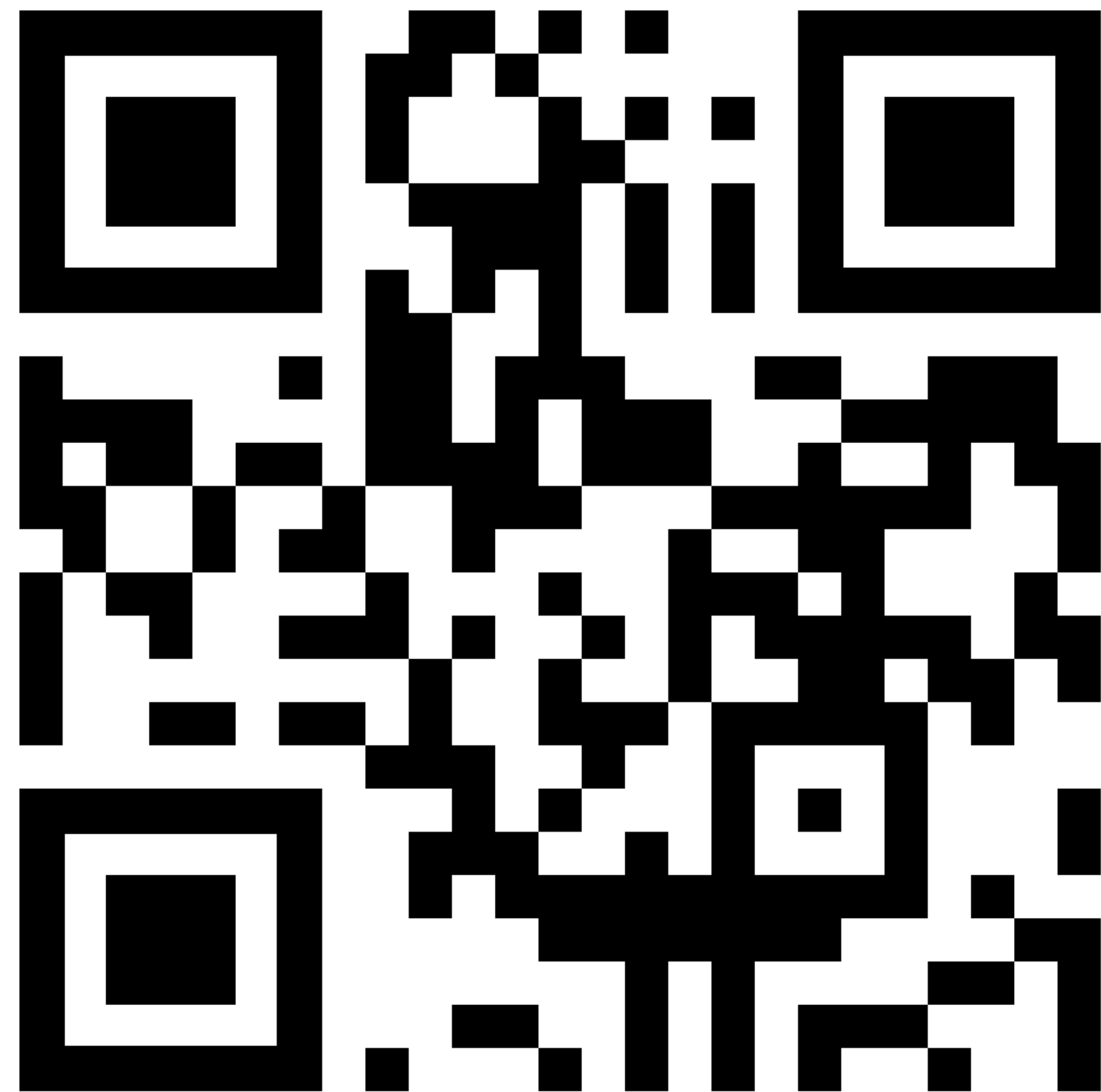
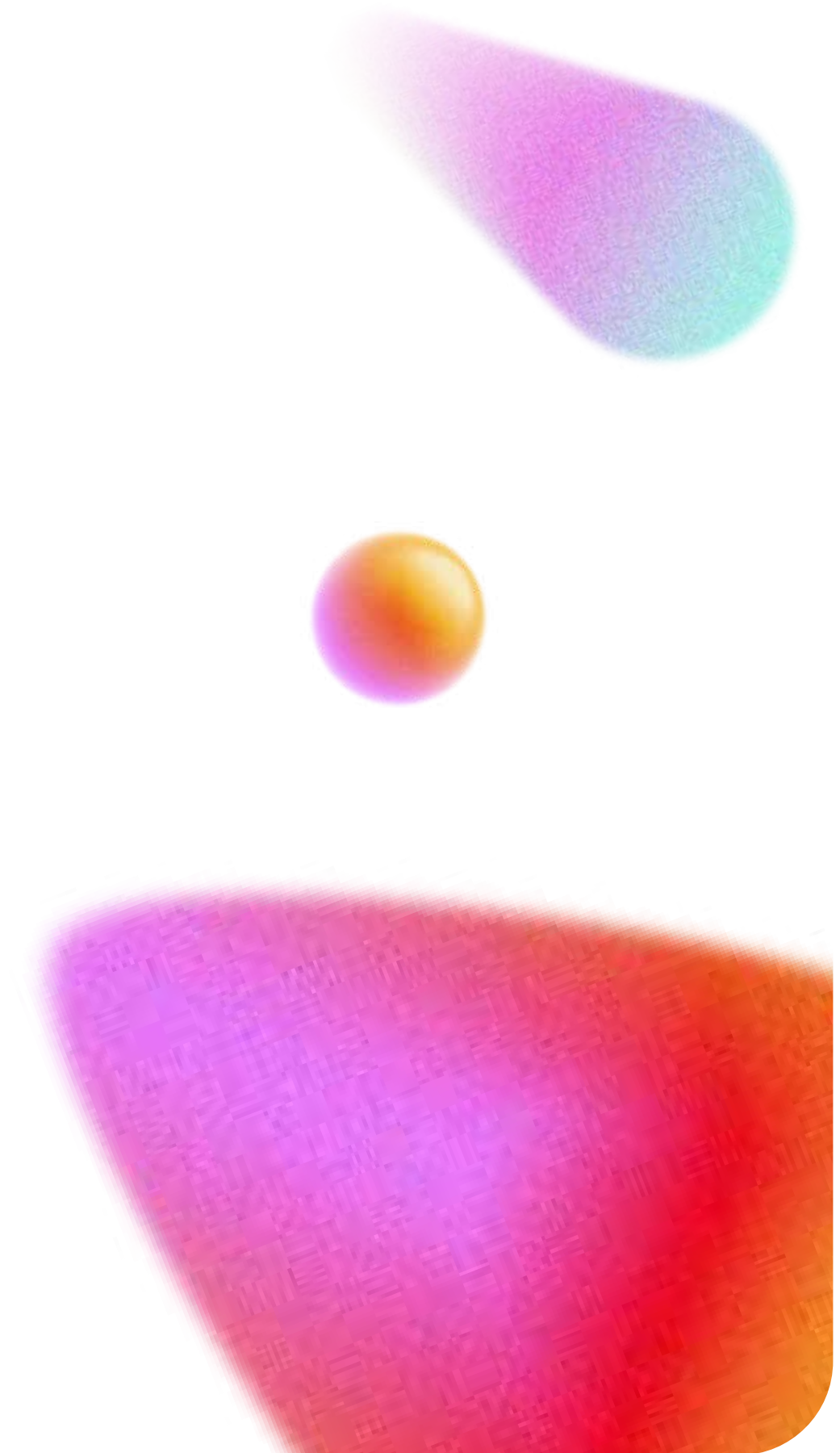


