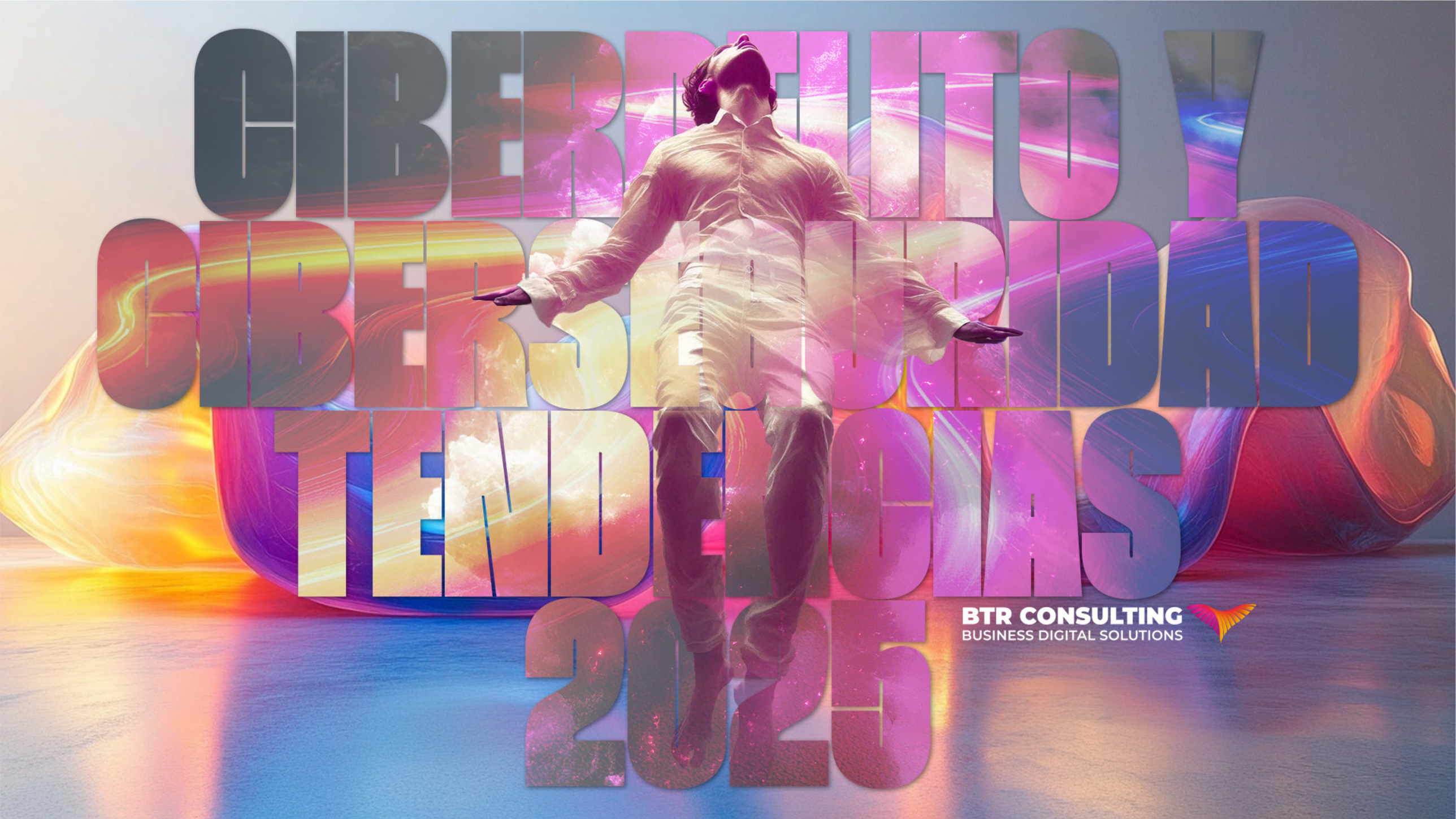
CIBERDELITO Y CIBERSEGURIDAD TENDENCIAS 2025



