Eleven Paths

Ciberseguridad para pequeñas y medianas empresas

Claves para su “nueva normalidad”

Telefónica CYBER SECURITY COMPANY

elevenpaths.com

01

Resumen ejecutivo

El largo y lento proceso de digitalización en las empresas pequeñas y medianas es un debate que lleva años sobre la mesa. Sin embargo, y debido a los cambios de hábitos de consumo y de los procesos productivos derivados de la emergencia sanitaria de la COVID-19, este proceso ha experimentado una fuerte aceleración en poco tiempo.

La digitalización ha pasado de ser una buena oportunidad de crecimiento a su tabla de salvación. Esto ha tenido como consecuencia directa que en todo el mundo se haya avanzado más en los últimos meses que en los últimos años.

Sin ir más lejos, en este segmento el comercio electrónico ha crecido en Argentina en 2020 un 35% interanual, según un informe de la consultora Focus Market.

En este marco digital, toma mayor relevancia **la urgencia de que las pymes tengan una estrategia de ciberseguridad que haga esa digitalización viable**. Además, las empresas que pertenecen a este segmento ya tenían una asignatura pendiente desde hacía tiempo con la ciberseguridad, ya que un gran porcentaje de las que sufren un ciberataque no se recuperan.

Por tanto, y como en todas las grandes crisis, hay que ver la situación actual de incertidumbre como una oportunidad histórica para que haya profundas reformas en este segmento empresarial que ayuden a hacer que sus **negocios sean más sostenibles y competitivos.**

En este documento, explicaremos la situación actual de la ciberseguridad en estas empresas partiendo de su definición, el estado de su digitalización, las consecuencias que ha tenido y tendrá la pandemia acaecida este mismo año, la propuesta de ElevenPaths y los beneficios que aporta esta propuesta a los clientes.

02

Contexto empresas pequeñas y medianas

A. ¿Qué es una pyme? Las pymes en cifras

Pero... ¿qué es una pyme? Es la pregunta que nunca falta en cualquier conversación sobre empresas de este segmento y realmente no hay una respuesta única para ella. Es decir, la respuesta depende directamente del contexto geográfico donde se realice. Cada país o área geográfica tiene potestad para definir que es una empresa pequeña y mediana en su región. La definición podría venir dada por aquellas empresas que están bien por debajo de un determinado número de empleados, por debajo de un determinado volumen de facturación, o por una combinación de ambos parámetros.

Por ejemplo, el número de empleados de una pyme dentro de América Latina es similar, un máximo de 200 empleados; que no es igual al número de empleados de la Unión Europa, que está en torno a los 250 empleados, y ambas están lejos de las pymes de Estados Unidos que se sitúan en torno a los 500 empleados. A esto hay que añadir que en todos los países se hace una subsegmentación interna de este tipo de empresas. Un ejemplo sería, autónomos, soho, pequeñas y medianas.

Mientras que en América Latina la definición viene dada por uno de los dos parámetros, en España es la combinación de ambos los que las definen.

Ahora bien, en lo que hay una clara unanimidad es en la importancia económica de las empresas de este segmento ya que son la espina dorsal del tejido empresarial en todos los países. Representan un alto porcentaje en volumen de tejido empresarial y de aporte al PIB.

Tanto en Europa como en América Latina, estas empresas representan el 99% del tejido empresarial y a nivel mundial no es inferior al 90% en ningún caso. El aporte al PIB es del 56% en Europa y el 25% en América Latina.

A pesar de que las empresas de este segmento son las más vulnerables en tiempos de incertidumbre económica, su buena salud es fundamental porque son el motor de la economía.

B. Madurez digital

La madurez digital es el término que explica el nivel de adopción de las tecnologías que se ha realizado por parte de una empresa dentro de las posibilidades existentes. Es decir, en qué punto se encuentra dentro del proceso de transformación digital.

Por lo tanto, podríamos decir que la madurez digital de una empresa **nos dice cuánto hace la tecnología por el progreso de esa empresa**. El objetivo final de este recorrido por la transformación digital será el obtener el máximo beneficio de las nuevas tecnologías para el rendimiento de la compañía.