Webinar:

Opera un **CyberSOC**
académico
sin interrupciones



Descubre
nuestras soluciones





Pablo García

BDM CyberSecurity Latam
TIVIT



Carlos Rincón

Head Oper CyberSecurity Latam
TIVIT

Servicios cybersoc

Agente IA

Automatización como primera línea de defensa

CSIRT

Eficiencia y agilidad en momentos críticos.

Threat Intel

Anticipación y valor directo al cliente.

Threat Hunting

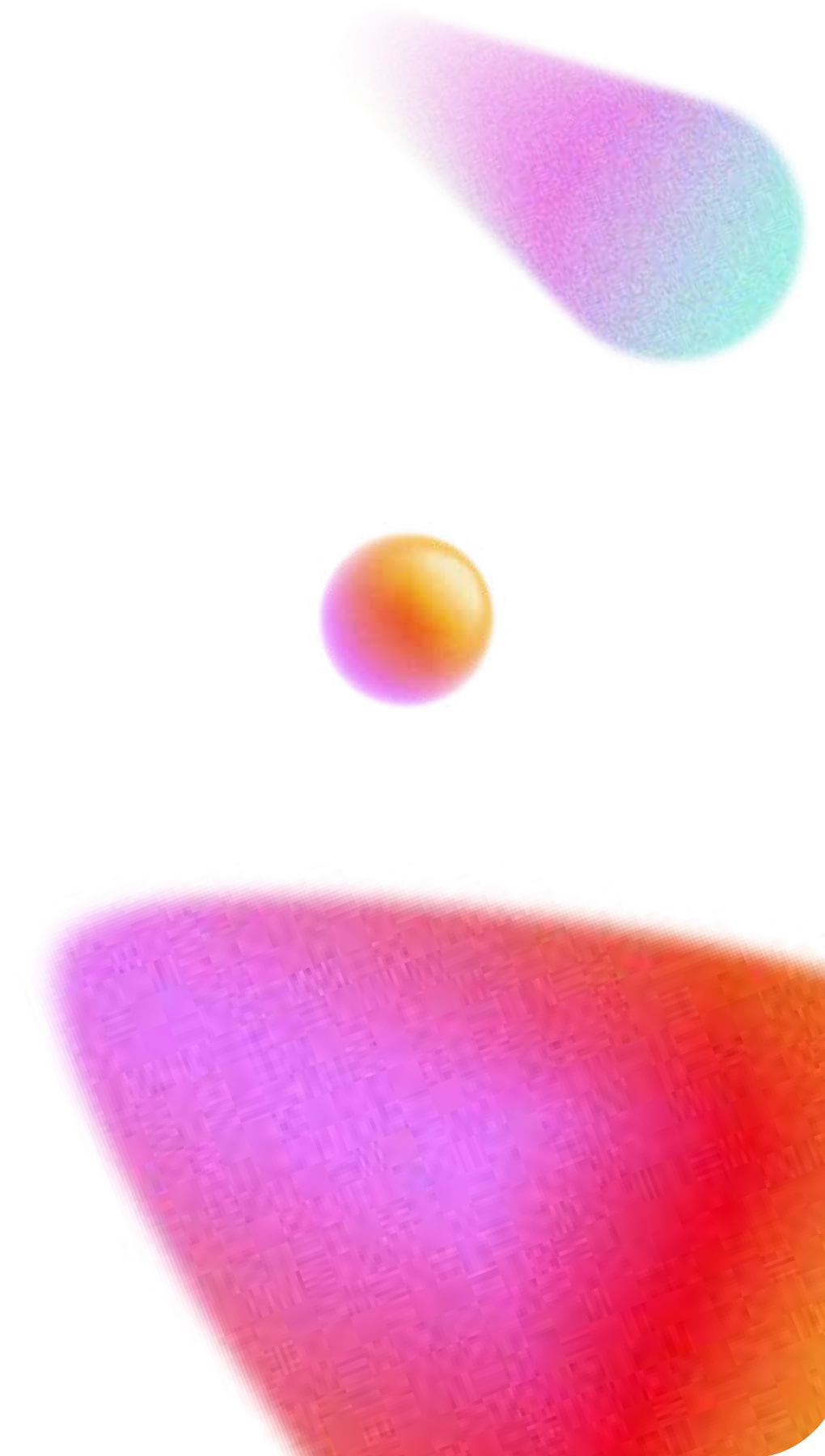
Evolución de un modelo reactivo a uno proactivo.

Análisis forense

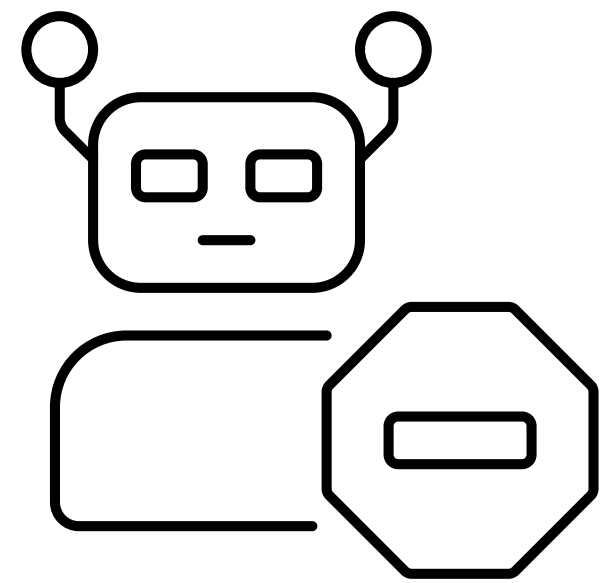
Aprendizaje post-incidente y visibilidad.