BTR CONSULTING
BUSINESS DIGITAL SOLUTIONS

AMEN
NAS
ZAS

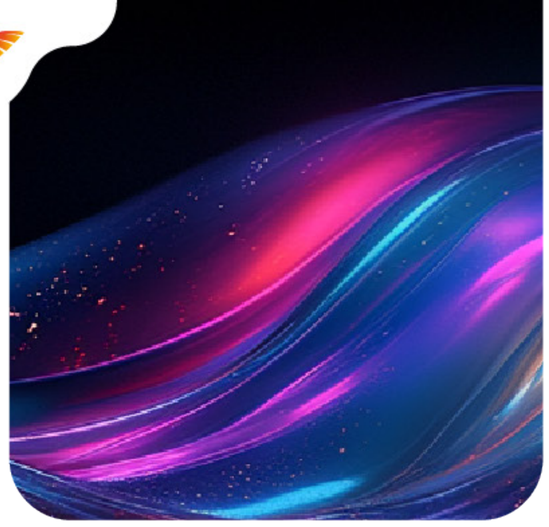
BTR CONSULTING
BUSINESS DIGITAL SOLUTIONS

300%

Aumento en Ataques por Email

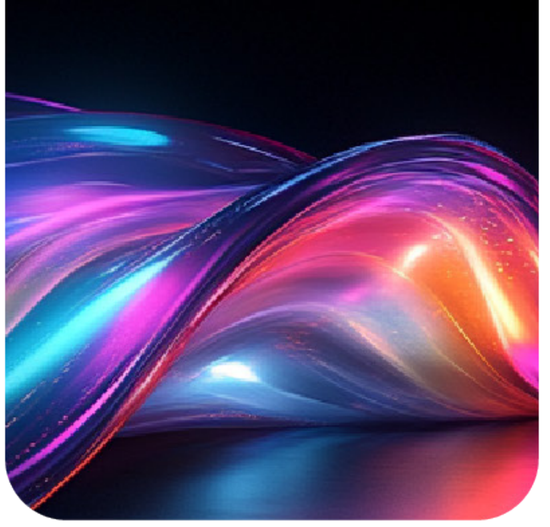
35%

Aumento en detección de ransomware



38%

No logran identificar los ciberataques a tiempo



40%

De los entornos están en riesgo de una invasión total por vulnerabilidades

CIBERDELINCUENTES SIGUEN USANDO HERRAMIENTAS DE IA MALICIOSAS COMO WORMGPT Y FRAUDGPT

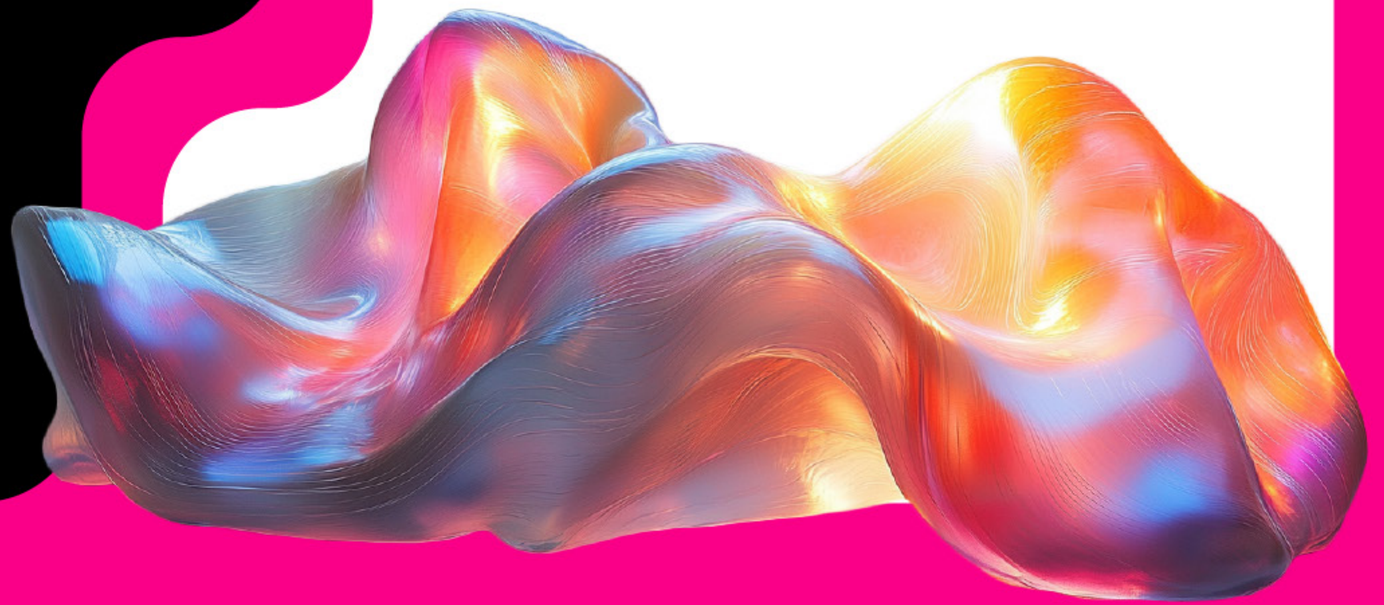
BTR CONSULTING
BUSINESS DIGITAL SOLUTIONS

