esta necesidad de capacitación y formación continuada "se acrecienta aún más si cabe pues nuestro producto es un intangible y el valor diferencial y claves del éxito será la capacidad de asesoramiento e información de los profesionales; los productos se copian y la tecnología se puede comprar". Por eso, anima a los profesionales del sector "a formarnos de manera permanente para garantizarnos la empleabilidad y éxito profesional. Desde CECAS queremos acompañar a los mediadores en este imprescindible viaje".

Europa comienza a actualizar la IDD

La presidenta de EIOPA, Petra Hielkema, ha comunicado, en una reciente reunión de BIPAR, que la Comisión Europea ha empezado a trabajar en la revisión de la IDD. El proceso se alargará hasta 2024, momento en que se publicará la actualización de la directiva que entró en vigor en España en febrero de 2020, aunque sigue 'atascada' en el Congreso de los Diputados lo que a revisión de enmiendas se refiere.

Como miembros de pleno derecho de BIPAR, el Consejo General ha puesto de manifiesto la situación paradójica de que en Bruselas haya empezado la revisión de una Directiva que, en España, último país en trasponerla y obligado por las sanciones europeas, todavía está pendiente de completar el trámite parlamentario de discusión de 122 enmiendas. El resultado final -se indica- "podría modificar su polémico reglamento de aplicación y hasta la propia ley, aunque no en sus mínimos, al tratarse de una trasposición europea".

En este sentido se recuerda que el Consejo General ha presentado 18 propuestas de enmiendas al Real Decreto Ley. De ellas 17 han sido admitidas a trámite por la Comisión de Hacienda del Congreso de los Diputados. "La mayoría -se subraya- tienen como objetivo corregir cuestiones de fondo que afectan a los diferentes distribuidores de seguros, particularmente a agentes y corredores".

Razones del retraso

Al dar cuenta de esta situación, se informa asimismo que, según el artículo 41 de la IDD, había de fecha límite el 23 de febrero de 2021 para que la Comisión Europea hubiese presentado un informe sobre la aplicación del artículo 1 de la IDD y comenzase a revisarla. Dos cuestiones han demorado todo: por una parte, la adopción tardía de la Directiva por varios países (entre ellos España) y la situación originada por el Covid. De esta forma, los informes previstos se han pospuesto; su publicación se prevé ahora que sea en el segundo semestre de 2022.

Valencia acogerá el congreso de mediadores más importante del año

Congreso MEDIADORES 2022
Valencia - Mayo, 19 - 20

Tras dos años de aplazamientos debido a la pandemia de COVID, los mediadores volverán a reunirse presencialmente en 2022. Será en Valencia, los días 19 y 20 de mayo, para celebrar su XII Congreso.

Es la gran cita de los agentes y corredores de seguros. Un punto de encuentro de toda la profesión: desde presidentes y consejeros delegados de aseguradoras a corredores unipersonales, miembros de las Administraciones, creadores de startup, proveedores tecnológicos, fundadores de insurtechs o miles de colegiados que compartirán experiencias y testimonios inspiradores para su trabajo diario.

Gestionando la incertidumbre es eslogan sobre el que girará el Congreso de Mediadores 2022. Ya no podemos hablar de cambio, de futuro, sino de cómo deslizarnos sobre la ola constante de la incertidumbre para avanzar en el desarrollo de nuestra profesión ganando clientes y mejorando nuestros servicios.

En la reunión de Valencia se hablará de muchos temas que nos afectan: del impacto de la sucesión en el negocio cuando la generación babyboom prepara su jubilación y debe decidir entre vender, aliarse con iguales o fusionarse; del impacto de la ciberseguridad en nuestra empresa; o de cómo actúa un cliente acostumbrado a la experiencia de Amazon, Airbnb o de la banca digital. No se puede dejar atrás una cuestión tan delicada como los efectos de la constante avalancha normativa que nos sigue llegando desde las distintas Administraciones y cómo cumplir con todos sus requerimientos sin morir en el intento.

Una profesión apasionante

En Valencia se hablará también de criptomonedas, un concepto que sonaba a ciencia ficción hace muy poco pero que ya ha llegado al Seguro y exige prepararse para operar con ellas en agencias y correduría. Se debatirá igualmente sobre la importancia de la gestión ética del negocio, algo que parecía reservado a las grandes corporaciones pero que afecta de lleno a cualquier actividad comercial, especialmente, si como la Mediación, está presidida por la transparencia. Los riesgos que ya están entre nosotros, pero no lo sabemos, tendrán un espacio específico y geoestratégico; igual que la desesperación de muchos profesionales de la Mediación cuando encuentran que determinadas actividades industriales o sectoriales incomprensiblemente no se pueden asegurar porque no existen productos específicos que les den cobertura.

El Congreso de Valencia no es una cita más para aburrirse con interminables mesas redondas de los habituales protagonistas del sector Es una oportunidad para la reflexión, para reforzar las relaciones profesionales y personales y, sobre todo, para reafirmarse en que pocas profesiones son tan apasionantes como la mediación profesional de seguros.

