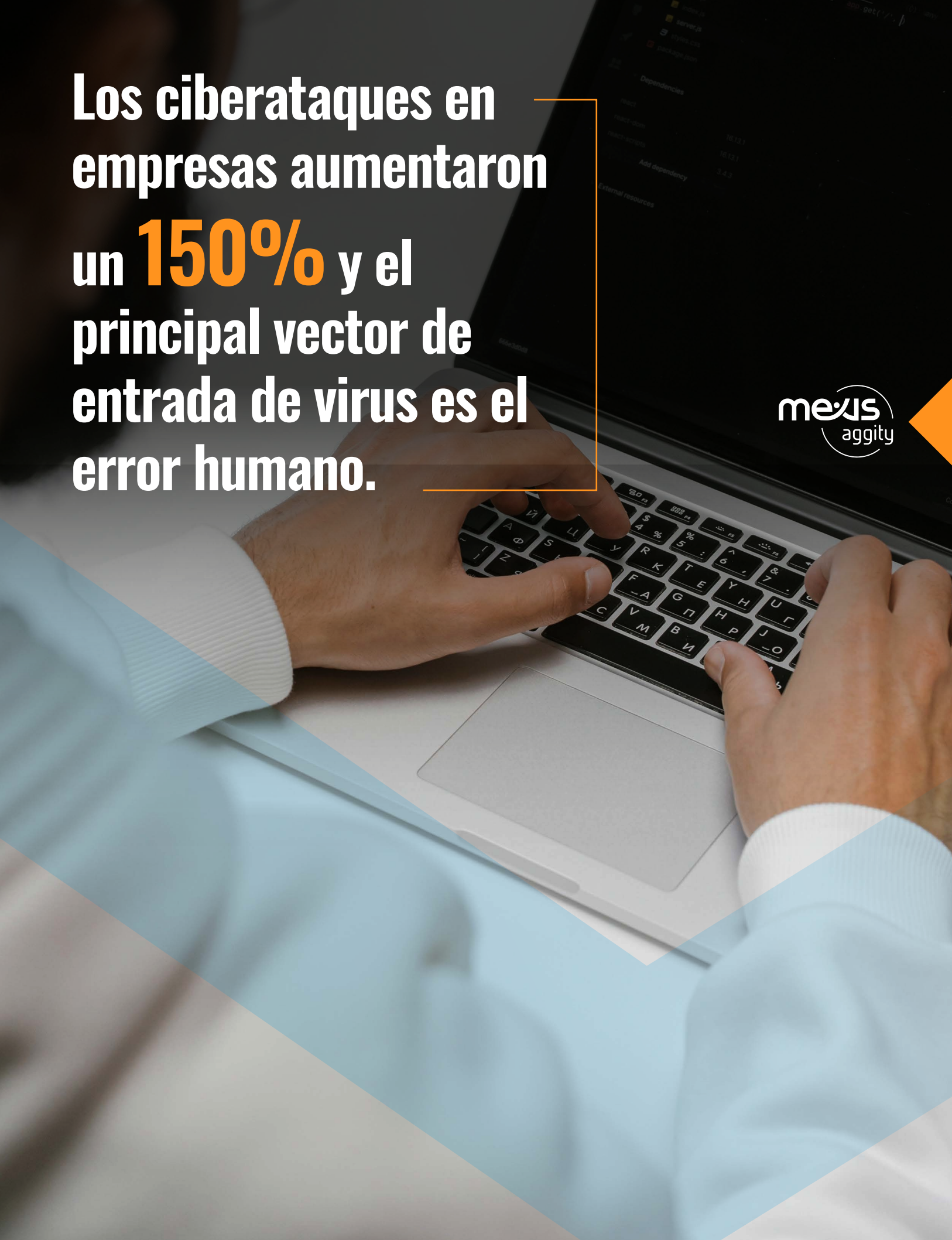
Los ciberataques en empresas aumentaron un 150% y el principal vector de entrada de virus es el error humano.
mexis aggity

Expertos en ciberseguridad analizan los riesgos de ataques que existen para las empresas y desvelan las claves para proteger a tu negocio de cualquiera de estos fraudes: la lucha empresarial contra el phising, el ransomware y el malware.

España es uno de los países que más ciberataques sufre a nivel mundial, teniendo en cuenta que las consecuencias que sufren las empresas son económicas, reputacionales y operativas. Cualquier negocio debe tener un buen sistema de protección, por consiguiente, necesitan el asesoramiento de profesionales para tener mecanismos de prevención.

El principal objetivo de los ciberataques es acceder a los datos privados de una empresa para impactar negativamente en su imagen y en la confianza de los clientes.

En los últimos años, los ciberataques han superado los porcentajes que conocíamos. **Solo en 2021 aumentaron en un 150% y cada vez son más las vías de entrada para aprovechar cualquier brecha de seguridad.**

Dichos ataques cibernéticos pueden suponer el cierre de la actividad empresarial porque los costes son inasumibles, además, **una falta de diligencia en el deber de protección supone sanciones.**

¿Estamos expuestos a los ciberataques?