MALWARE

Es la amenaza con mayor crecimiento en el 2024

41% de las empresas fueron testigos de ataques, seguidos por **Phishing y Ransomware**

27%
aumentó la cantidad de empresas que sufrieron un ataque de **Ransomware** más que el año pasado



BTR CONSULTING
BUSINESS DIGITAL SOLUTIONS

INGENIERÍA SOCIAL

IA

LA IA SE CONVIERTE EN UN ARMA Y LAS TÉCNICAS DE PHISHING EVOLUCIONAN

71%
De los ataques intentan engañar a los empleados mediante el uso de Phishing y QR

51%
Es el fuerte aumento de Phishing con códigos QR

70%
De organizaciones considera que su seguridad actual es efectiva ante un ataque basado en imágenes

BTR CONSULTING
BUSINESS DIGITAL SOLUTIONS

RANSOMWARE EN 2024

50%
Es el aumento de grupos Ransomware

22%
De víctimas reportadas aumentó en lo que va de este año

BTR CONSULTING
BUSINESS DIGITAL SOLUTIONS

+36%

Phishing en redes sociales, siendo el canal más atacado en lo que va del 2024

+50%

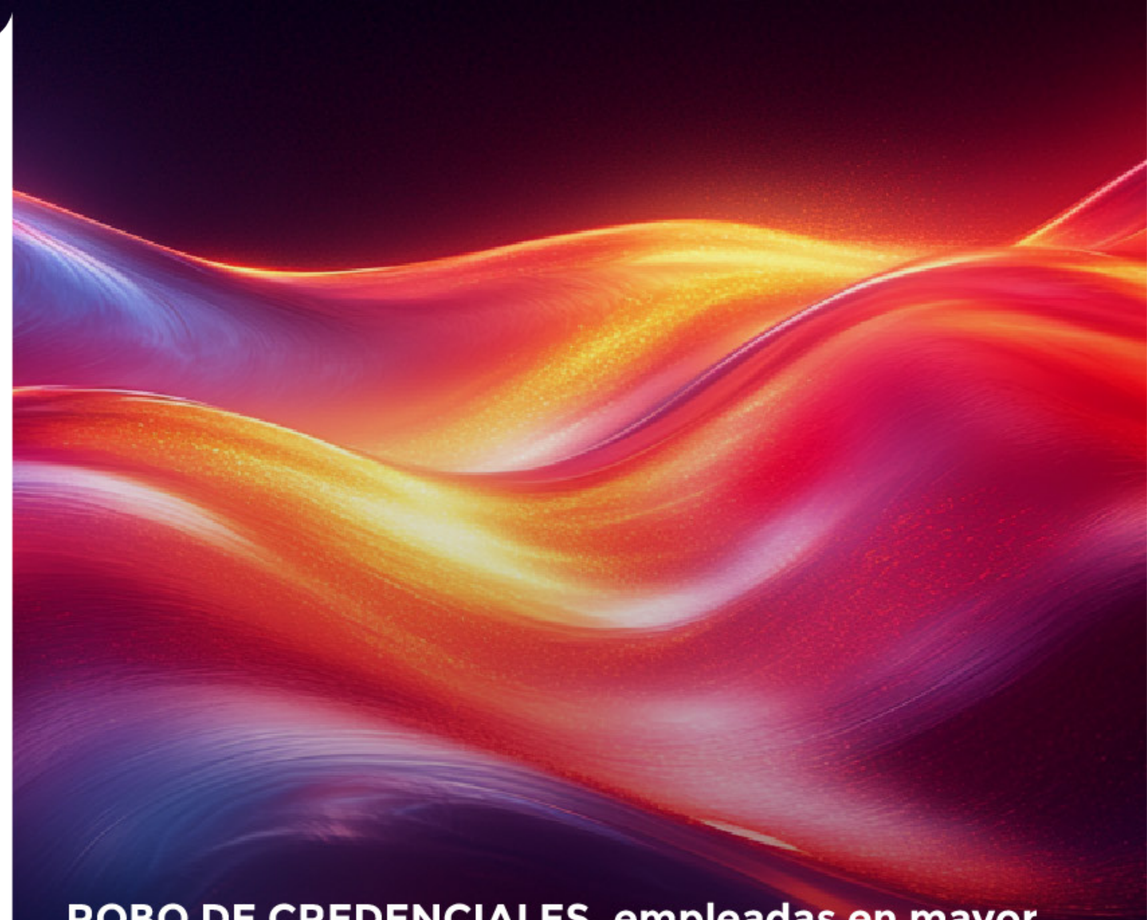
De malware detectado en pymes, son: **keyloggers, spyware, robo de datos y credenciales de empresas**