RedTeam

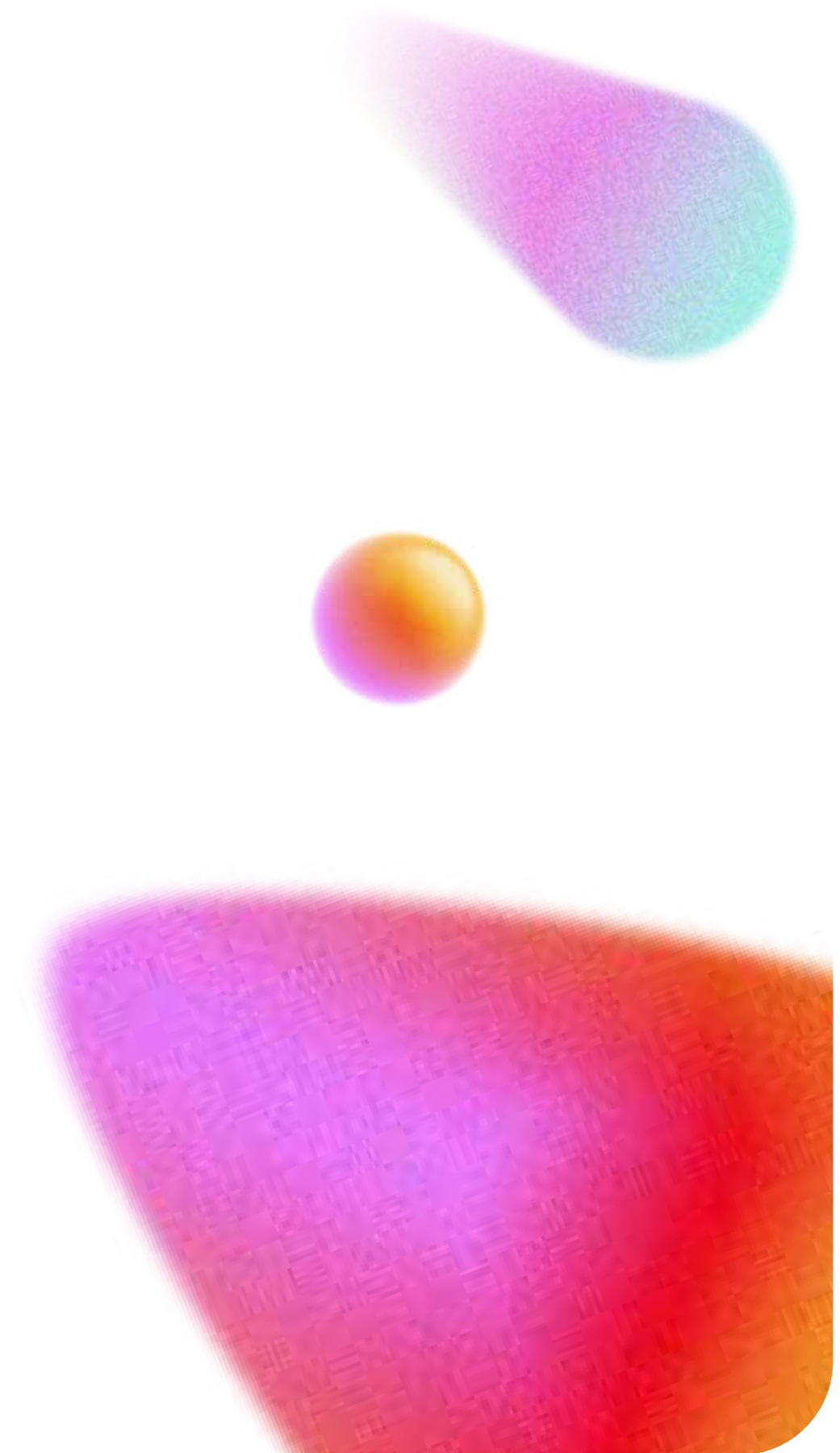
Validación continua de nuestras defensas.



Agente IA *Propósito Estratégico*



Transformar la operación del **SOC** mediante la automatización inteligente del análisis inicial de eventos de seguridad, liberando a nuestros analistas para tareas de alto valor estratégico.



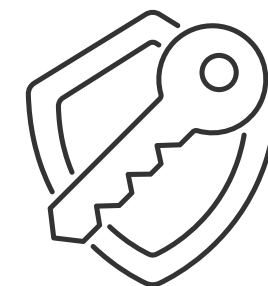
Agente IA Propósito Estratégico

 **Con esta iniciativa buscamos:**



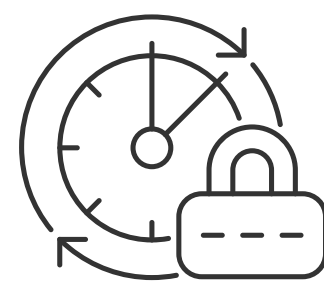
Eficiencia Operativa:

Automatizar al 100% el triage de Nivel 1 y el enriquecimiento de datos, eliminando la fatiga de alertas.



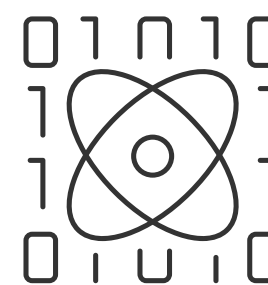
Agilidad y Cumplimiento:

Reducir drásticamente los tiempos de respuesta (MTTR) para garantizar el cumplimiento de SLAs críticos y complejos.



Calidad y Precisión:

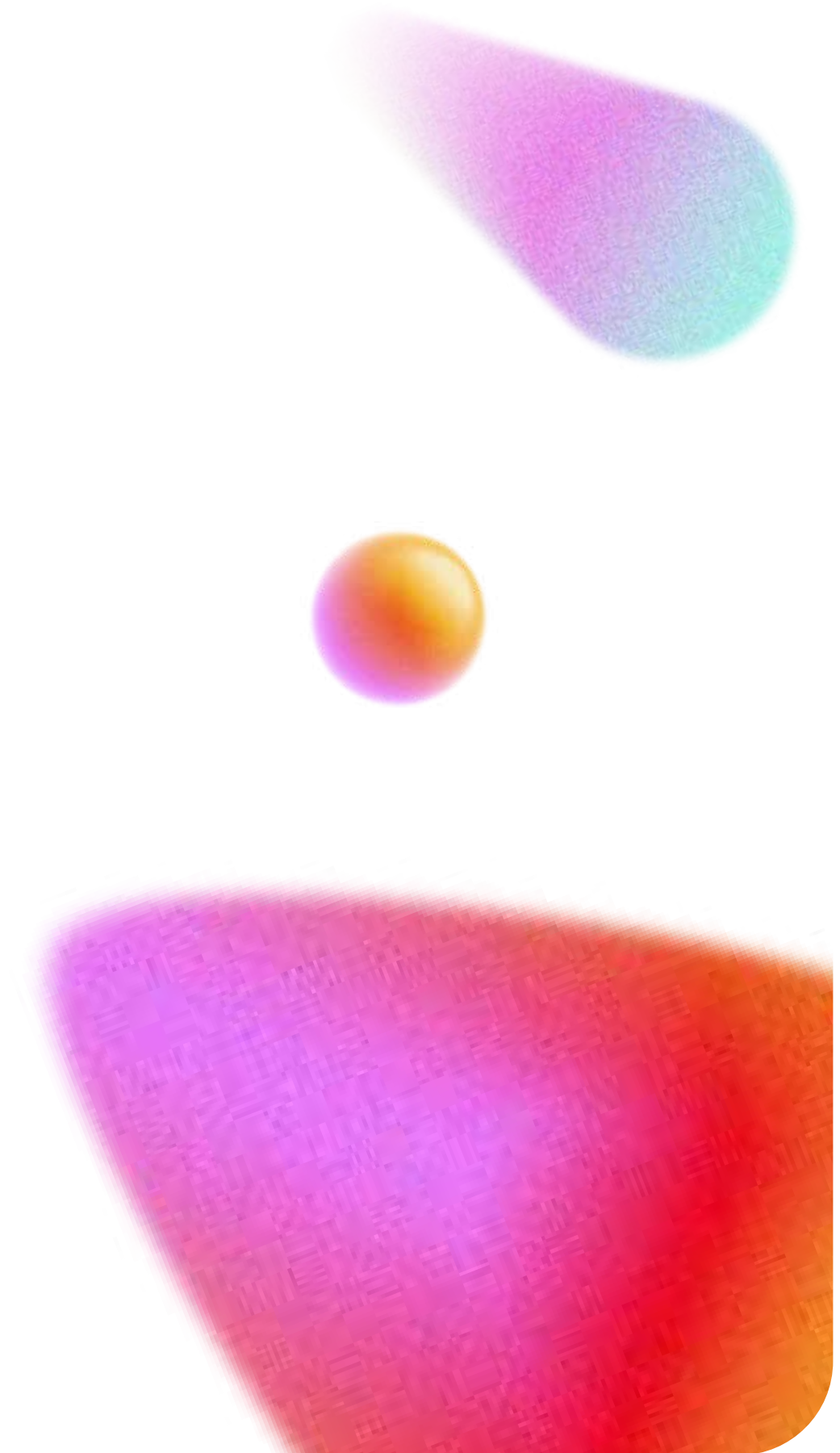
Generar análisis estructurados, estandarizados y con contexto profundo, elevando el nivel de las notificaciones hacia el cliente.



Control Inteligente:

Mantener un modelo seguro (Human-in-the-loop), donde la IA procesa el volumen masivo y el humano toma la decisión final.

Resultado esperado consolidar un SOC corporativo altamente eficiente, nativamente escalable frente a picos de amenazas, y con procesos de resolución estandarizados impulsados por IA.



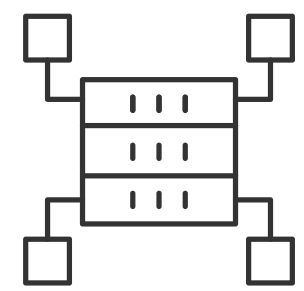
Agente IA Flujo de análisis



Transformar la operación del **SOC** mediante la automatización inteligente del análisis inicial de eventos de seguridad, liberando a nuestros analistas para tareas de alto valor estratégico.

Agente IA *Flujo de análisis*

 **El proceso consta de los siguientes pasos clave:**



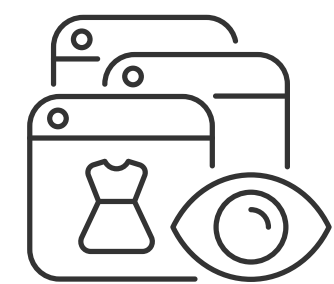
Extracción e Ingesta:

Se recopila la alerta del SIEM y se extraen los Indicadores de Compromiso (IOCs) como IPs, hashes y dominios.



Enriquecimiento y Contexto:

Los IOCs se enriquecen consultando múltiples fuentes externas de inteligencia (VirusTotal, AlienVault, etc.) y se contextualizan combinándolos con datos históricos.



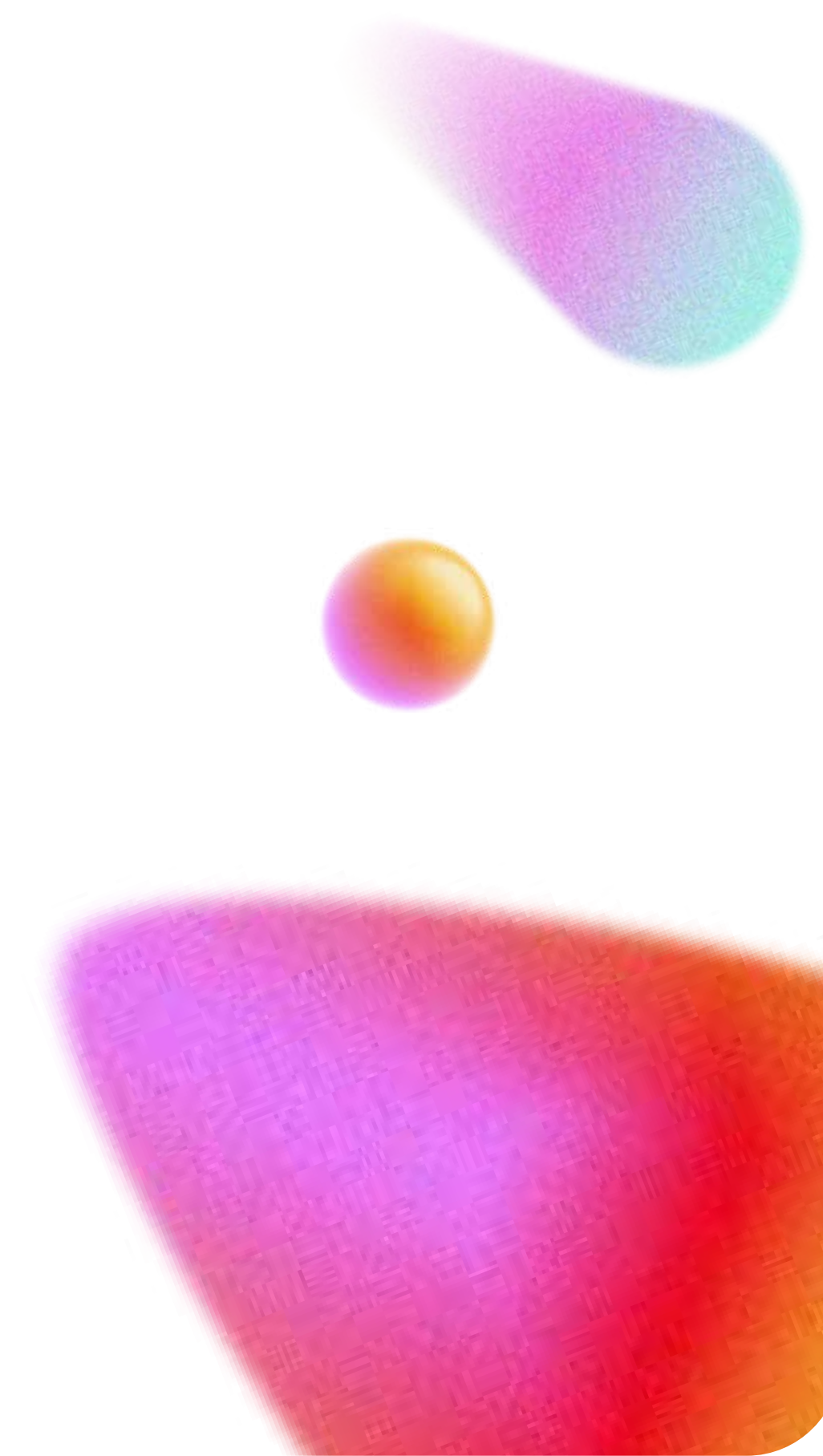
Análisis por IA Especializada:

Tres agentes de IA distintos (Validación, Análisis, Decisión), impulsados por un núcleo central de Gemini 2.5 Flash, procesan la alerta para validar su autenticidad y determinar la mejor línea de acción.



Reporte y Acción:

Una vez tomada la decisión, el flujo genera un reporte detallado y envía notificaciones automáticas a través de email (vía SendGrid) y Google Chat para una respuesta rápida y validación humana.

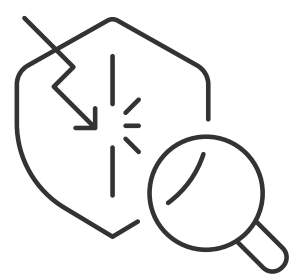


Equipo CSIRT

Flujo de Triage Avanzado y Gestión de Incidentes CSIRT

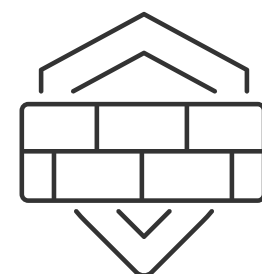
¿Qué hace el CSIRT?

El CSIRT es nuestro equipo de especialistas responsable de resolver de principio a fin las alertas críticas escaladas por el SOC. Su trabajo se resume en 3 acciones clave:



Validación Definitiva:

Analiza a fondo el evento para confirmar si es un ataque real o descartar como falso positivo.



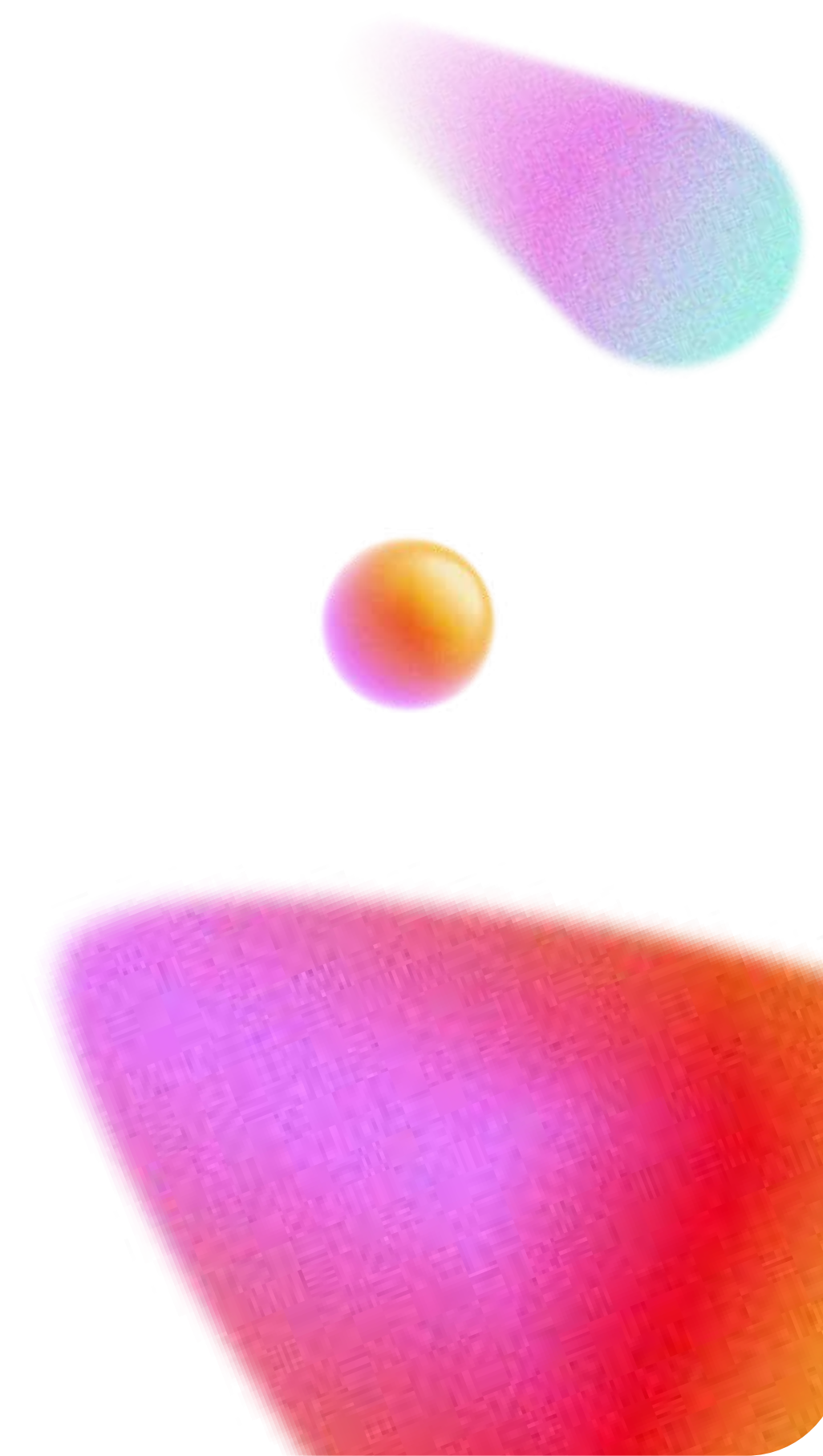
Contención Inmediata:

Si hay riesgo, ejecuta y coordina los bloqueos necesarios en la infraestructura para detener el ataque al instante.



Cierre y Transparencia:

Elabora el "Informe oficial de cierre", dándole al cliente visibilidad total sobre qué pasó y cómo se soluciona.