Unit Linked, atractivos para la Mediación, pero...

La cercanía al cliente de agentes y corredores, unida a la necesidad de asesoramiento y seguimiento que requieren los productos de inversión, los convierten en una oportunidad para ampliar el negocio en tiempos de baja rentabilidad. Y en una clara apuesta de futuro.

Aparecieron en el mercado hace dos décadas, pero en los últimos tiempos los unit linked, en particular, han vuelto a ganar protagonismo tras años con tipos de interés que primero eran bajos, luego ultrabajos y actualmente incluso negativos. Son de nuevo una opción, de las pocas, para rentabilizar los ahorros de aquellas personas con capacidad de generarlos, pero que aún ven lejos la jubilación y están dispuestos a correr un mayor riesgo a cambio de una expectativa de rentabilidad. Eso sí, estos productos requieren un asesoramiento a lo largo del tiempo capaz de adaptarse a la evolución del mercado y el perfil del cliente. En el centro de esta ecuación aparece el mediador de seguros. Pero, ¿por qué ahora es el momento?

Mientras los productos con rendimientos garantizados duermen el sueño de los justos y ante la práctica desaparición de los depósitos a tipo fijo, la inversión en bolsa e instrumentos financieros no ha dejado de ganar popularidad. El último informe de balance de 2020 y perspectivas para 2021 de Inverco sobre fondos de inversión prevé un incremento del patrimonio invertido del 5%, pero, lo que es más importante, apunta un cambio en el perfil de riesgo de los partícipes: si en 2014 el 51% del patrimonio de los fondos de inversión pertenecía a perfiles conservadores (23% monetarios y renta fija a corto plazo y 28% garantizados), en diciembre de 2020 solo el 25% del ahorro en fondos se canalizaba a través de estos instrumentos.

"El mediador tiene que saber lo que está pasando en los mercados"

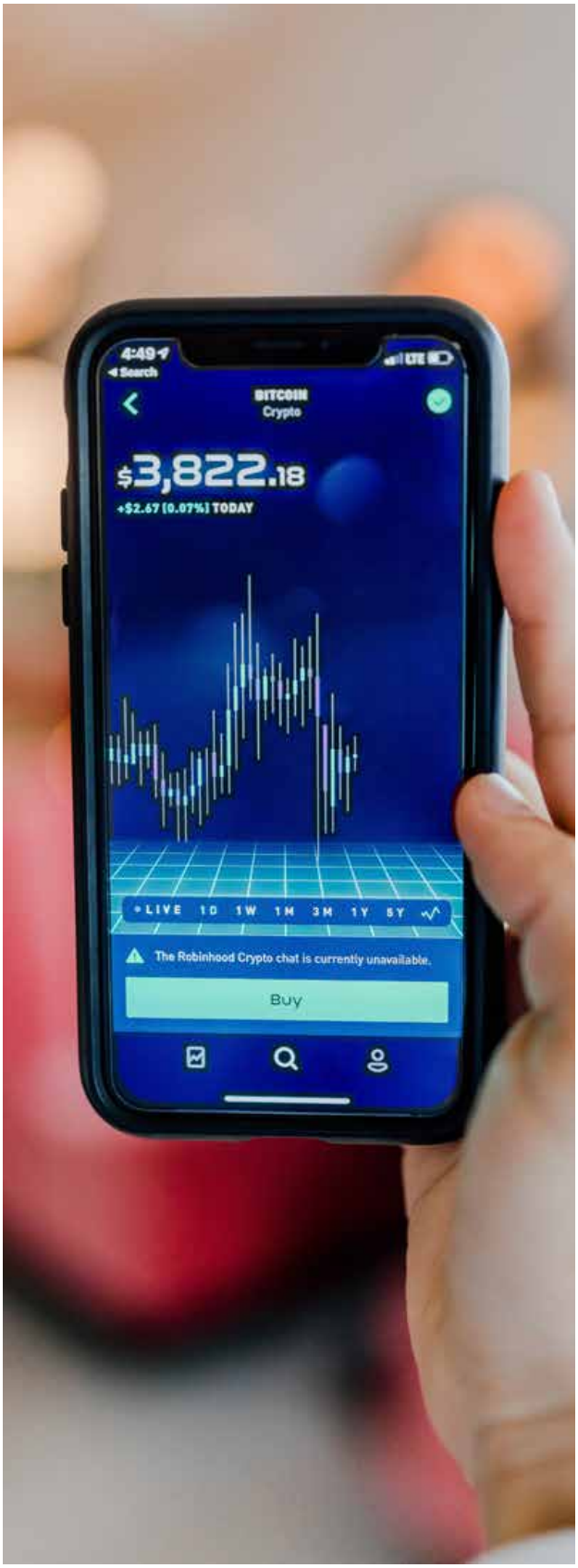
Otro tanto sucede con el horizonte temporal de los inversores: el de menos de 12 meses ha pasado del 33% hace ocho años hasta el 15% actual, mientras que el 51% de los ahorradores se decanta por el medio plazo (de 1 a 3 años) y 35% por el largo (más de 3 años).