+34%

De los mensajes Vishing híbridos, fueron utilizados como señuelo para una estafa

TENDENCIAS 2025

SE SOSTIENE LA TENDENCIA DE CONSOLIDACIÓN DE LA INDUSTRIA



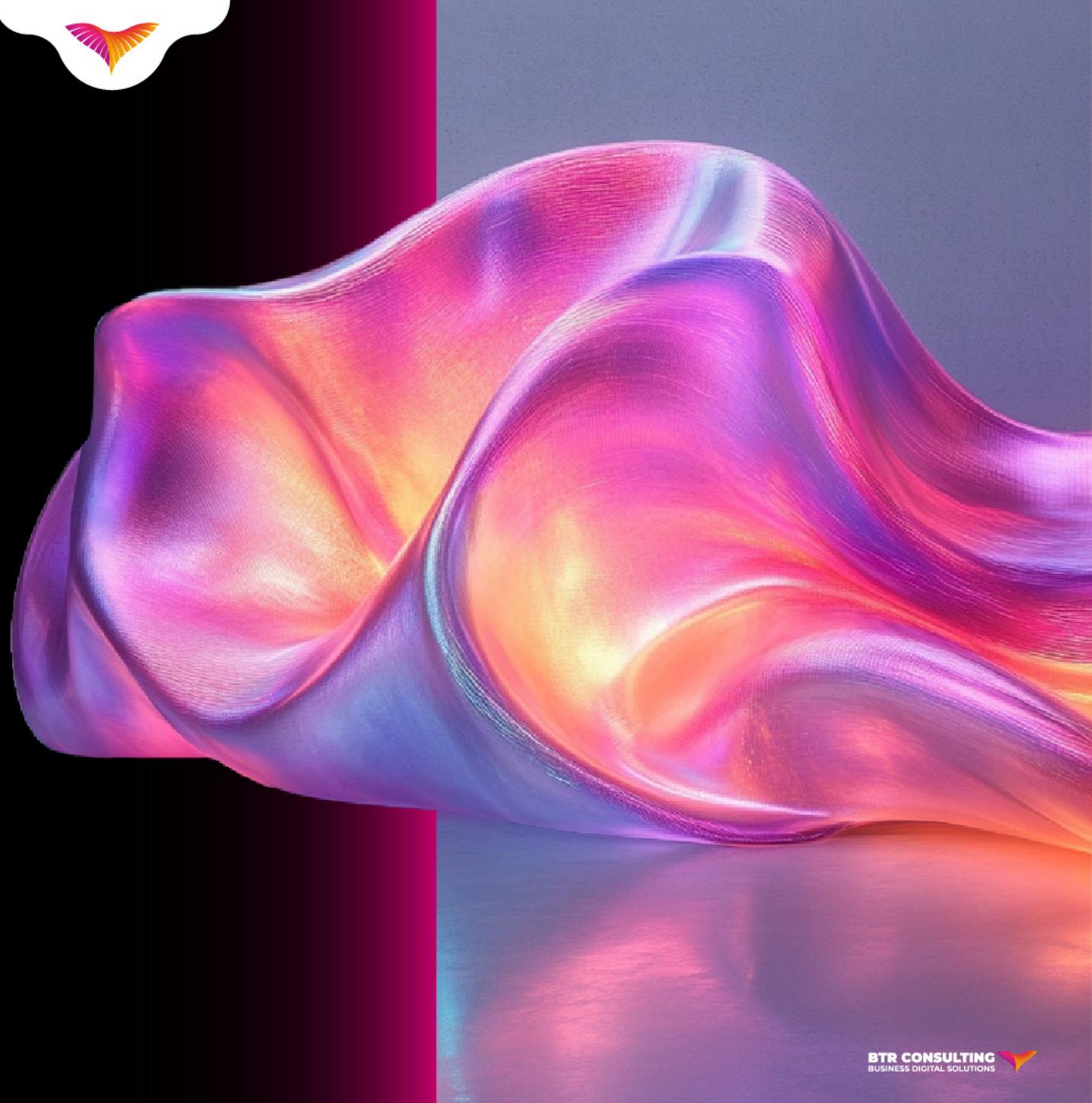
ROBO DE CREDENCIALES, empleadas en mayor proporción para lanzar ataques de ransomware dirigido a grandes y medianas empresas, incluidas las organizaciones gubernamentales. Para obtener estas credenciales, los atacantes utilizan principalmente técnicas de **PHISHING**, en la misma galería de delitos se presentan como variantes para continuar confundiendo al mercado y sus victimas, Vishing, Anuncios Fraudulentos-Ad Words, Cuento del Tío Digital y Skimming Online, entre otros.