Equipo CSIRT

Flujo de Triage Avanzado y Gestión de Incidentes CSIRT

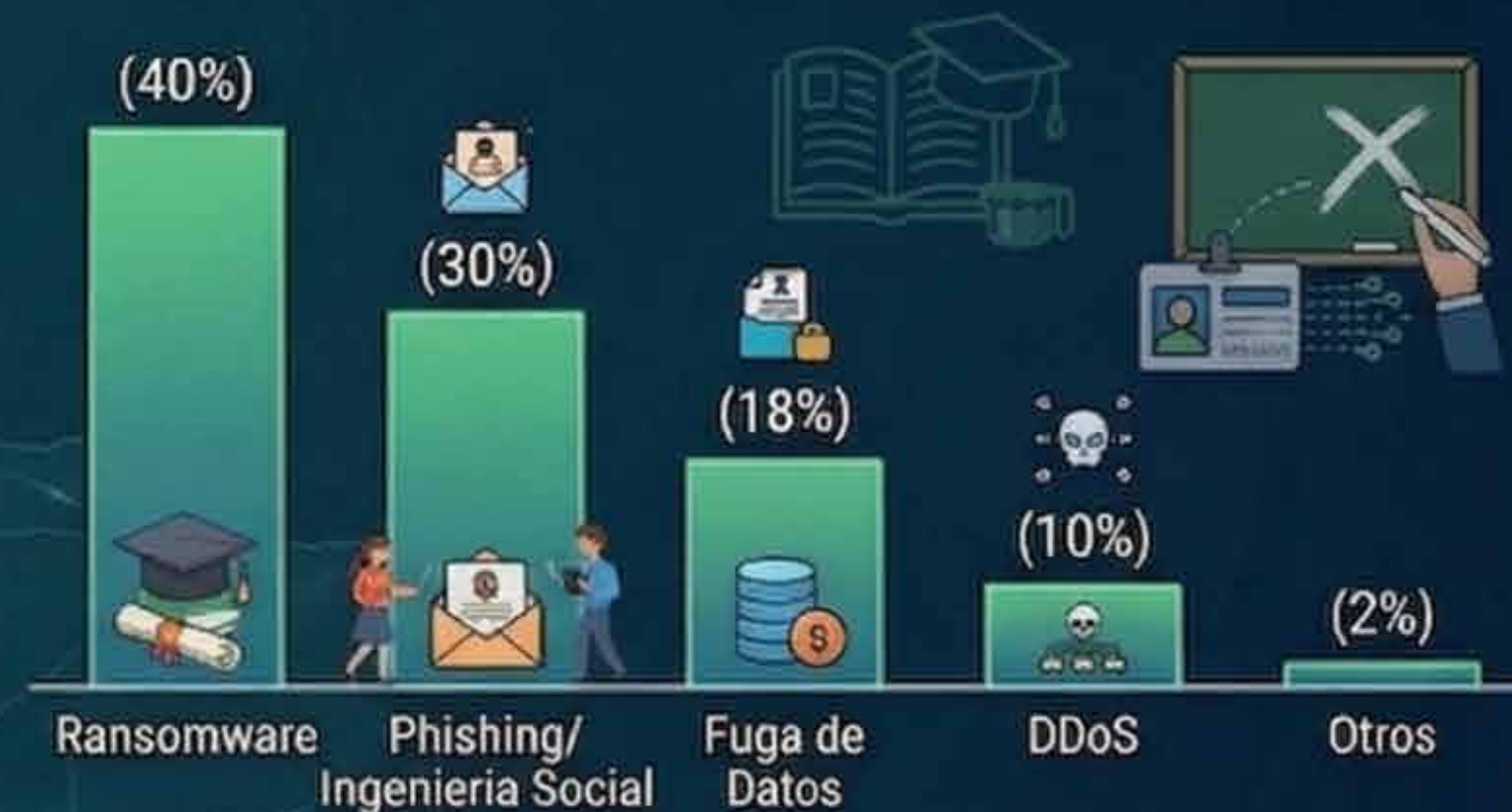


ESTADÍSTICAS DE CIBERATAQUES EN EL SECTOR EDUCACIÓN - COLOMBIA 2026

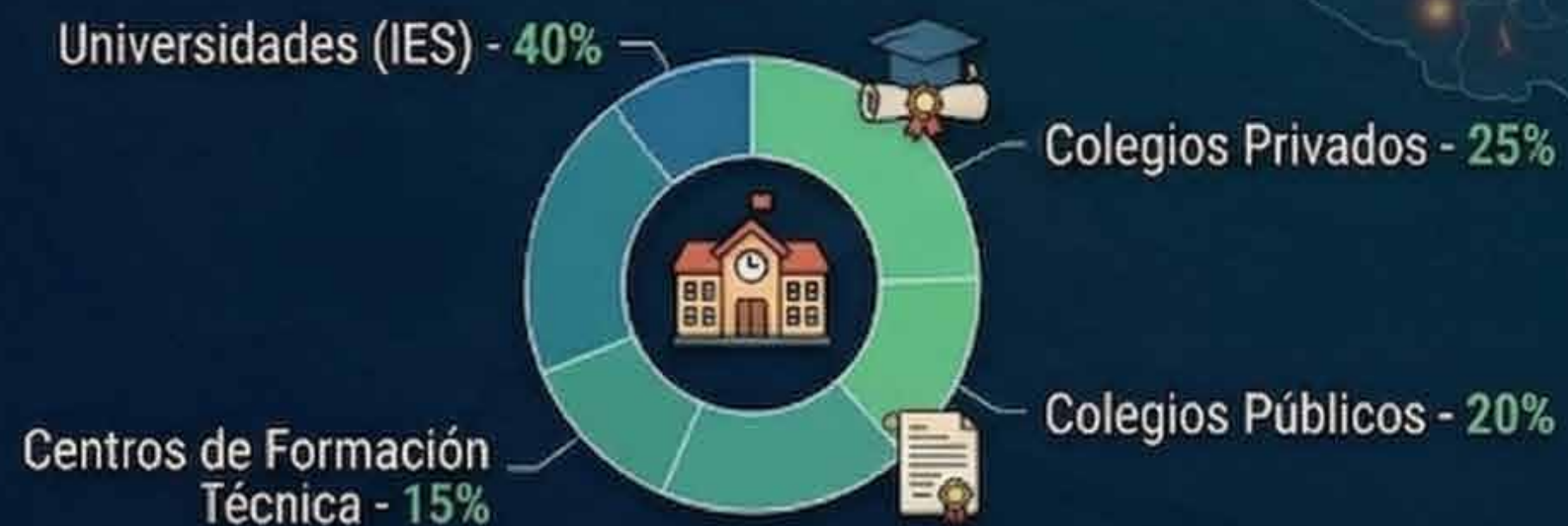
PANORAMA GENERAL



TIPOS DE ATAQUES MÁS FRECUENTES



ENTIDADES MÁS AFECTADAS (IES, Escuelas)



IMPACTO DE LOS CIBERATAQUES

1. Interrupción de Clases y Exámenes
2. Robo de Datos de Estudiantes y Personal
3. Robo de Propiedad Intelectual/Investigación
4. Daño Reputacional y Pérdida de Matrículas
5. Pérdidas Financieras y Multas