Formación e información

Este viento de cola a favor de los instrumentos de inversión basados en seguros tiene también su reflejo en la formación de los nuevos mediadores de seguros. De hecho, los cursos formativos que han sustituido a

LO QUE HAY QUE SABER SOBRE IBIPS

Mercados financieros, fundamentos de cálculo y fiscalidad y, por supuesto, qué son y cómo funcionan los productos de inversión basados en seguros. Estos son los principales contenidos del curso 'Productos financieros: IBIPs' que el CECAS ofrece en modalidad de e-learning. Compuesto por 30 horas lectivas, el módulo aborda, entre otros aspectos, las ventajas y desventajas de las distintas opciones de inversión para los clientes de los mediadores de seguros, los potenciales riesgos financieros, la normativa fiscal aplicable y hasta la gestión del conflicto de intereses. También se estudian los Planes y Fondos de Pensiones.



partir de este año el Curso Superior de Seguros incorporan mucha más formación sobre IBIPs, o, lo que es lo mismo, productos de inversión basados en seguros como son los unit linked que incorporan un seguro de vida. "Son 50 horas en un programa de 200 para el nivel 2 y de 300 en el nivel 1. Ahora tiene entidad propia. La razón principal es que el regulador quiere proteger al cliente ya que, en este caso, el riesgo de la inversión recae sobre él", apunta Javier Romero, consultor y formador experto de Formación en Seguros.

Este experto, que ha colaborado con el CECAS en el desarrollo del módulo sobre IBIPs, recomienda a quienes vayan a distribuirlos "una formación de base, porque a veces encontramos a mediadores con mucha experiencia, pero que tienen pocos conocimientos de cálculo financiero, fiscal y de inversión".

Y hay una segunda parte, que es la información: "El mediador tiene que saber lo que está pasando en los mercados, si hay una crisis de semiconductores, por ejemplo; no es necesario que sea tan experto como un agente de bolsa, pero sí tener información periódica sobre estos asuntos", concluye Romero.

Luis Vallejo, director general comercial de Plus Ultra Seguros

"No tengo ninguna duda que los corredores serán capaces de seguir adaptándose a cualquier reto que se les plantee en el futuro". El director general adjunto comercial de Plus Ultra Seguros, Luis Vallejo, se muestra así de confiado en un canal, el de la Mediación, que seguirá siendo clave en el desarrollo de su compañía. Por eso, reconoce, "seguiremos fomentando su crecimiento" y le anima a seguir el camino de la digitalización y la conectividad para, junto al asesoramiento personal, tener realmente al cliente en el centro de las estrategias.

¿Cuáles van a ser las líneas principales de vuestra estrategia comercial en 2022?

Nuestra estrategia se asienta en la Mediación. Seguiremos fomentando su crecimiento y colaborando con el canal de forma muy estrecha. Para ello, avanzaremos en materia de conectividad, fomentando nuestra relación con las asociaciones y renovando los productos. También mantendremos el foco en el cliente, a quien queremos acompañar ofreciéndole servicios que le ayuden a prevenir riesgos y a vivir mejor. Desde el punto de vista de negocio, continuaremos esforzándonos en un crecimiento y un desarrollo equilibrado y uniforme.

¿Qué productos consideras más atractivos para el próximo año?

Nos encontramos inmersos en una potente renovación de nuestros productos, a los que estamos añadiendo servicios adicionales que ofrezcan un valor diferencial. Nos reafirmamos en una estrategia de mantener una oferta actualizada,

"La situación actual nos ha confirmado el enorme valor de la Mediación en la relación con los clientes"

adaptada a las necesidades del mercado y buscando siempre un equilibrio en la cartera. Continuamos focalizándonos en aquellos ramos estratégicos, como Particulares, Vida y Salud.

¿Surgen nuevas oportunidades tras la crisis de la pandemia?

La situación actual nos ha confirmado, una vez más, el enorme valor que tiene la Mediación en la relación con los clientes y la rápida adecuación que ha demostrado ante nuevos escenarios. Por otro lado, es evidente que están surgiendo nuevas formas de vivir, de trabajar, de movilidad urbana e incluso nuevos hábitos de consumo. Ante este escenario, debemos evolucionar al ritmo que lo hace la sociedad e innovar en soluciones que respondan a las necesidades que vayan surgiendo, así como adaptar los procesos y servicios a los retos que se van a plantear en el futuro.

¿Cómo pueden aprovechar los corredores estas oportunidades?

La digitalización está permitiendo a los corredores ganar en eficiencia, tiempo de respuesta y servicio a sus clientes. En este sentido, consideramos que es importante contar con productos conectados en plataformas para facilitar la gestión al corredor. Junto a los apoyos tecnológicos es fundamental la atención y el asesoramiento personal del mediador. Incluso los clientes más digitales, en algunos momentos, valoran el contacto presencial para exponer sus necesidades.