Negarlo sería una ilusión, especialmente en un momento histórico como este, en el que 'el dato' ha cobrado la relevancia actual. Sin entrar a pormenorizar las distintas consecuencias del robo de datos, sabemos que nuestra información depende del grado de seguridad personal o corporativa que hayamos interpuesto.

Las obligaciones de seguridad que tiene una empresa.

El responsable de datos debe aplicar las medidas necesarias para impedir cualquier vulnerabilidad, de esta manera, **la empresa tendrá que justificar qué prevenciones ha tomado.**

Cualquier negocio tiene que ser capaz de gestionar los sistemas de información mediante medidas físicas y técnicas para mantener la confidencialidad, disponibilidad y la integridad de sus recursos. Asimismo, tienen que llevar a cabo evaluaciones de riesgos y están obligados a asegurar la información de los trabajadores y clientes.

La importancia de protegerse para que un negocio funcione correctamente.

Una empresa no puede defenderse de las campañas de violación de datos sin un programa de ciberseguridad, además, los lugares de trabajo deben incluir programas de concienciación sobre seguridad cibernética para educar al personal.

Todas las organizaciones deberían tomar medidas para protegerse de un posible ciberataque. La protección no solo se basa en una serie de controles genéricos, sino que han de ser un conjunto de medidas adaptadas al contexto de cada organización. La ciberseguridad no es un coste sin retorno, sino que es **una inversión que permitirá la implantación de medidas y el entrenamiento del personal mediante la formación.**

Los riesgos que corre el cliente ante un posible ciberataque de la empresa.

Sufrir un ciberataque puede suponer un parón temporal o el cese total de la actividad. Los ciberdelincuentes acceden a los sistemas y sustraen los datos privados externos, conllevando responsabilidades subsidiarias y dejando al descubierto vías de entrada para atacar a terceros, ya sean proveedores, colaboradores y clientes.
Los ataques cibernéticos pueden detener las operaciones en línea en solo unos minutos y demorar semanas en resolverse.

Los datos robados podrían usarse para exponerlos públicamente, realizar chantajes o extorsiones, o ser ofrecidos a la competencia".

Aquellos clientes con datos personales comprometidos deben ser informados por parte de la empresa, de forma que puedan tomar las medidas necesarias para evitar problemas inmediatos o futuros.

Los riesgos "dependen del tipo de ataque y tipo de empresa. Hay ataques que son capaces de paralizar la actividad durante un período de tiempo más o menos extenso y, en consecuencia, esto implica que el cliente puede dejar de recibir servicios o suministros más o menos críticos".

¿La vulnerabilidad depende de la empresa o del empleado?

El principal vector de entrada de virus informáticos viene provocado por errores humanos, por ello, una buena formación a empleados y directivos en materia de ciberseguridad puede evitar muchos problemas. Si los trabajadores no están capacitados, será difícil proteger los sistemas contra la variedad de amenazas que los ciberdelincuentes utilizan para robar datos.

Qué vulnerabilidades existen.

El aumento de los ciberataques aumentó a raíz del teletrabajo, debido a que se ha puesto a prueba las barreras de seguridad de las empresas y dificultó la labor de control sobre la actividad.

Desde el inicio de la pandemia destacan los ataques de ransomware. Esta vulnerabilidad provoca la encriptación de la información y paraliza la actividad de la empresa. Asimismo, en la mayoría de los casos, el pago de un rescate es la vía más rápida para retomar el funcionamiento del negocio.

Otros de los riesgos son:

• Fraude por phishing: Se simula un correo legítimo para engañar al usuario y conseguir algún dato personal relevante, como las claves de su banca online.

• Malware: Un fichero malicioso que se ejecuta e infecta el dispositivo.

• Scam: Se envía un correo para cometer una estafa basándose en supuestos ingresos económicos.

Cómo protegerse.

En primer lugar, cualquier negocio se tiene que poner en manos de profesionales que protejan los datos de manera privada. Posteriormente, es recomendable tener un alto nivel de formación para evitar los posibles errores humanos.

Los usuarios se pueden proteger de la siguiente manera:

• Establecer una política de contraseña fuerte, con al menos ocho caracteres, mayúsculas, minúsculas, números y caracteres especiales.

• No hay que pinchar en los enlaces que se reciban por correo electrónico.

• Desconfiar de las redes WiFi públicas.

• Proteger todos los dispositivos mediante un antivirus con herramientas extra de seguridad, como almacén de contraseñas y verificador de enlaces o conexiones.

• Usar perfiles de usuario con permisos restrictivos que no permitan acceder a ninguna información más que la estrictamente necesaria para el desempeño profesional.

• Mantener los equipos bloqueados con contraseñas.

Fuente de información: www.20minutos.es