Cifras ilustrativas basadas en proyecciones y tendencias actuales para 2026

ESTADÍSTICAS DE CIBERATAQUES EN EL SECTOR SALUD - COLOMBIA 2026

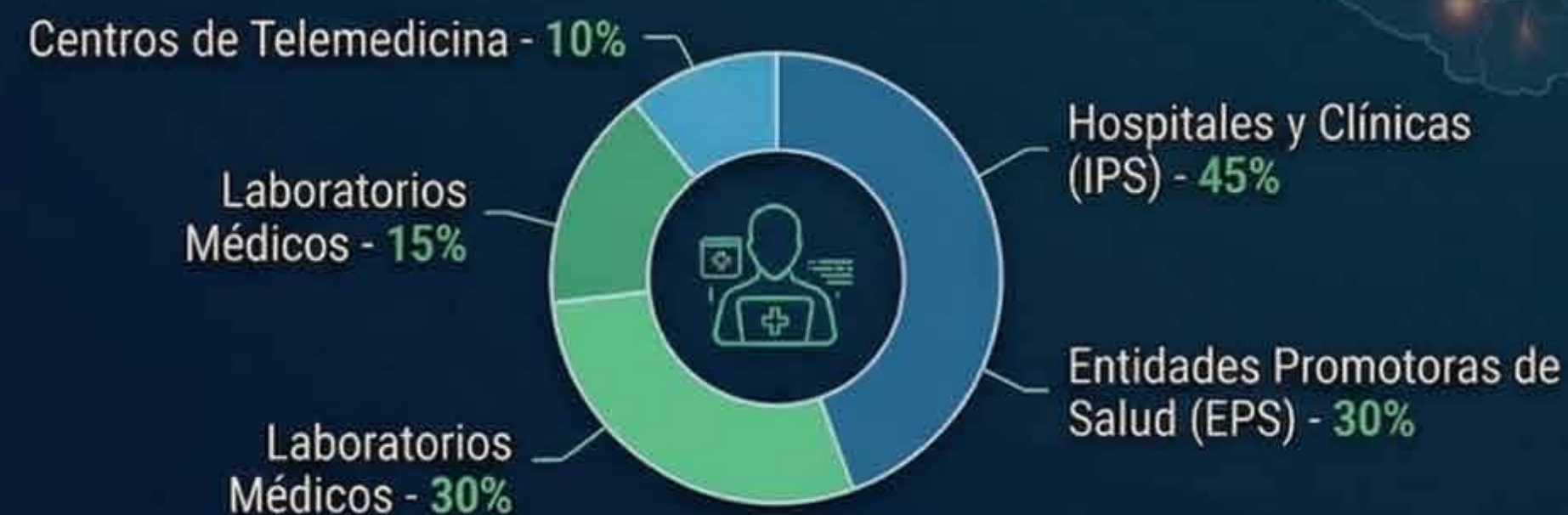
PANORAMA GENERAL



TIPOS DE ATAQUES MÁS FRECUENTES



ENTIDADES MÁS AFECTADAS (IPS y EPS)



IMPACTO DE LOS CIBERATAQUES

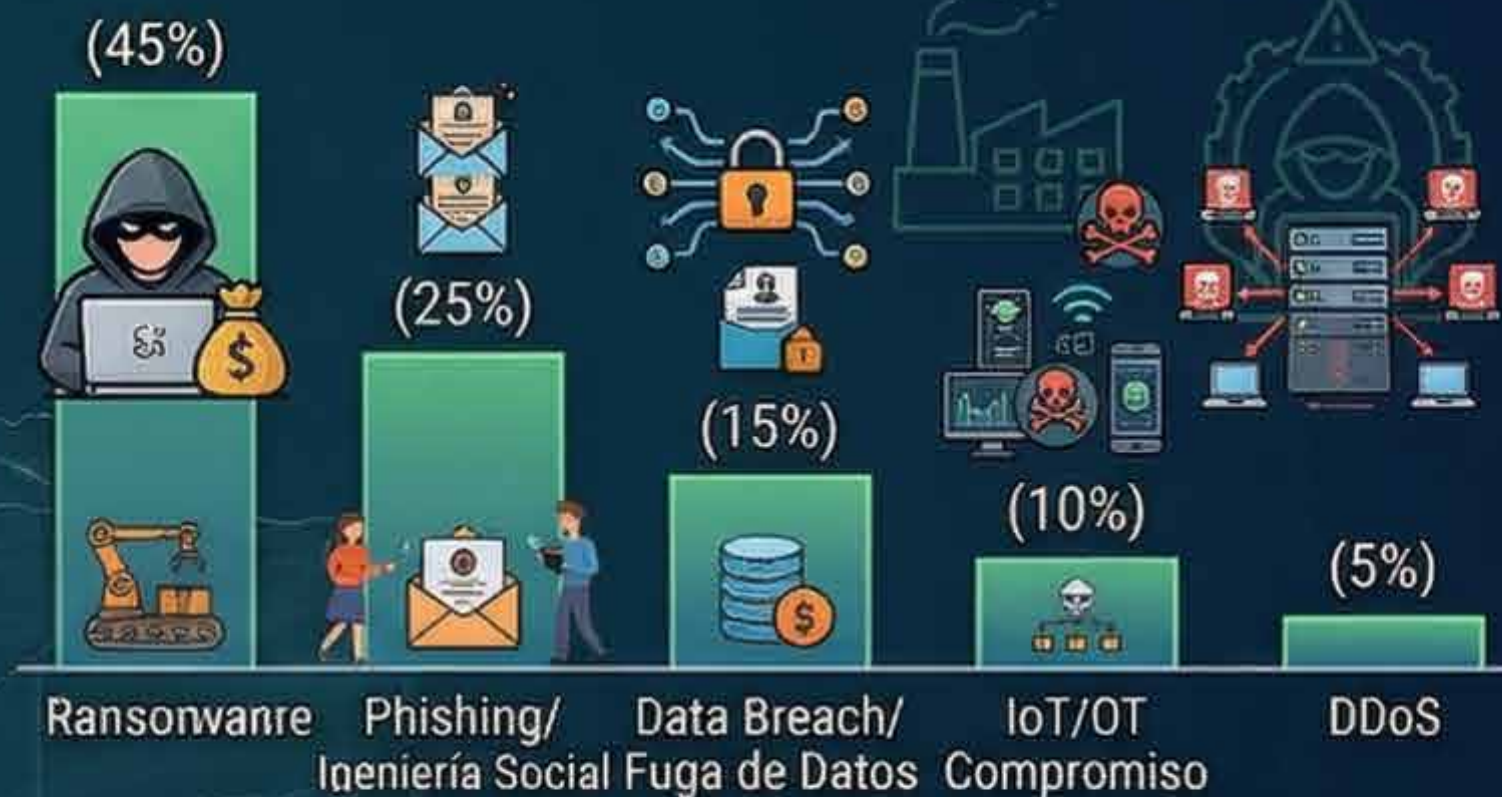
1. Interrupción de Servicios Médicos
2. Robo de Datos Personales y Clínicos
3. Daño Reputacional
4. Multas y Sanciones Regulatorias
5. Pérdidas Financieras Directas