En función de su grado de evolución hacia la digitalización, variarán las soluciones que necesitan para mejorar su madurez y, por consiguiente, los riesgos a los que se exponen.

Alcanzar este objetivo no es algo que vaya a suceder de la noche a la mañana, sino que las compañías tienen un camino que recorrer y que irán avanzando de forma paulatina. Es más, no es un camino que tenga una meta clara, puesto que el entorno digital es un entorno siempre vivo en el que las actualizaciones son una constante.

La transformación digital se puede decir que tiene dos grandes dimensiones: la interna y la externa.

La perspectiva externa

Hace referencia a cómo se presenta la empresa ante sus consumidores y cómo se relaciona con ellos. Para que esta aproximación sea correcta, hay que entender que esos clientes (existentes y potenciales) ya son digitales, y por lo tanto habrá que adaptarse a esa situación sino se quiere errar en el intento.

En esta perspectiva es dónde más han podido avanzar las empresas, debido al impacto directo que esta relación con el cliente tiene en sus ingresos. Por tanto, si el cliente ya es digital es fundamental tener esa visibilidad digital también y estar en los mismos entornos que ellos.

En la actualidad, la primera acción que realiza cualquier consumidor cuando está valorando el adquirir un producto o servicio es la búsqueda online de las opciones existentes. Sabiendo que esta es la situación real de los consumidores, **las empresas deben encontrarse de la forma más visible y eficiente posible en esta plataforma digital.**

Esto no significa que todas tengan que poder vender online, pero sí saber que ha entendido perfectamente todas las soluciones existentes y posteriormente han escogido e implementado la solución más beneficiosa de las posibles.

La perspectiva interna

Hace referencia a todo aquello que para el cliente es transparente. Es decir, a los procesos internos y a la forma de trabajar de la compañía.

Por procesos internos hacemos referencia a una gran cantidad de **tareas de carácter repetitivo y mecánico.** La digitalización de estos procesos supone el uso de todas aquellas herramientas que hacen más eficiente y fiable estas labores.

Es habitual que las empresas de este segmento realicen gran cantidad de tareas de forma manual, con el consiguiente coste económico, y con un aumento de probabilidad de error. La inclusión de herramientas maduras en el mercado que permitan la automatización de los procesos, como el CRM para todo el manejo de datos de la compañía, es un claro ahorro de esfuerzos. La digitalización de estos procesos aumenta la productividad y la eficiencia. También la inclusión de tecnologías como *Cloud* y sus herramientas colaborativas, el *Big Data* que ayuda a mejorar la toma de decisiones de negocio basándose en datos o las tecnologías IoT y sus funciones de apoyo a la logística, pueden ser potenciadores de productividad en muchas empresas.

Respecto a la forma de trabajar, va más allá de la adopción de nuevas tecnologías. Un cambio en la forma de trabajar es un cambio de hábito y este puede llevar un tiempo de adopción para que la asimilación sea correcta.

Dentro de estas nuevas formas de trabajar, se debe tener en cuenta el uso de **metodologías Ágiles**. El principal objetivo de este tipo de metodologías es tener como prioridad la satisfacción del cliente y, por tanto, la empresa debe tener la capacidad de responder rápidamente ante cualquier situación y ser rápida en la adaptación a ambientes cambiantes.

Sin embargo, el mayor cambio ocurrido en los últimos tiempos en la cultura empresarial ha sido la forma de relacionarse con compañeros, clientes y proveedores. Se ha pasado de la tradicional forma presencial, a establecer relaciones únicamente online a través de videoconferencias, teléfono...etc. **Un cambio potenciado por la llegada de la COVID-19 y que ha puesto de manifiesto que los que mejor se han podido adaptar son aquellos que estaban más avanzados en su digitalización.**

La relevancia de la sostenibilidad de las pymes para la economía supone a los gobiernos apoyarlas a través de financiación. Pero estas ayudas serán solo temporales y los negocios que se pretendan mantener en el mercado y los que deseen crecer serán necesariamente digitales. La tecnología se presenta más accesible que nunca y las nuevas empresas que han surgido en los últimos meses son ya nativas digitales.

Por último, no es el momento de recortar esfuerzos en transformación digital, sino de prepararse para un futuro sostenible e incierto.