BTR CONSULTING
BUSINESS DIGITAL SOLUTIONS

Las redes sociales se han posicionado como materia prima para la acción de "ciberinteligencia" por parte de los delincuentes y los propios usuarios se han convertido en responsables y participes necesarios de su conversión en víctimas.

Esto exacerbado por la penetración de las redes sociales, los sistemas de mensajería instantánea y el efecto pandémico, mayor cantidad de dispositivos a los que nos conectamos cada vez más tiempo, desde que nos despertamos hasta la hora de volver a dormir.

La pendulante predilección de las distintas configuraciones de ciberdelincuentes, estados, bandas internacionales, grupos carcelarios y lobos solitarios que atacan indiscriminadamente a Gobiernos, Mercados, Empresas, Familias y a Doña Rosa. Todo aquello que dotado de oscurantismo y misterio parecía proliferar en la Dark Web, ahora emerge como un cadáver putrefacto en Telegram y otras plataformas de fácil y popular acceso.



EL RANSOMWARE NO DARÁ TREGUA

El ransomware será la principal amenaza para las empresas en 2025, con ataques cada vez más frecuentes y sofisticados

81%

Aumentaron en 2024 en comparación con el 2023. Los grupos criminales se están volviendo más ágiles y concentrados, adoptando tácticas de doble extorsión que combinan el encriptado de datos con el robo de información para aumentar la presión sobre las víctimas.

EN 2025, EL ENFOQUE VOLVERÁ A ESTAR PUESTO EN EL DESARROLLO DE LA RESILIENCIA Y REDUCIR LA EXPOSICIÓN AL RIESGO. {CONFIANZA CERO}

Proteger lo esencial es clave. Estados, empresas e instituciones deben fortalecer sus defensas, actualizar marcos de privacidad, capacitar equipos y responder rápido a riesgos. Seguridad es confianza y ventaja competitiva.

01 LA ESCASEZ DE TALENTO Y SU CALIDAD

La ciberseguridad es una responsabilidad compartida, por lo que es urgente que el personal adapte los conocimientos necesarios ante la crisis laboral que este cambio producirá. El gasto en tecnología es importante, pero hay que incluir con una formación a toda la mano de obra que la implementará, es imperativo mejorar la calidad de estos recursos.

02

HUMANIZACIÓN Y MADURACIÓN

DEL MODELO DE CIBERSEGURIDAD

Las empresas y los proveedores de servicios deben lograr que sus sistemas de detección temprana y defensa se actualicen en tiempos cada vez más reducidos para garantizar las necesidades de cobertura.

