ARTÍCULO

LA ESCALADA DEL CIBERRIESGO

EN LA AGENDA DEL DIRECTIVO

medio
corredores de seguros

2020_
BEATRIZ CARRATALÁ

LA ESCALADA DEL CIBERRIESGO

EN LA AGENDA DEL DIRECTIVO

El **riesgo cibernético** ya no puede seguir mirándose de reojo ni por pequeñas ni por grandes empresas, la indiscutible dependencia de los negocios en la economía digital es hoy, sin saberlo, el **talón de Aquiles de muchas empresas.**

En España, el **coste de los ciberataques** ya se cifra en **40 millones de euros**, dirigiéndose el 70% hacia la pequeña y mediana empresa.

Mientras, **ocho de cada diez micropymes españolas no están preparadas para un ataque cibernético** (Informe de Ciberpreparación_Hiscox 2020), lo que no extraña, pues el 99,8% del tejido empresarial español no se considera un objetivo atractivo para un ciberataque ("Panorama actual de la Ciberseguridad en España" (2019) Google).

ESPAÑA_ **TRES MILLONES** DE EMPRESAS **SIN PROTECCION** FRENTE A HACKERS.

Esta falta de concienciación se traduce en que **casi 3 millones de empresas en España están poco o nada protegidas contra hackers**, apenas el 36 % de las pymes encuestadas tienen establecidos protocolos básicos de seguridad y sorprende confirmar que, todavía a día de hoy, mantienen una cultura de la ciberseguridad peligrosamente reactiva, mientras la realidad es bien distinta, la pyme es el eslabón más vulnerable de la cadena.

Solo en 2019 el Centro Criptológico Nacional (CCN) gestionó **42.997 incidentes de ciberseguridad**, al tiempo que el INCIBE_CERT se ocupó de **107.397 incidentes**, de los cuales 72.858 correspondieron a ciudadanos y empresas y 33.743 a la red académica.

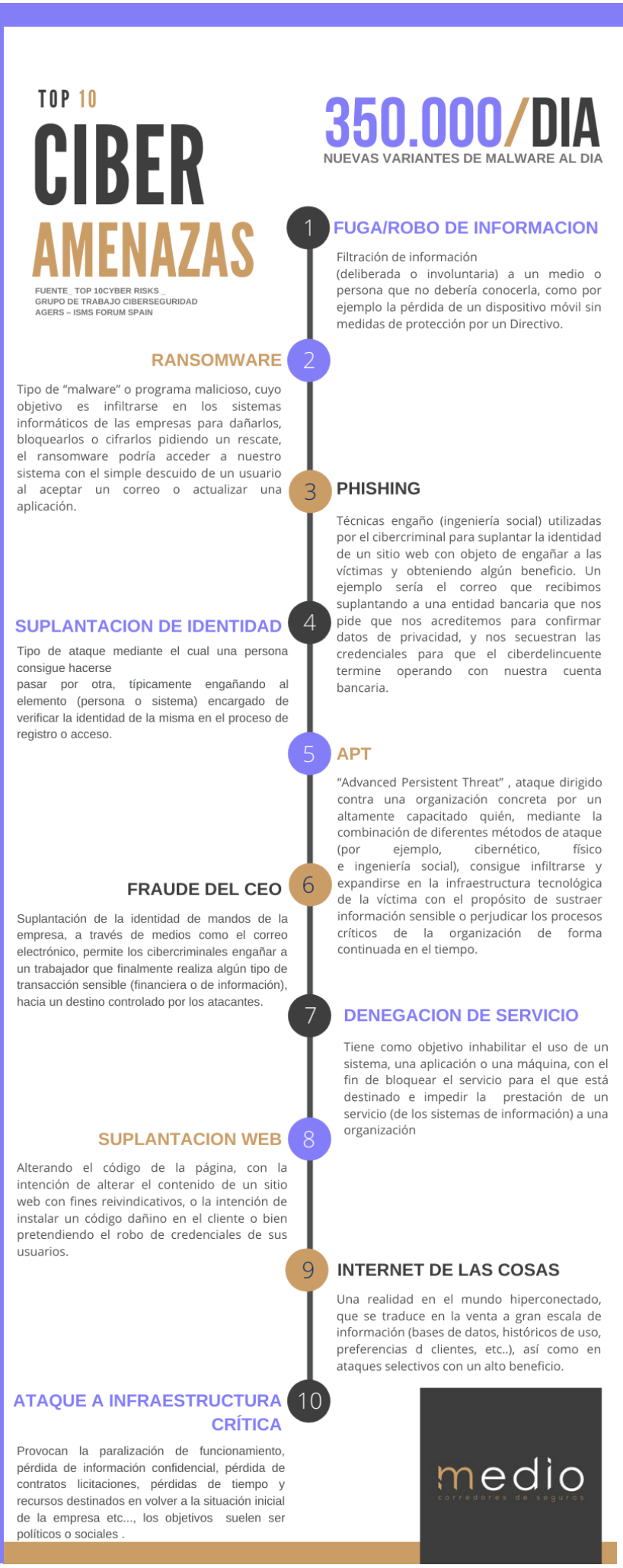
La **imparable y rápida evolución del entorno digital**, no nos ofrece un único cariz positivo favorecedor de la innovación estratégica, interconectividad y digitalización del tejido empresarial español, esta, **es sólo una cara de la moneda.**

En la **otra cara**, tenemos **ciberdelincuentes** avezados que alimentan su creatividad de forma igualmente exponencial y cada vez más sofisticada, dificultando la adaptación y protección de las empresas a esta amenaza invisible con no improbables efectos devastadores.