¿Cómo valoras el cambio de hábitos del cliente y de sus necesidades aseguradoras en la era postCovid?

En un entorno de avances en la digitalización y de cambio de hábitos de consumo, debemos colocar al cliente como punto central de nuestra estrategia. Esto nos ofrece las claves para entenderle mejor y responder a sus necesidades reales. Sabemos que nos enfrentamos a un cliente cada vez más digitalizado, que valora que se le ofrezca diferentes vías de acceso y comunicación con su mediador o compañía. En este sentido, la tecnología debe servirnos para acercarnos y adaptarnos a él. Entendemos la digitalización como un instrumento de apoyo y complemento que nos permita mejorar nuestro servicio.

¿Cuáles son, desde tu punto de vista, los 3-4 retos principales que debe afrontar la Mediación?

La digitalización del sector es uno de los desafíos principales, entendida como un instrumento que facilita su labor diaria y que redunda en un mejor servicio a sus clientes. Por otro lado, hay que avanzar en materia de conectividad, para lograr mayor nivel de agilidad y eficiencia. Además, la Mediación es clave a la hora de asesorar al cliente y de generar una relación de confianza, que incremente la presencia de productos de previsión social, claves ahora y en el futuro, entre otros.

El proceso de adaptación de los corredores a los retos de la profesión, ¿es el adecuado?

Los corredores tienen una gran capacidad para adoptar cambios e introducirlos de manera natural en su actividad y así se ha demostrado. En un momento como el que nos ha tocado vivir, el sector en general; y los corredores en particular, han sabido adaptarse a una nueva metodología de trabajo, ya no solo de forma eficaz, sino que lo han hecho en un periodo de tiempo muy breve. No tengo ninguna duda que los corredores serán capaces de seguir adaptándose a cualquier reto que se les plantee en el futuro.

"La digitalización está permitiendo a los corredores ganar en eficiencia, tiempo de respuesta y servicios a sus clientes"

Sigue la denuncia contra la mala práctica de la banca

El Consejo General sigue trabajando de forma muy activa en defensa de la profesión. En esta línea, ha mantenido reuniones institucionales con representantes de la Administración Pública, más allá del sector asegurador, a los que ha trasladado las preocupaciones del colectivo mediador y, en particular, las relativas a los posibles abusos de la banca en la venta de seguros.

La institución refuerza con estos contactos su valor como Corporación de Derecho Público que representa a toda la profesión. Además, ha logrado la voluntad de las distintas instituciones para colaborar en favor de los derechos de los clientes y la credibilidad del sector.

Entre otros, los representantes de Consejo General, encabezados por su presidente Javier Barberá, se han reunido con el secretario general del Ministerio de Consumo, Rafael Escudero, que mostró su disposición a colaborar con los mediadores para realizar, dentro de sus competencias, las actuaciones precisas para evitar malas prácticas que perjudican al consumidor. Además, propuso abrir una vía de contactos regulares entre el Consejo y el equipo técnico del Ministerio.

De la misma manera, tras la reunión mantenida con Bartolomé Martínez, director del Área de Economía y Hacienda del Defensor del Pueblo, ambas partes han acordado abrir una línea de colaboración para canalizar las posibles infracciones en la comercialización de seguros y actuar según sus competencias en defensa de los derechos del cliente.

Competencia y Banco de España

Además, la institución colegial trasladó a la presidenta de la Comisión Nacional del Mercado de la Competencia, Cani Fernández, la necesidad de establecer un sistema de control en el proceso de contratación de seguros en sucursales para asegurar que la entidad bancaria está cumpliendo la normativa sobre operaciones combinadas.

Por otro lado, en la reunión que Barberá mantuvo con el equipo del Banco de España (Fernando Navarrete, director del Gabinete del Gobernador, Fernando Tejada, director del Departamento de Conducta de Entidades, y Arancha Gutiérrez, responsable de la Unidad Normativa de Transparencia) señaló la necesidad de regular las prácticas comerciales de las entidades bancarias para mejorar en transparencia y establecer reglas de actuación definidas que protejan al cliente.

Sentirse **seguro**

En IRIS GLOBAL ponemos a tu disposición todo lo que tus clientes necesitan

Los Seguros de **Defensa Jurídica** ofertan a Pymes, autónomos, particulares y familias, las mejores coberturas para que puedan centrarse en lo que de verdad importa sin preocuparse por los aspectos legales.

917 70 07 17
www.irisglobal.es

IRIS GLOBAL
Iris Global Soluciones de Protección Seguros y Reaseguros, SAU

¿Lluvia de millones para digitalizar las pymes?