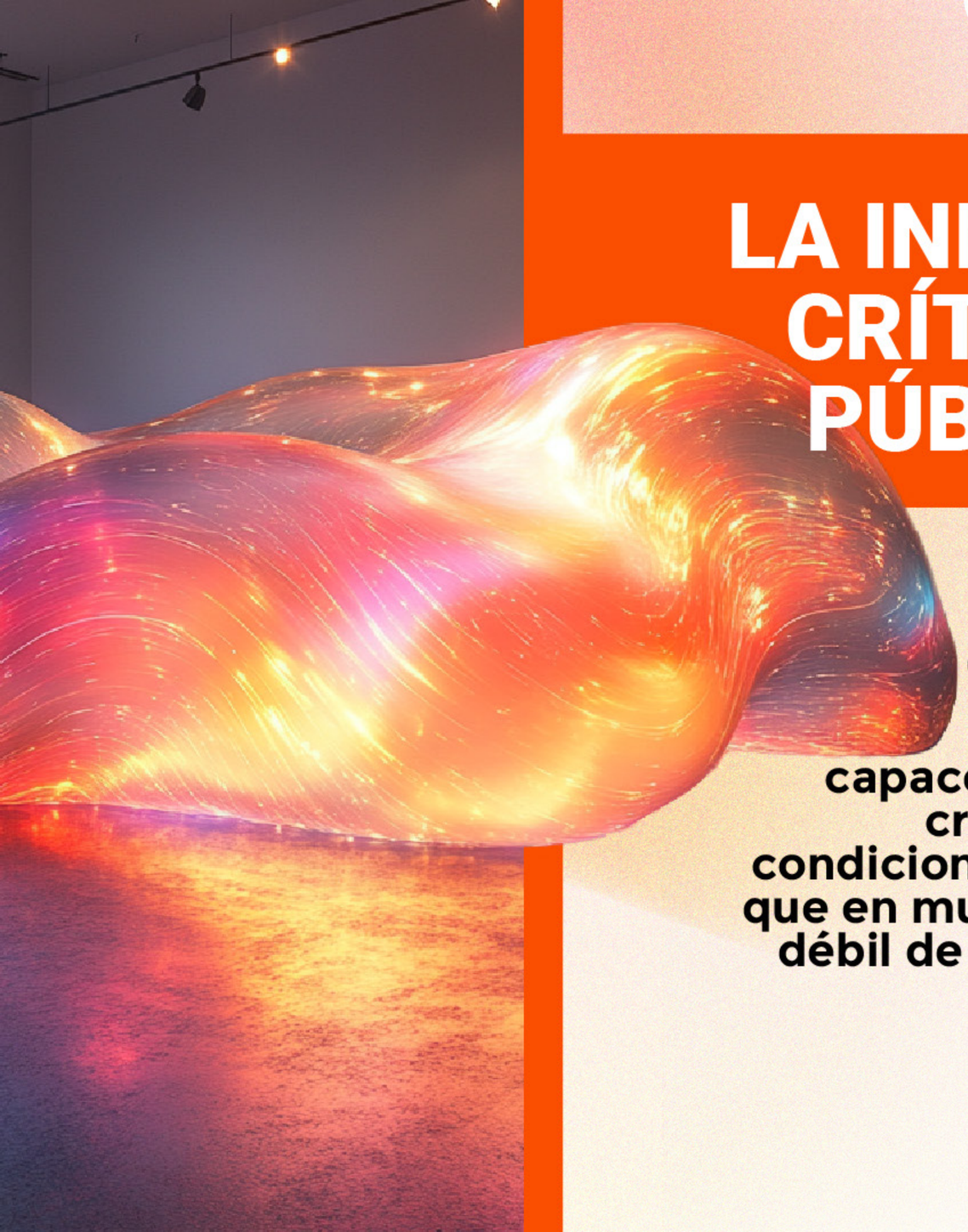
ES DECIR, ES INDISPENSABLE UNA GESTIÓN MULTIDISCIPLINARIA DE LA CIBERSEGURIDAD.

03

DIRECTORIOS CON MAYOR CONOCIMIENTO E INVERSIÓN

Sin una comunicación cotidiana entre el directorio, el negocio y el equipo de riesgo tecnológico, las organizaciones se expondrán a un peligro cada vez mayor. Las empresas e instituciones prosperan porque son capaces de ejercer el control y tomar decisiones informadas ante situaciones de crisis.

BTR CONSULTING
BUSINESS DIGITAL SOLUTIONS



LA INFRAESTRUCTURA CRÍTICA Y EL SECTOR PÚBLICO EN LA MIRA

04

EL SECTOR PÚBLICO ES UN OBJETIVO PRIORITARIO PARA LOS CIBERDELINCUENTES,

capaces de paralizar la infraestructura crítica, esto expondrá aún más las condiciones de ciberseguridad deficitaria que en muchas ocasiones es el punto más débil de los servicios esenciales por más que sean privatizados.

LOS ATAQUES SOBRE OT E IOT SERÁN CADA VEZ MÁS FRECUENTES

05

La expansión del Internet de los objetos conectados (IoT) representa un gran desafío en ciberseguridad. Con más de 32 mil millones de dispositivos IoT proyectados para 2030, cada nuevo equipo conectado aumenta la superficie de ataque, permitiendo a los ciberdelincuentes infiltrarse en redes críticas. Asimismo, los ataques a las Tecnologías Operativas (OT) serán más frecuentes, poniendo en riesgo infraestructuras esenciales como energía y transporte.