Según un estudio realizado por Sage, el 48% de las pymes invertirá en digitalización como parte de su estrategia empresarial para adaptarse a la nueva situación.

C. COVID-19 - La "nueva normalidad" de las pequeñas y medianas empresas

El pasado 12 de marzo la OMS declaraba la COVID-19 como una pandemia mundial y como consecuencia a los pocos días en algunos países como España se estableció un confinamiento domiciliario con el fin de evitar el colapso total del sistema sanitario.

Según la encuesta sobre pymes y digitalización del trabajo en España realizada por Fiverr, **el 51% de las empresas encuestadas considera no haber estado preparada para esta crisis** y entre los principales motivos destaca el no estar suficientemente preparados para el teletrabajo (un 47%) y no contar con la tecnología necesaria para afrontar la situación (un 39%). Con estos datos, quedan claras las carencias de digitalización existentes.

Este acontecimiento histórico pilló a todos por sorpresa, y en ese justo momento **se puso a prueba la resiliencia digital de las pymes**. Es decir, había algunas -las menos- que estaban más preparadas para adaptarse a este nuevo escenario, mientras que otras se encontraron ante una situación para la que no tenían puntos de apoyo suficientes.

Ese nuevo contexto obligaba, de un día para otro, a repensar el modelo de negocio para frenar el impacto negativo del confinamiento y poder sobrevivir. Se tenía que encontrar una solución para poder mantener la continuidad de negocio sin la existencia física del mismo. Esta continuidad del negocio pasaba por permitir que los empleados continuasen realizando sus funciones desde casa (gestionando pedidos, atendiendo el teléfono, etc.) para que los clientes pudiesen seguir contratando esos productos o servicios a través de canales digitales, como redes sociales o páginas web.

La presencia online de la pyme no se limitaba a tener un comercio electrónico a través del cuál poder adquirir productos, sino iba más allá y abría nuevas vías de negocio a aquellos sectores con una fuerte tradición presencial.

Por ejemplo, los restaurantes que no podían abrir de forma presencial y que supieron transformarse rápidamente, volcándose en ofrecer sus platos a través de plataformas de servicio a domicilio de comida.

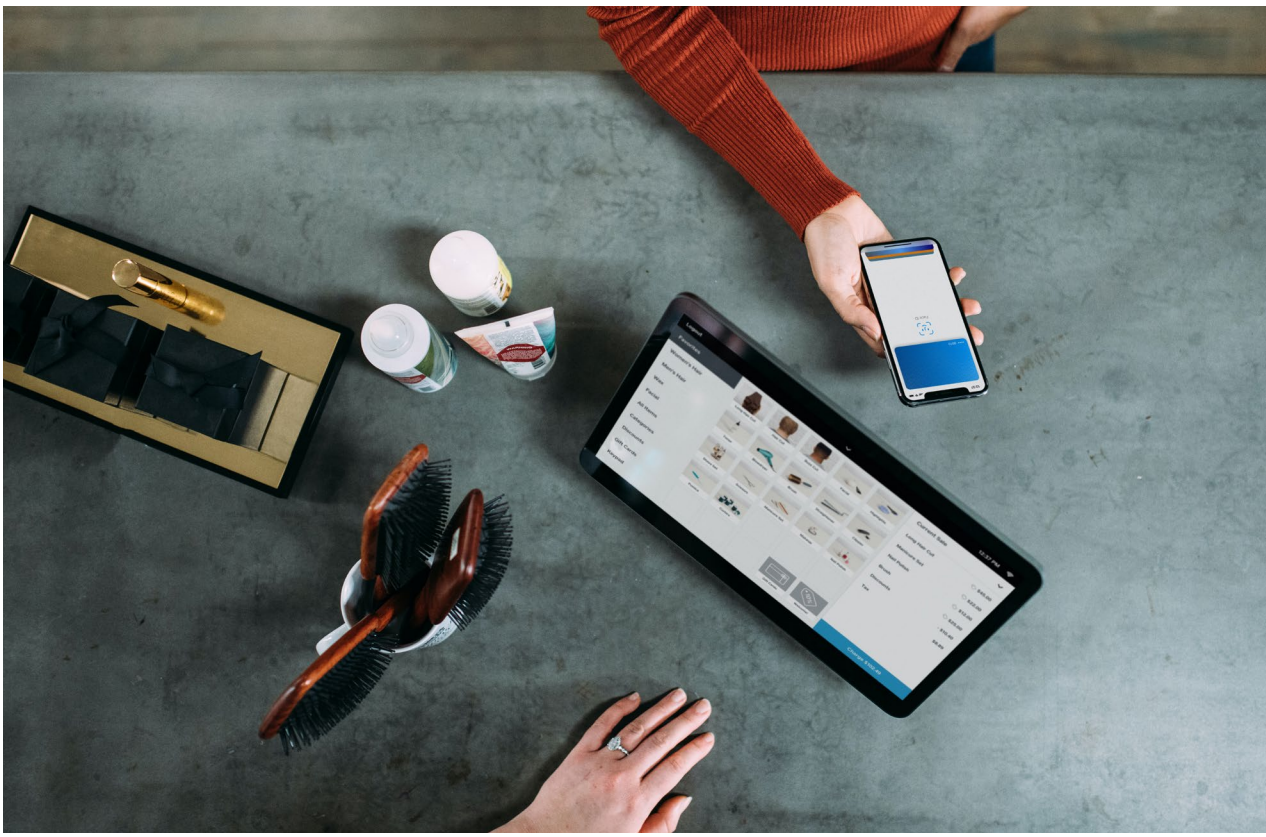
Desde las fases iniciales, según la situación evolucionaba, y en la propia actualidad, se puede observar una evolución de las necesidades empresariales en materia de tecnología.