Las pymes españolas esperan el reparto de cerca de 5.000 millones de euros para impulsar sus procesos de digitalización casi con más ilusión que al sorteo de lotería de Navidad. Forman parte de unas medidas ya anunciadas el año pasado, confirmadas a principios de éste y que se espera que empiecen a ejecutarse plenamente en 2022. Como pymes o autónomos, la inmensa mayoría de corredurías y corredores de seguros teoricamente podrían beneficiarse de ellas y dar el impulso decisivo a su modernización, subiéndose, así, al tren de la digitalización.

Todo está preparado para que, en las primeras semanas de 2022 se pongan a disposición de las pymes españolas las primeras partidas de euros para potenciar su digitalización. Al menos, así lo anunció a finales de septiembre la secretaria de Estado de Digitalización e Inteligencia Artificial, Carme Artigas. Se trata del Plan de Digitalización de Pymes, un proyecto a cinco años al que el Estado dotará con casi 5.000 millones de euros para apoyar el crecimiento, la competitividad e internacionalización de 1,5 millones de pequeñas y medianas empresas, autónomos y micropymes, mediante el impulso de su transformación digital, incluyendo la inversión en capacitación y herramientas digitales, como páginas web, aplicaciones para la gestión empresarial, marketing digital o canales de venta por internet, entre otras cosas.

El plan se articula en 5 ejes:

- impulso a la digitalización básica
- apoyo a la gestión del cambio
- innovación disruptiva y el emprendimiento digital
- apoyo a la digitalización de algunos sectores estratégicos
- reforma de los instrumentos y redes de apoyo al emprendimiento, la innovación y la digitalización de las pymes

Dentro de este amplio plan, Digital Toolkit es el programa más ambicioso. Cuenta con 3.000 millones de euros para su implantación y va destinado a financiar la integración en las pymes de un conjunto de paquetes básicos de digitalización (herramientas habilitadoras, formación, página web, sistema de gestión de recursos ERP, sistema de gestión de clientes CRM, venta por internet, marketing digital, ciberseguridad). Para su despliegue e implementación se considerarán diferentes instrumentos de colaboración público-privada que permitan acelerar la digitalización de las pymes, especialmente micropymes y autónomos, como es el caso de pequeñas corredurías y corredores de seguros.

El otro programa interesante de este plan, y que también puede ser utilizado por corredores y corredu-

“El programa Digital Took es el más ambicioso y está destinado a financiar paquetes básicos de digitalización”

rías, es el de Agentes del Cambio. Dotado con 300 millones, se destinará a financiar la incorporación de profesionales en transformación digital en las pymes para desarrollar su plan de digitalización y acelerar su transformación digital. Es decir, se subvencionará la contratación de un técnico que desarrolle el plan de digitalización.

El Sector, atento a las ayudas

La industria aseguradora y los colegios de mediadores a través del Consejo General están pendientes del reparto de estas ayudas para informar y facilitar a sus

¿POR QUÉ ESTOS PLANES?

En España, según datos oficiales, las empresas de menos de 50 trabajadores, micropymes y autónomos, suman el 98,99% del total de empresas y mantienen sobre sus espaldas casi la mitad del empleo de todo el país (el 49,58%). El peso de las pymes es aquí mayor que en el conjunto de la UE, situándose su contribución al empleo y valor añadido bruto empresarial, aproximadamente 5 puntos porcentuales por encima de las respectivas medias europeas.

Los últimos datos de la Dirección General de Industria y de la Pequeña y Mediana Empresa, correspondientes a septiembre, el número de pymes en España era de 2.919.456. Por número de trabajadores se dividen en microempresas (1-9 asalariados): 1.123.936; pequeñas (10-49 asalariados): 155.502 y medianas (50-249 asalariados): 25.253.

UN DINERO PARA....

Según el plan, los pequeños y medianos negocios mediadores podrán destinar estas ayudas a:

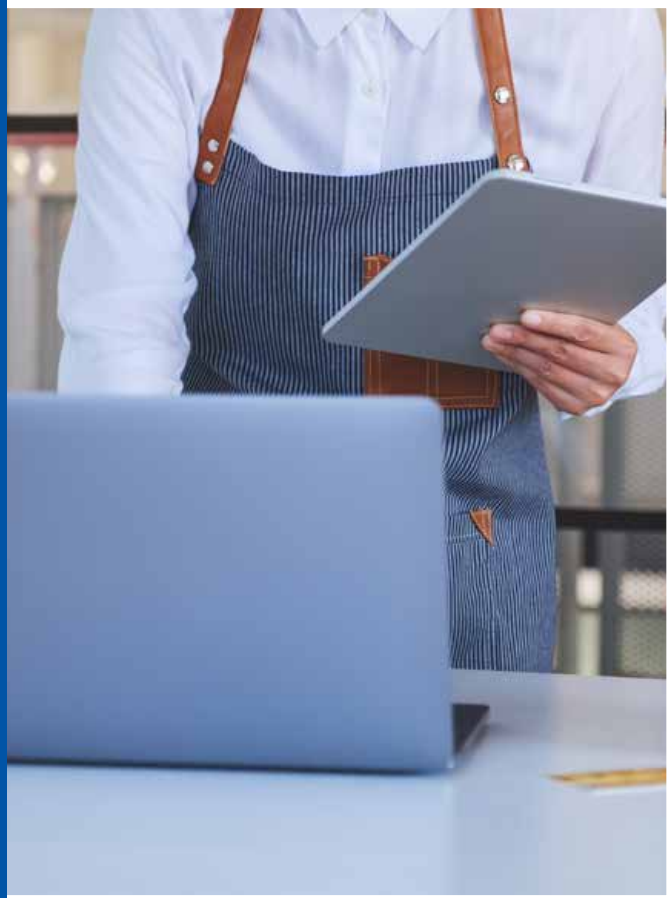
- Incrementar la presencia en Internet: inversión en web, redes sociales, etc. y todo lo relativo al marketing digital.
- Mejorar la conectividad a Internet, mediante la contratación de paquetes más amplios, mayor ancho de banda, redes privadas virtuales, herramientas de teletrabajo, etc.
- Impulso de la venta a distancia y el comercio electrónico. Lograr la mayor conectividad con los procesos y ser capaces de facilitar la emisión online de pólizas.
- Formación de directivos y personal en la gestión digital de la empresa.
- Inversión en sistemas de gestión de recursos ERP, gestión de clientes CRM, así como ampliación de los programas de gestión de las correduría.
- Inversión en ciberseguridad para cubrirse de las posibles amenazas cibernéticas de la digitalización.
- Implementar la Inteligencia Artificial en los procesos.
- Inversión en renovación y modernización de equipos y redes informáticas.
- Contratación de profesionales especializados en transformación digital

asociados el acceso a las mismas. También desde proyectos tecnológicos sectoriales, como CIMA, esperan como agua de mayo las condiciones de dichas ayudas para poder beneficiar con ellas a los mediadores en su transición tecnológica hacia la digitalización.

El denominado Plan de Digitalización de Pymes, junto al Plan de Digitalización de las Administraciones Públicas y el Plan Nacional de Competencias Digitales son tres de las medidas para este trienio enmarcadas dentro de la Agenda España Digital 2025 y financiados por los fondos europeos del Mecanismo de Recuperación y Resiliencia.

El Plan de Digitalización de las Administraciones Públicas prevé movilizar una inversión pública de, al menos, 2.600 millones para los próximos tres años, destinados a mejorar la accesibilidad de los servicios públicos a los ciudadanos y empresas.

Por su parte, el Plan Nacional de Competencias Digitales está dotado con 3.750 millones en el período 2021-2023 y tiene como objetivo alcanzar un nivel de capacitación digital entre la ciudadanía española que esté a la altura del reto del proceso de digitalización.



PlusUltra Seguros

Seguridad que se comparte

Pase lo que pase, total tranquilidad

Seguros de vida

Empieza a estar cubierto de cara al futuro desde hoy para que tú y los tuyos podáis disfrutar de la vida con tranquilidad. Si quieres asegurar la protección de tu familia y no correr riesgos, nuestros seguros de vida te darán la tranquilidad que necesitas.

www.plusultra.es

Actualización de Windows 11: cuestión de seguridad

Los equipos informáticos están expuestos a muchas vulnerabilidades por lo que la actualización del sistema operativo es vital para conservar la privacidad de los datos y evitar daños en el dispositivo. Con el lanzamiento de Windows 11, Microsoft refuerza la seguridad frente a versiones anteriores.

La falta de prevención es una de las principales causas de los miles de ataques informáticos que se producen en el mundo diariamente. Contar con un buen antivirus, utilizar contraseñas seguras o prestar especial atención a los archivos adjuntos o enlaces que recibimos a través del correo electrónico son algunas de las acciones preventivas que hemos interiorizado en los últimos años. Pero ¿qué hay de las actualizaciones del software que tenemos instalado en nuestros equipos?

Sistema operativo: el corazón del equipo

Cualquier programa informático cuenta con vulnerabilidades que los hackers pueden aprovechar para robar información, suplantar nuestra identidad o infectar el sistema con algún virus. Por esta razón, según los expertos, es importante, siempre que sea posible, no usar versiones desactualizadas: a pesar de funcionar correctamente, pueden estar expuestas a fallos, que suelen corregirse con parches de seguridad en cada actualización.

"Las actualizaciones periódicas protegen los equipos ante ciberamenazas"

El sistema operativo es el corazón de cualquier dispositivo y requiere actualizaciones periódicas con el fin de mejorar el rendimiento del equipo y, lo más importante, protegerlo ante ciberamenazas.

Windows 10

Windows es un sistema operativo que, habitualmente, cuenta con una gran cantidad de vulnerabilidades. Constantemente surgen nuevos virus, spyware, bugs (errores de software) que necesitan la revisión y actualización del software. Para solucionar estos problemas, existen las actualizaciones de Windows, visibles a través de Windows Update.