La infraestructura crítica será prioridad para los ciberdelincuentes porque engloba los servicios e industrias de atención médica, transporte, alimentos, defensa, minería, suministro de agua, Internet, energía, petróleo, entre otros.

06

MÁS INFORMACIÓN, MÁS PRIVACIDAD

SERÁ RELEVANTE EN EL FUTURO CERCANO

Se implementarán al menos ocho nuevas leyes en 2025. con el fin de controlar y transparentar los datos personales que las empresas registran y procesan a sus clientes. Será necesario trabajar en regulaciones que permitan mayores estándares, como así también establecer las responsabilidades de las compañías.

07 CONCIENTIZACIÓN, CULTURA DE RESILIENCIA Y SEGURIDAD

La reducción de las vulnerabilidades depende del nivel de capacitación y concientización entre el personal de trabajo. Los líderes empresariales deben transmitir actitudes de cuestionamiento sobre solicitudes de alto riesgo, como enviar información confidencial por mails o procesar pagos.

INNOVACIÓN 08

El cibercrimen y los ciberataques aumentaron debido a la digitalización acelerada y la proliferación de grupos de hackers, desde pequeñas bandas hasta actores respaldados por estados.

Innovación en el Aprendizaje Organizacional y la Ciberseguridad a través del diseño de juegos electrónicos, es posible abordar problemas complejos de manera innovadora y efectiva.

BTR CONSULTING
BUSINESS DIGITAL SOLUTIONS

GAMIFICACIÓN

Desde hace varios años, el ciberdelito sigue en constante crecimiento, lo que refuerza la importancia de educar y capacitar a las personas en prácticas preventivas, una prioridad clave para empresas y organizaciones.

En este contexto, la gamificación emerge como una herramienta de alto impacto en el ámbito empresarial. Esta técnica, que aplica dinámicas de juego en escenarios no recreativos, potencia significativamente la interacción, el compromiso y la motivación de los participantes. Además, facilita la adquisición rápida y la retención efectiva de conocimientos.

75%

De la fuerza laboral en 2025 será millennial y centennial, generaciones digitales que valoran la innovación

Fomentamos la concientización en ciberseguridad a través del juego, respondiendo al desafío del creciente ciberdelito

BTR CONSULTING
BUSINESS DIGITAL SOLUTIONS

LA IA EMPODERA A LOS CIBERCRIMINALES

Los ciberdelincuentes emplean IA para envenenar datos, inyectando información falsa en los conjuntos de entrenamiento, y para generar malware automatizado con programas como ChatGPT.

09

Además, los deepfakes permiten crear contenido falso, los sesgos en modelos de IA pueden ser explotados para manipular resultados, y los ataques a sistemas de toma de decisiones autónoma se están convirtiendo en una amenaza creciente.

10 CONFLICTOS BÉLICOS

En un mundo hiperconectado y dependiente de la tecnología, las ciberhostilidades se convierten en armas estratégicas de estados y grupos terroristas.

Los conflictos trascienden la frontera digital, acelerando la evolución de las técnicas de cyberattacks como suplantación de identidad, fake news y ataques anónimos que siembran incertidumbre y temor en la sociedad. Estos actos, difíciles de rastrear y atribuir, forman parte de una nueva contienda global donde el poder se ejerce tanto con armamento convencional como con tecnología informática avanzada.

El caso reciente de los ciberataques en Israel y Ucrania evidencia cómo estas tácticas afectan infraestructuras críticas, desde sistemas de alerta temprana hasta servicios públicos y gubernamentales. Grupos organizados de cybergangs y otros asociados a intereses pro-rusos o iraníes han ejecutado campañas dirigidas a desestabilizar, generar terror social y amplificar el impacto de sus actos con propaganda y noticias falsas. En esta era, la ciberguerra no solo destruye sistemas, sino que manipula percepciones, redefiniendo el alcance del conflicto moderno.