Comenzando por la prisa inicial por poder trabajar a distancia en el mes de marzo, que incrementó el interés en herramientas de comunicación, mejora de la conectividad, escritorios virtuales, firewalls y herramientas de monitorización de redes; pasando por la atención a las mejoras de la infraestructura en abril, y la seguridad de los trabajadores remotos en Junio, hasta la creación de tiendas online para negocios minoristas después del verano enfocadas en fechas relevantes de consumo masivo como el *Black Friday* o la Navidad.

Y esto no ha terminado aquí. Según Gartner, las pequeñas y medianas empresas adaptarán sus infraestructuras IT para que los empleados puedan trabajar desde casa durante todo el 2021.

A diferencia de las recomendaciones habituales de una adopción gradual de tecnología, las empresas se han visto obligadas a saltar cualquier barrera que tuviesen en el camino de la digitalización de forma abrupta.

Como consecuencia de toda esta digitalización que han tenido que ejecutar las empresas, se las ha expuesto a un mayor riesgo de convertirse en víctimas de un ciberataque elevando el porcentaje de éxito de estos delincuentes. Todo ello, pone de manifiesto la necesidad urgente de avanzar en materia de ciberseguridad para que la digitalización sea posible.



03

Principales riesgos de seguridad de la información en las pequeñas y medianas empresas

A. Falta de concienciación

Teniendo clara la foto de la situación digital de las pymes, se puede entender mejor cuáles son los principales riesgos a los que se tienen que enfrentar.

El mayor riesgo al que se enfrentan las pymes en materia de ciberseguridad es la falta de concienciación sobre esta materia. Hasta hace poco no eran todas conscientes de la importancia de la digitalización y, por tanto, desconocían el componente de seguridad asociado.

Muchas empresas de este segmento creen que no pueden ser objetivos de ciberataques y desconocen las nefastas consecuencias de sufrir uno a pesar de ser el principal foco de los ataques.

Las pymes tienen las mismas necesidades en materia de seguridad de la información que las grandes compañías, pero con fuertes limitaciones en presupuesto, conocimiento y personal cualificado.

Por todo lo anterior, las pymes son un blanco fácil para los ciberdelincuentes.

En España, según el Centro Criptológico Nacional, durante las tres primeras semanas de marzo de este año los ataques a pequeñas empresas y autónomos creció hasta un 70%.

Por lo tanto, esa concienciación debe de llegar a todos empleados de la empresa puesto que saber actuar en un momento determinado es tarea de todos.