PRIMER RIESGO MUNDIAL

El **Fondo Económico Mundial**, refiere en su reciente Informe de Riesgos Globales 2020 que los **ataques cibernéticos se encuentran dentro de los diez principales riesgos que enfrentaremos a nivel globa**l durante 2020.

En lo que respecta al **ámbito empresarial,** por primera vez en la historia, los **incidentes cibernéticos aparecen como el más importante riesgo para las empresas a escala mundial**, por delante del hasta ahora primero en la clasificación como primer riesgo, la pérdida de beneficios, según las conclusiones del noveno Barómetro de Riesgos de Allianz 2020.



Y es que la cuestión no es baladí, **un ciberataque puede comprometer seriamente la continuidad de una empresa saneada**, pues la potencialidad de su ocurrencia y la magnitud de sus efectos son ambas cuestiones de difícil pronóstico y cuantificación, razón por la cual **riesgo cibernético es protagonista hoy en la agenda de todo directivo**, para quién protegerse ante lo incierto debe ser hoy más que nunca un objetivo en el que la empresa en su conjunto esté implicada y comprometida.

El **60% de las pymes europeas víctimas de ciberataques,desaparece a los 6 meses siguientes al incidente,** en su mayoría lastradas por el coste medio del ataque.

El **coste medio necesario para restablecer la actividad** de las compañías españolas tras un fallo de seguridad **superó los 75.000 euros,** incluyendo en el coste la detección, investigación, gestión y recuperación del incidente, así como acciones posteriores para mitigar la interrupción del negocio y la pérdida de clientes.

- Interrupción del negocio
- Pérdida de información
- Pérdida de ingresos
- Deterioro de marca
- Deterioro reputacional
- Sanciones legales
- Responsabilidad civil
- Daños en los equipos
- Costes técnicos de investigación
- Costes técnicos de remediación

OBSERVAR PARA PREVENIR

El **análisis, externo e interno, del entorno digital de la empresa**, deben ser **el primer foco de atención**, y ello porque sólo si el Directivo tiene una comprensión adecuada de los riesgos cibernéticos, podrá mitigar su impacto.

Esta **actitud proactiva** le permitirá establecer **protocolos eficaces de prevención y mitigación** de aquellos potenciales ataques, asignando los oportunos recursos económicos y humanos que le permitan navegar de forma más segura en la incertidumbre del entorno digital.

La **conciencia del impacto del cibercrimen en la cuenta de resultados de la empresa será clave para el desempeño de todo directivo** que busque maximizar el valor de su empresa también a través de una estrategia adecuada de ciberseguridad que le permita innovar de forma segura y crecer con confianza.

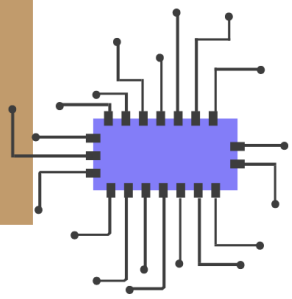
UN RIESGO POTENCIALMENTE SEGURO

CON PÓLIZA CIBERRIESGO

Hoy, **todo emprendedor** autónomo, propietario, directivo o trabajador de una pyme, **está expuesto a ser blanco de un ciberataque**, pues con toda seguridad trabaja con un dispositivo con acceso a internet, se comunica con sus clientes, proveedores y compañeros a través de redes sociales, apps móviles, y correo electrónico, realiza a diario transacciones bancarias y cuenta con un CRM o website corporativa.

Así, en este marco tan desdibujado, con una deficiente preparación de las empresas y una cada vez mayor dependencia tecnológica de las mismas, hay una cosa cierta, **España es el 12º país más atacado diariamente**, donde un **68% de los ataques se dirigen a empresas y particulares**, es por ello que hoy en día t**oda empresa, autónomo particular que realice una correcta gestión de riesgos, debe contar con una solución aseguradora adecuada,** un seguro con cobertura específica ante el riesgo Cibernético, con carácter general y con carácter especial perfectamente adecuado a su negocio y riesgo informático, que active un correcto ciclo de coberturas y servicios que den la máxima respuesta a los diferentes daños y responsabilidades que se desencadenan a causa de un ataque o incidente informático, incluyendo los adecuados servicios especializados (informáticos, legales,..) para gestionar el incidente y ofreciendo la adecuada protección financiera para cubrir las consecuencias económicas, legales y reputacionales derivadas del mismo, con el objetivo de garantizar la continuidad de la empresa.

ACCIÓN EXTERNA



Profesionalización del atacante, especialización por objetivos.

Ataques menos dirigidos y más masivos.

Los datos no son el único objetivo.

Nuevas amenazas a sistemas centrales de industrias buscan la destrucción de cadenas de suministro e infraestructuras industriales críticas.

Ataques de mayor impacto.

Metodología de ataque avanzada orientada a explotar el factor humano a través de ataques de ingeniería social.

CIBER ATAQUE

PRO_ACCIÓN INTERNA

Auditoría interna de exposicion al riesgo cibernético.

Formación y actualización contínua acerca de riesgos y amenazas informáticas.

Cultura empresarial comprometida con la seguridad informática.

Testeo y actualización de sistemas constante.

Reforzar la securización de sistemas y protocolos de acceso.

Plan de contingencia para la mitigación de consecuencias del ataque y garantizar la continuidad de la empresa tras el indicente.

Póliza de Ciberriesgos adecuada a la empresa y riesgo.