ESTADÍSTICAS DE CIBERATAQUES EN EL SECTOR INDUSTRIA - COLOMBIA 2026

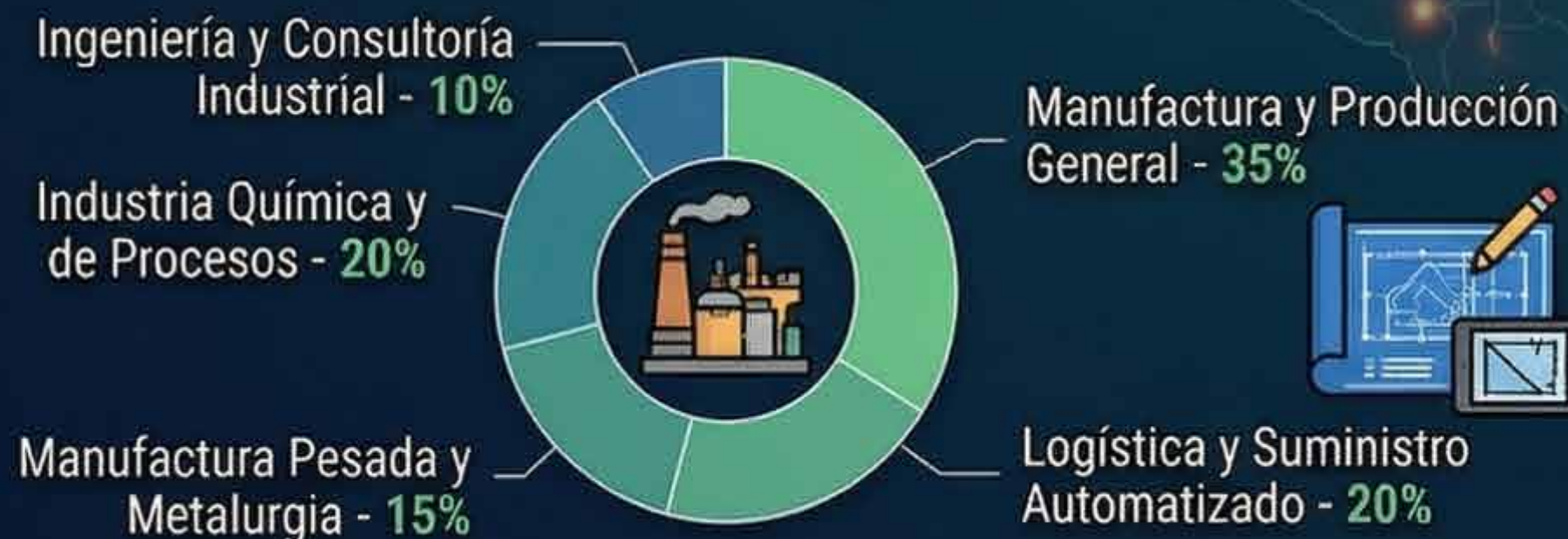
PANORAMA GENERAL



TPOS DE ATAQUES MÁS FRECUENTES



ENTIDADES MÁS AFECTADAS (Manufactura y Suministro)



IMPACTO DE LOS CIBERATAQUES

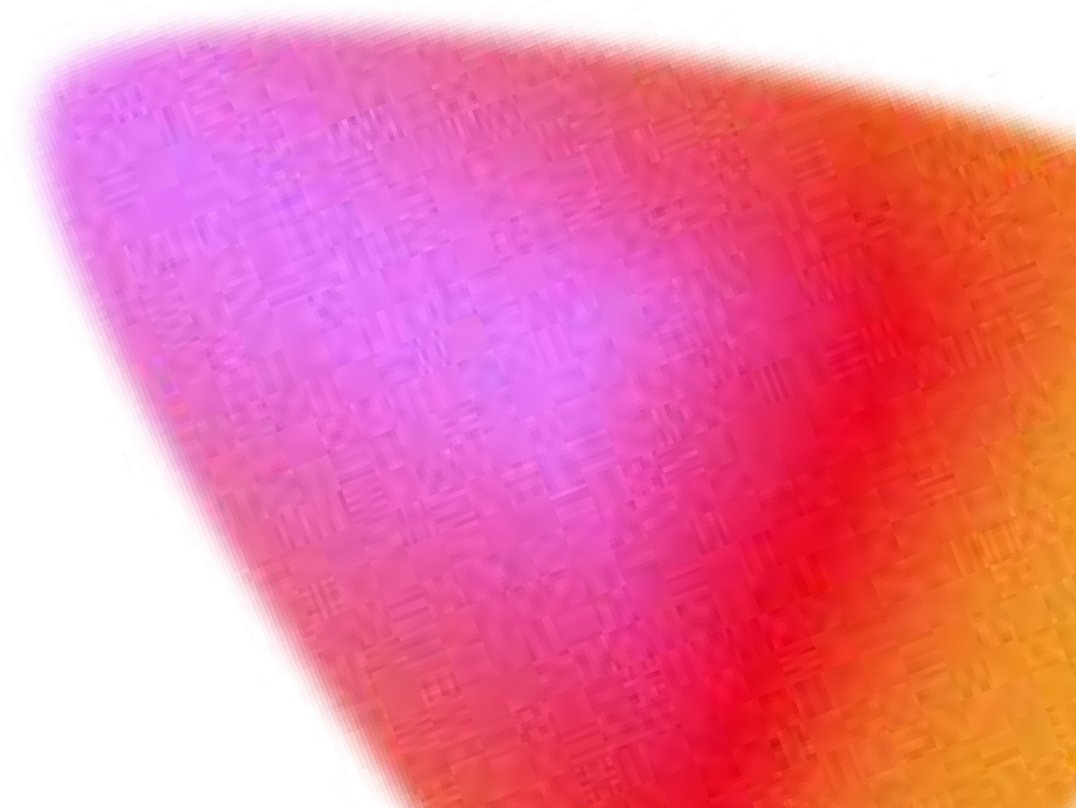
1. Interrupción de Cadena de Suministro y OT
2. Paralización de Líneas de Producción
3. Robo de Propiedad Intelectual Industrial
4. Daño Reputacional y Pérdida de Clientes B2B
5. Multas, Sanciones y Costos Financieros Directos

CONSEJO DE CIBERRESILIENCIA INDUSTRIAL ICS



SEGMENTACIÓN DE RED OT/IT Y AUDITORÍAS ICS/SCADA

¿Preguntas?





*Asesórate
para implementar
este producto
en tu negocio*

*Escríbenos
marketinglatam@tivit.com*