B. *Phishing* y *Malware*

Algunos de los ataques que reciben las Pymes son: todo tipo de virus (*bots*, troyanos, *adware*... etc.), fugas de información, amenazas internas y externas, ataques de denegación de servicio, ataques de contraseña,etc .

A continuación, vamos a profundizar en dos de los más habituales y en sus consecuencias.

Phishing

Consiste en suplantar a un remitente legítimo para obtener información a través de diferentes canales como SMS, telefónico o el correo electrónico. Este último es el más habitual debido al elevado volumen de correos electrónicos que se manejan diariamente. Debido a que el *phishing* es uno de los ataques más habituales, también es el más conocido y, por tanto, los cibercriminales han aumentado su creatividad de sus métodos para lograr su objetivo.

Cada vez cuentan con mayor número de métodos y son más sofisticados: *Pharming*, *Spear Phishing*, *Clickjacking*, *Phishing Spray and Pray* son solo algunos de ellos.

Por ejemplo, una empresa pequeña recibe un correo que se hace pasar por una organización pública que gestiona ayudas económicas a las pymes por la pandemia y solicita ciertos datos bancarios para poder hacer el ingreso de estas ayudas. Si la empresa no detecta esta suplantación y proporciona su información bancaria, puede estar dando todos sus ahorros económicos a los ciberdelincuentes con la consecuente quiebra económica que supondría la desaparición de la empresa.

Malware

Cualquier tipo de *software* malicioso que puede infectar los equipos y ocasionar distintos perjuicios. El *malware* puede llegar a la empresa a través de diferentes canales: a través de la conexión a Internet, del correo electrónico, agujeros de seguridad, aplicaciones y redes WIFI públicas. Además, hay distintos tipos de *malware*: gusanos, troyanos, *Spyware*, *Exploits* y el *ransomware* que es el más relevante en los últimos tiempos.

Según Kaspersky, **el 71% de los ataques de *ransomware* tienen como objetivo las pymes.**

Por ejemplo, mientras un usuario está navegando y se descarga un archivo, sin saber que se trata de un ransomware, en ese momento aparece un mensaje en pantalla que le informa de que debe pagar un rescate si quiere poder recuperar la información de su equipo.

Esta situación puede suponer un empeoramiento en la imagen de marca hacia sus clientes por parte de la empresa en caso de que pueda recuperar la información y la desaparición de la misma si finalmente no puede recuperarla.

C. Teletrabajo

Si el riesgo de estos ataques ya era elevado, el teletrabajo los ha aumentado de forma exponencial. De hecho, **el teletrabajo se ha convertido en la principal brecha de entrada para la seguridad de las empresas**. El comienzo y posterior uso del teletrabajo supone que la información de la compañía se expanda por diferentes puntos, que los empleados trabajen en algunas ocasiones con equipos personales sin medidas de seguridad o con equipos profesionales que no tienen estas medidas actualizadas. El acceso remoto y las videollamadas no siempre son lo suficientemente seguros, pero su uso es constante.

Es decir, las empresas que tenían alguna medida de seguridad ya implementada en la empresa las perdían al permitir que sus empleados trabajaran desde casa. Por ejemplo, aquellas que ya habían tomado medidas para controlar ataques como *phishing* o *malware* dentro de la red corporativa, tenían que buscar una alternativa en el ámbito doméstico.

Mientras que intentan adaptar las medidas de ciberseguridad domésticas a las corporativas, los cibercriminales obtienen rentabilidad de esta situación puesto que la tipología de los ataques es la misma, pero con una clara disminución de los controles de seguridad.

El impacto de los ciberataques es enorme tanto en pérdidas económicas como de reputación. Por ello, las pequeñas y medianas empresas incrementarán el presupuesto en seguridad a pesar de la complicada coyuntura económica que atraviesan.

04

La propuesta de ElevenPaths

A. *Peace of Mind*

El contexto actual de las pequeñas y medianas empresas, entre emergencia sanitaria y emergencia económica, donde salir adelante es más difícil que nunca, no tiene por qué estar reñido con la necesidad de cuidar y proteger su negocio que, como hemos visto, cada vez es más digital.

Por todo ello, creemos que es importante enfocar la oferta de ciberseguridad a este segmento, hacia el "*Peace of Mind*" del cliente.