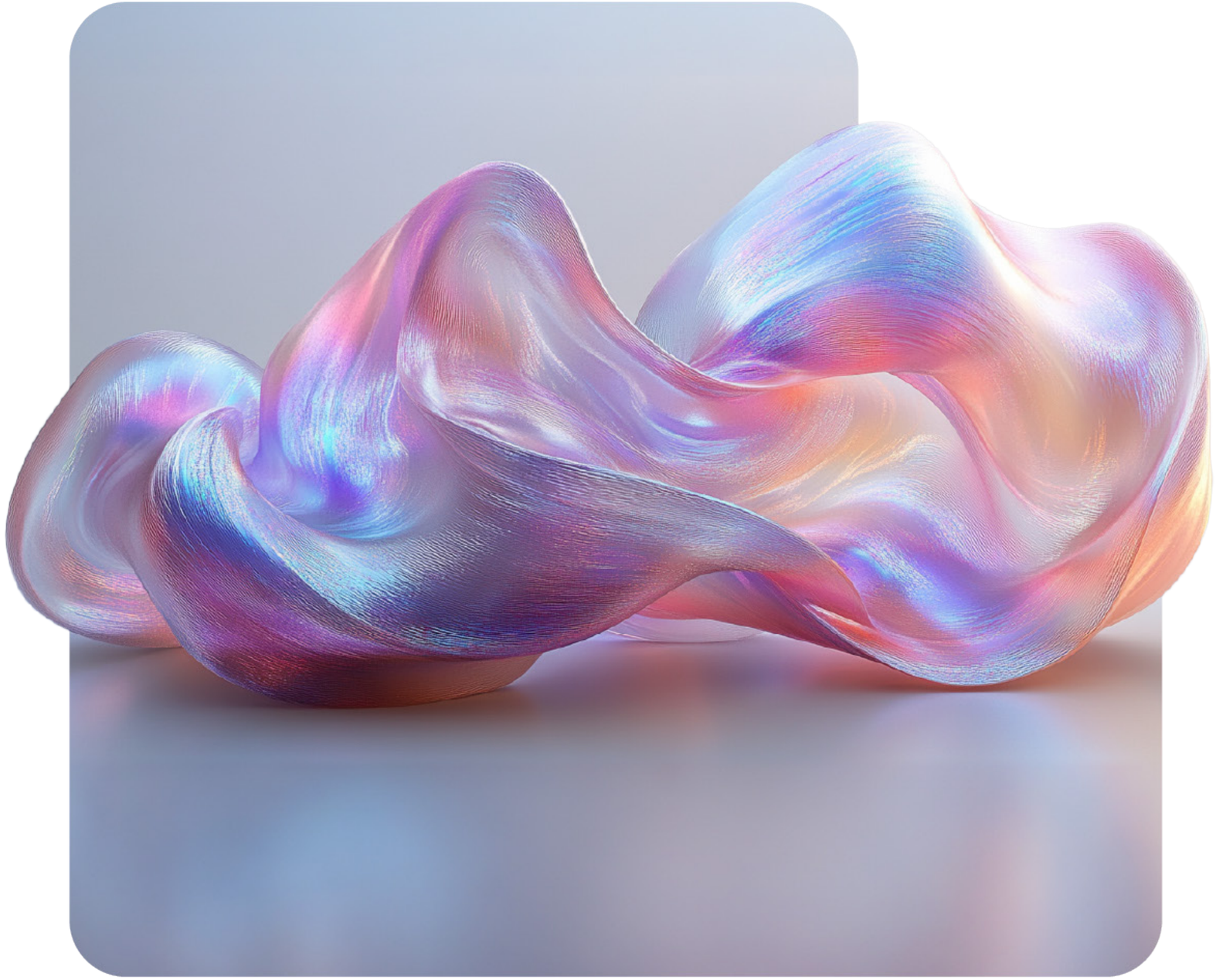
KEEP GOING

Entre 2024 y 2025, el cibercrimen muestra un crecimiento acelerado y sofisticado. En 2024, la detección de ataques por Ransomware aumentó 35%, y el phishing con QR creció 51%, mientras que un 27% más de empresas sufrieron ataques respecto al año anterior.

En 2025, las amenazas se intensificarán, impulsadas por IA y enfoques como deep fakes y ransomware dirigido. Proteger infraestructuras críticas y fomentar resiliencia serán prioridades esenciales.

Vivimos hiperconectados: más dispositivos, más datos y usuarios desde niños hasta adultos mayores. Nos convertimos en fábricas de materia prima digital: nuestros datos, deseos y comportamientos. Para nosotros, tienen valor; para el mercado y los ciberdelincuentes, precio. Se comercializan, trafican y explotan.

¿SOMOS CONSCIENTES DE LO QUE ENTREGAMOS?



BTR CONSULTING
BUSINESS DIGITAL SOLUTIONS

CONSTRUIMOS UN MUNDO DIGITAL
MÁS SEGURO Y HUMANO

/btrconsulting
btrconsulting.com