Hasta la fecha, todas las versiones de Windows solían tener un recorrido parecido: se lanzaba su versión principal, y con el tiempo se lanzaban dos o cuatro grandes actualizaciones, los Service Packs, hasta la próxima versión de Windows. Sin embargo, con Windows 10, Microsoft cambió la filosofía y adoptó otra conocida como Rolling Release o lanzamiento rotativo. En este caso, la versión del sistema operativo es siempre la misma, pero va recibiendo novedades con actualizaciones frecuentes.

Así, desde que salió Windows 10, en julio de 2015, los usuarios han tenido siempre la misma versión que se ha ido mejorando año tras año con actualizaciones. Las principales: dos grandes actualizaciones al año, que añaden nuevas funciones y características al sistema operativo.

Windows 11: listo para su descarga

Hace algunas semanas, Windows 11 pasó a estar disponible para todos los usuarios.

Desde la publicación de su disponibilidad, Microsoft ha comenzado el despliegue gradual de su sistema a través de una actualización gratuita, que llegará a los ordenadores con Windows 10 que cumplan con los requisitos. Estos son: tener una unidad de al menos 64GB, procesador de dos núcleos, TPM 2.0, 4GB de memoria RAM, firmware UEFI y tarjeta gráfica compatible. Aun así, Microsoft ofrecerá la aplicación PC Health Check para saber si un ordenador es compatible con la nueva versión.

"Microsoft ha comenzado el despliegue gradual de su sistema a través de una actualización gratuita"

Este sistema por fases tiene como objetivo garantizar la calidad del despliegue en el que tendrán prioridad los equipos nuevos. Después, se irá extendiendo al resto de equipos mediante el uso de un sistema de priorización inteligente que evaluará, entre otros aspectos, el hardware de cada dispositivo. Los usuarios que tengan un ordenador con Windows 10 apto para actualizar a la nueva versión recibirán un mensaje de Windows Update cuando la instalación esté disponible.

Además de las mejoras visuales, la nueva versión de Windows incorpora funciones como una gestión de ventanas más eficiente; nuevos widgets que recuerdan a los de Windows Vista, un nuevo menú de inicio con diseño mejorado y ventanas flotantes transparentes, la integración de Teams en la barra de tareas o numerosas mejoras para gamers y la tienda de Windows.

CÉSAR GARCÍA

Mediador de Seguros.
Doctor en Derecho

Valor añadido del mediador en los riesgos extraordinarios

Estos meses estamos viendo, con pesar e impotencia, como la lava del Cumbre Vieja está engullendo las viviendas de muchos de nuestros conciudadanos. Toda la sociedad se está volcando en apoyar a través de donativos, envíos de artículos de necesidad, voluntariado..., para minimizar el impacto del volcán, al menos en el ámbito material.

Según datos de la patronal del sector, en la isla de La Palma había muy poca penetración de los seguros de hogar, lo que hace que muchos de los damnificados, al carecer de un seguro, no reciban las indemnizaciones del Consorcio de Compensación de Seguros por la pérdida del inmueble.

A la luz de los hechos y de la conciencia de tener nuestro patrimonio asegurado, se han disparado las contrataciones de este riesgo en la isla. No obstante, muchos consumidores tienen su póliza de hogar vinculada al contrato hipotecario, donde el banco aparece como beneficiario de la indemnización en caso de pérdida total de la vivienda.

Indemnización para el banco

Esta situación supone que decretada la pérdida total del bien, la indemnización no irá al propietario, sino al acreedor hipotecario, quedando, en la mayoría de las ocasiones, la hipoteca cancelada por pago anticipado, pero el consumidor se quedará sin casa. De otro lado, en las pólizas suscritas a través de un mediador de seguros (agente o corredor), se coloca como beneficiario de la indemnización al propietario de la vivienda.