Es decir, una solución que permite a la empresa que se pueda centrar en su propio negocio porque ElevenPaths se encarga de su seguridad.

Además, no quieren delegar solo la seguridad sin ninguna garantía, sino que quieren delegar esa parte de sus tareas internas en los mejores proveedores del mercado.

B. Servicio de Seguridad Gestionado

ElevenPaths propone una solución de ciberseguridad basada en la gestión de la seguridad de sus clientes. Es decir, al contratar esta solución de seguridad la pyme está contratando un "solucionador" de sus necesidades en materia de seguridad. Con ello, **ElevenPaths se convierte en el gestor de seguridad de las empresas de este segmento.**

¿Cómo es esta solución para que los clientes alcancen el "*Peace of Mind*"?

Estas son algunas de sus características:

Gestionada:
La pyme se despreocupa de la seguridad y la delega completamente en ElevenPaths.

Acompañada:
Se da asistencia tanto en las incidencias/dudas de seguridad, como en su proceso de digitalización.

Sencilla:
Servicios de seguridad intuitivos y mejor experiencia de cliente.

Para poder alcanzar estos beneficios de la solución, ElevenPaths pone a disposición de sus pymes las siguientes capacidades:

Atención a medida:
soporte específico para la pequeña empresa, que habla su mismo lenguaje y con alta calidad de entrega.

Servicio extremo a extremo:
se proporciona a las empresas un servicio completo que cubre todo el ciclo de vida del servicio. No es solo una reventa.

Compatibilidad con el ecosistema IT:
la oferta comercial de seguridad es compatible con otras ofertas comerciales de otras áreas IT (*Cloud*, *Big Data*, IoT...).

Confianza en la operadora:
solo una operadora puede garantizar la seguridad en las comunicaciones por defecto. Es decir, desde el minuto cero que se contratan las comunicaciones ya vienen securizadas sin necesidad de contratar servicios adicionales de seguridad, por los despliegues de seguridad en red realizados previamente.

Capilaridad:
la gran cantidad de canales (presencial, online, telefónico, etc.) a través de los cuales podemos llegar a ellas.

C. Centro de seguridad Pyme

Debido a la relevancia que tiene la gestión de la seguridad dentro de esta propuesta de valor, se cuenta con un centro de soporte para Pymes. Este centro se trata de **un grupo de expertos que acompañan a la empresa en todo momento, y que a través del conocimiento de seguridad y especializado en hablar el mismo lenguaje que estos clientes, convierten la seguridad en algo sencillo para ellas.**

Este completo servicio abarca desde los primeros pasos para la protección de la empresa (con recomendaciones de la solución más adecuada), hasta el envío de informes periódicos, pasando por el apoyo en el despliegue, el mantenimiento de los sistemas de seguridad y la resolución de amenazas e incidentes de seguridad. Todo ello con una disponibilidad de 24x7 todos los días del año.

También incluye el asesoramiento para el cumplimiento normativo de las ultimas normas internacionales de seguridad.

D. Tecnología y formación

Por lo tanto, esta propuesta se basa principalmente en la gestión, más allá de la tecnología subyacente. La constante y rápida evolución de la tecnología obliga a las empresas a delegar las tareas técnicas en proveedores que están continuamente actualizados y tienen la suficiente experiencia en el sector para hacerse cargo de las decisiones de seguridad por ellos.

En ElevenPaths, el catálogo de servicios de seguridad de la información es amplio y se realiza en colaboración con los proveedores líderes del mercado de la seguridad y algunos desarrollos propios.

Comprende desde las soluciones más comunes a las empresas (independientemente de su sector o grado de digitalización) como Antivirus y Antirsansomware, navegación segura, seguridad de la sede, acceso remoto seguro y Correo Limpio; hasta algunas algo más avanzadas como *Web Application Firewall*, CASB, Firma Digital, soluciones de cumplimiento normativo GDPR, ciberseguro o, incluso, formación específica en materia de seguridad para poder concienciar a los empleados de la empresa.

La educación en ciberseguridad para los empleados de cualquier empresa es fundamental para que tengan conocimientos sobre ella y que conozcan las mejores prácticas en esta área. Con ello la empresa estará más preparada en caso de sufrir un ciberataque y la probabilidad de recibirlos será menor.

E. Beneficios para los clientes

Algunos de los beneficios de esta solución para los clientes serían:

- **Calidad de entrega:** de los servicios de ciberseguridad en general, y la de la conectividad en particular, ya que solo una operadora puede dar las comunicaciones seguras desde el principio.
- **Factura única:** con la reducción en la gestión de proveedores.Conectividad y seguridad unificados, pero también podrían unirse otros servicios IT como *Cloud*, *Big Data*, IoT...
- **Mensualizado:** coste periódico sin necesidad de inversión inicial haciéndolo más accesible en cualquier momento para las empresas.
- **Acompañamiento a la empresa** en todo su crecimiento digital. Esta solución de ciberseguridad crece de la mano de la digitalización de la empresa. Gestionando en todo momento la ciberseguridad.

05

Conclusiones

La nueva realidad en la que se encuentran las pymes después de la pandemia, ocurrida este mismo año, ya ha marcado un antes y un después en su nivel de concienciación en materia de ciberseguridad como consecuencia de la digitalización que han acometido de forma disruptiva en algunas ocasiones.

La ciberseguridad se ha convertido en un pilar fundamental de la estrategia empresarial de las empresas de este segmento y ahora es el momento de poner en marcha esa nueva estrategia de la forma más eficaz posible.

ElevenPaths ha creado una solución de seguridad clara y comprensible, para ayudar en la ardua tarea de acercar la seguridad a las pequeñas y medianas empresas, con una oferta adaptada a las necesidades de protección que tenga la compañía y encargándose de la administración y mantenimiento de la misma.

Se trata de una solución integral de la seguridad. Desde la concienciación de su necesidad, hasta la puesta en marcha de la solución y la resolución de incidencias, acompañado por el soporte más especializado a sus necesidades.

Desde ElevenPaths, como parte del grupo Telefónica, y ahora integrado en la nueva Telefónica Cybersecurity Tech cuentan con años de experiencia en abordar la problemática de las pymes con diferentes tipos de soluciones desplegadas en más de 11 países. Así como acuerdos con los mejores fabricantes del mercado, desarrollos propios realizados a medida para las empresas de este segmento, una oferta integrada con el resto de áreas involucradas en la digitalización como *Cloud* o *Big Data* y la confianza que ofrece ser la operadora segura, ya que es la mejor posicionada para poder dar seguridad sobre las comunicaciones que también ofrece.

Confía en ElevenPaths como tu compañero de viaje en esta nueva etapa llamada a ser la nueva revolución digital para las pequeñas y medianas empresas.

Sobre ElevenPaths

ElevenPaths es la compañía de ciberseguridad de Telefónica, integrada dentro del holding Telefónica Tech, que aglutina los negocios digitales con mayor potencial de crecimiento de la compañía.

En un mundo en el que las ciberamenazas son inevitables, como proveedores de servicios de seguridad gestionada inteligente, nos enfocamos en prevenir, detectar, dar respuesta y disminuir los posibles ataques a los que se enfrentan las empresas. Garantizamos la ciber-resiliencia de nuestros clientes a través de un soporte 24/7 gestionado desde once i-SOC alrededor del mundo con capacidad operativa global.

Creemos en la idea de desafiar el estado actual de la seguridad, c aracterística que debe estar siempre presente en la tecnología. Nos replanteamos continuamente la relación entre seguridad y las personas con el objetivo de crear productos innovadores capaces de transformar el concepto de seguridad y, de esta manera, logramos ir un paso por delante de nuestros atacantes, cada vez más presentes en nuestra vida digital.

Trabajamos para garantizar un entorno digital más seguro a través de alianzas estratégicas que nos permitan mejorar la seguridad de nuestros clientes, así como a través de colaboraciones con organismos y entidades líderes como la Comisión Europea, Cyber Threat Alliance, Cloud Security Alliance, Cyber Security Alliance, EuroPol, Incibe, OpenSSF, OEA, ISAAC, OCA, FIRST, IoT Security Foundation, Centro de Ciberseguridad Industrial (CCI) y APWG.

Más información

elevenpaths.com | **@ElevenPaths** | **blog.elevenpaths**