Mejor con un mediador

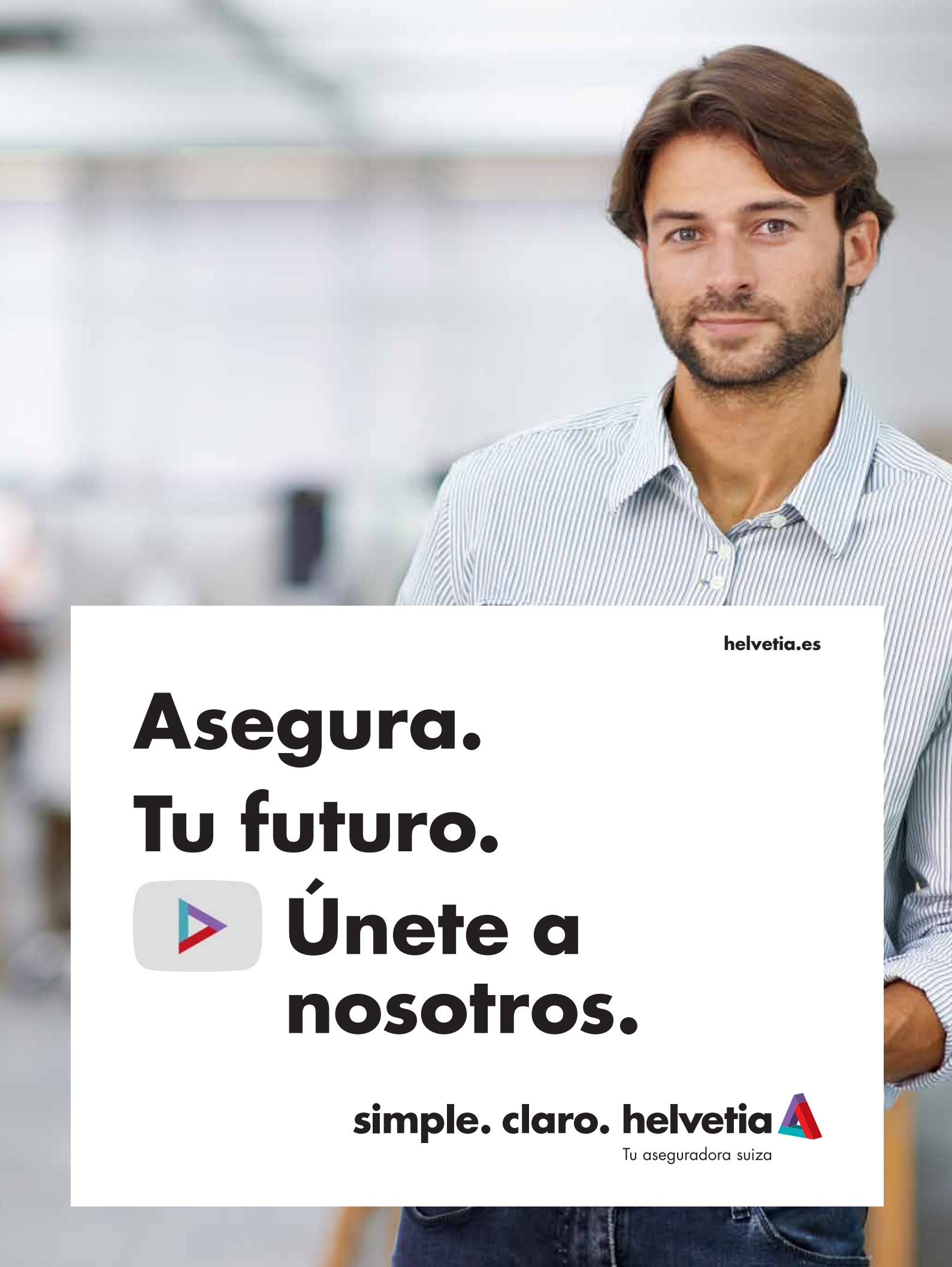
Contratando el seguro a traves de un mediador lo normal es que la indeminación irá al propietario. Eso sí, deberá seguir pagando la hipoteca como venía haciendo hasta la fecha. Pero, "no se quedará sin casa", salvo que fuera imposible su reconstrucción, donde sí podrá cancelar la deuda, aunque en este caso será él quien decida si reconstruye o si liquida la hipoteca. Por las imágenes que vemos a diario, muchas viviendas no se podrán reconstruir, pero algunas otras sí.

Y fuera de la situación del volcán, como son las DANAS, los terremotos de Lorca, es también interesante saber que podremos designar, como beneficiarios de la indemnización, a los propietarios y no a los acreedores hipotecarios, por lo que recibirá el consumidor la indemnización, rehabilitará o reconstruirá su vivienda y seguirá pagando la hipoteca como tenía previsto.

Para los que aún están pagando la hipoteca de su vivienda, cabe formular la siguiente pregunta: Tras una catástrofe consorciable, ¿qué queremos, no tener hipoteca o no tener casa?

Si queremos no tener hipoteca, dejemos designado como beneficiario a la entidad financiera. Si queremos tener casa, vayamos a un mediador (agente o corredor) y dejemos designado como beneficiario al propietario. Estamos por lo tanto ante una ventaja más de contratar nuestra póliza a través de un agente o un corredor.

En el caso que nuestra póliza ya está contratada a través de un banco, ¿no podemos cambiar el beneficiario? Sí se podrá, pero, para ello, recomendamos no acudir directamente al banco, sino hacerlo con el asegurador o con un agente de la compañía con quien tengamos la póliza o con un corredor de seguros, que asesorará al consumidor sobre cómo poder hacer ese cambio.


helvetia.es
Asegura.
Tu futuro.
Únete a
nosotros.
simple. claro. helvetia
Tu aseguradora suiza

*Consulta condiciones en mapfre.es. Planes de Pensiones promovidos y gestionados por MAPFRE VIDA PENSIONES. Entidad depositaria de los Fondos de Pensiones BNP PARIBAS. Existe un documento de datos fundamentales a disposición de los partícipes en la WEB.

MAPFRE

Tu aseguradora global de confianza