Magneto INTelligence

Seguridad Integral en Banca: Protegiendo Datos, Activos y Confianza

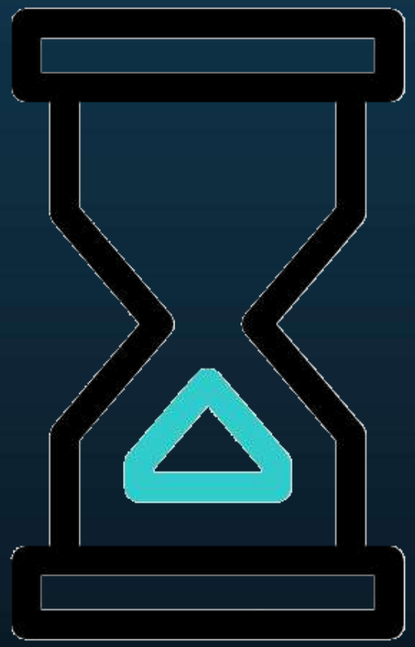
VI CONGRESO INTERNACIONAL
DE CIBERSEGURIDAD, PROTECCIÓN DE DATOS, PREVENCIÓN DE FRAUDES Y SEGURIDAD FÍSICA

"CONSTRUYENDO CONFIANZA DIGITAL: INNOVACIÓN, IA SEGURA Y DATOS PROTEGIDOS EN UN MUNDO INTERCONECTADO"

01

TIEMPO MEDIO DE DETECCIÓN DE UNA AMENAZA

¿Cuánto tiempo lleva un atacante dentro antes de ser descubierto?



¿Cuánto tiempo lleva un atacante dentro antes de ser descubierto?

11

Días de media

Tiempo medio global de permanencia de un atacante en los sistemas antes de ser detectado.

194

Días en OT/ICS

En entornos de tecnología operacional e infraestructuras críticas, el tiempo de permanencia puede superar los 6 meses

21

Días hasta contención

Tiempo medio adicional para contener el incidente una vez identificado.

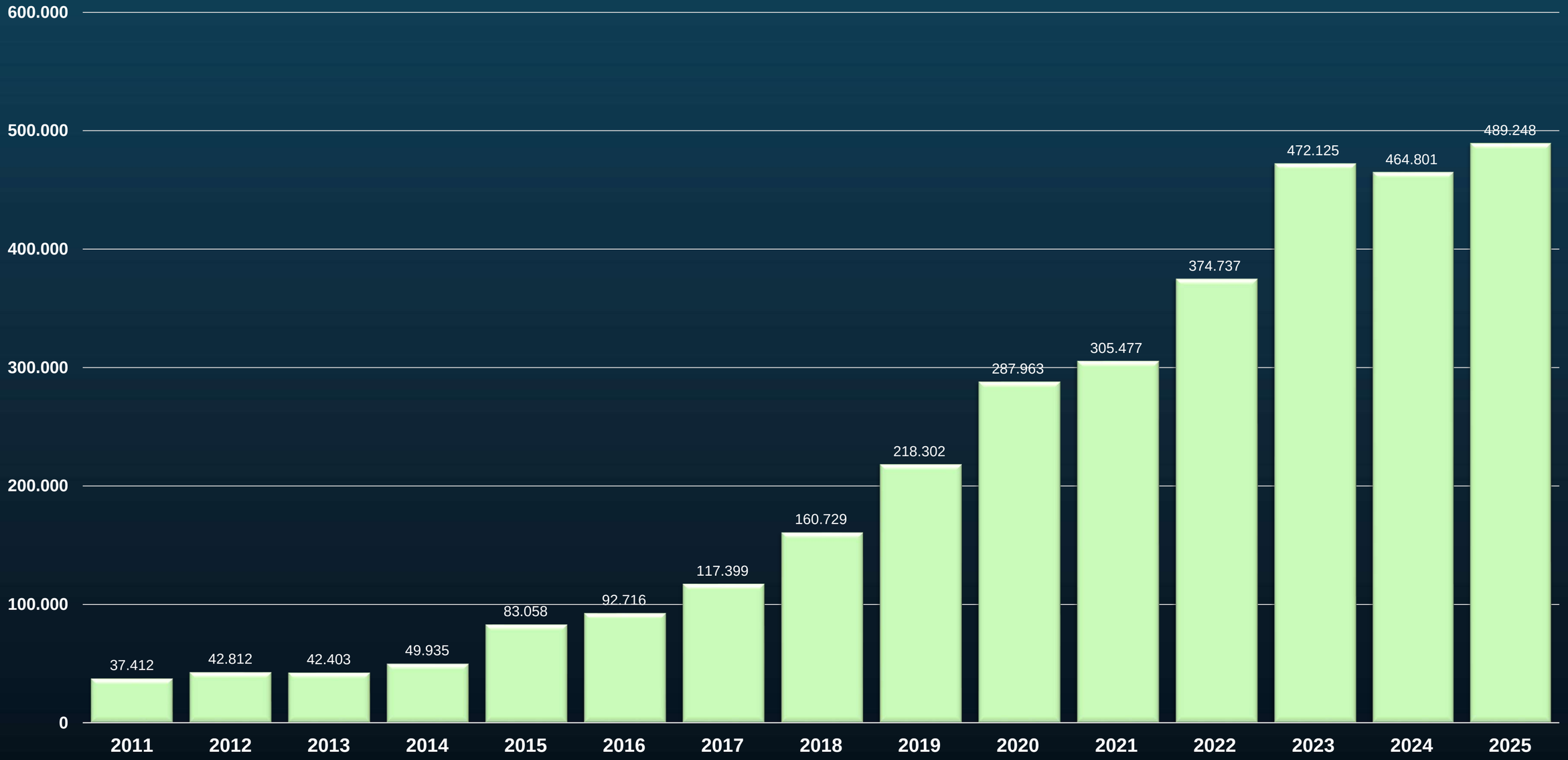
Cada día sin detección es una oportunidad para el atacante: exfiltración de datos, movimiento lateral y preparación de sabotaje.

Distribución del Tiempo de Permanencia

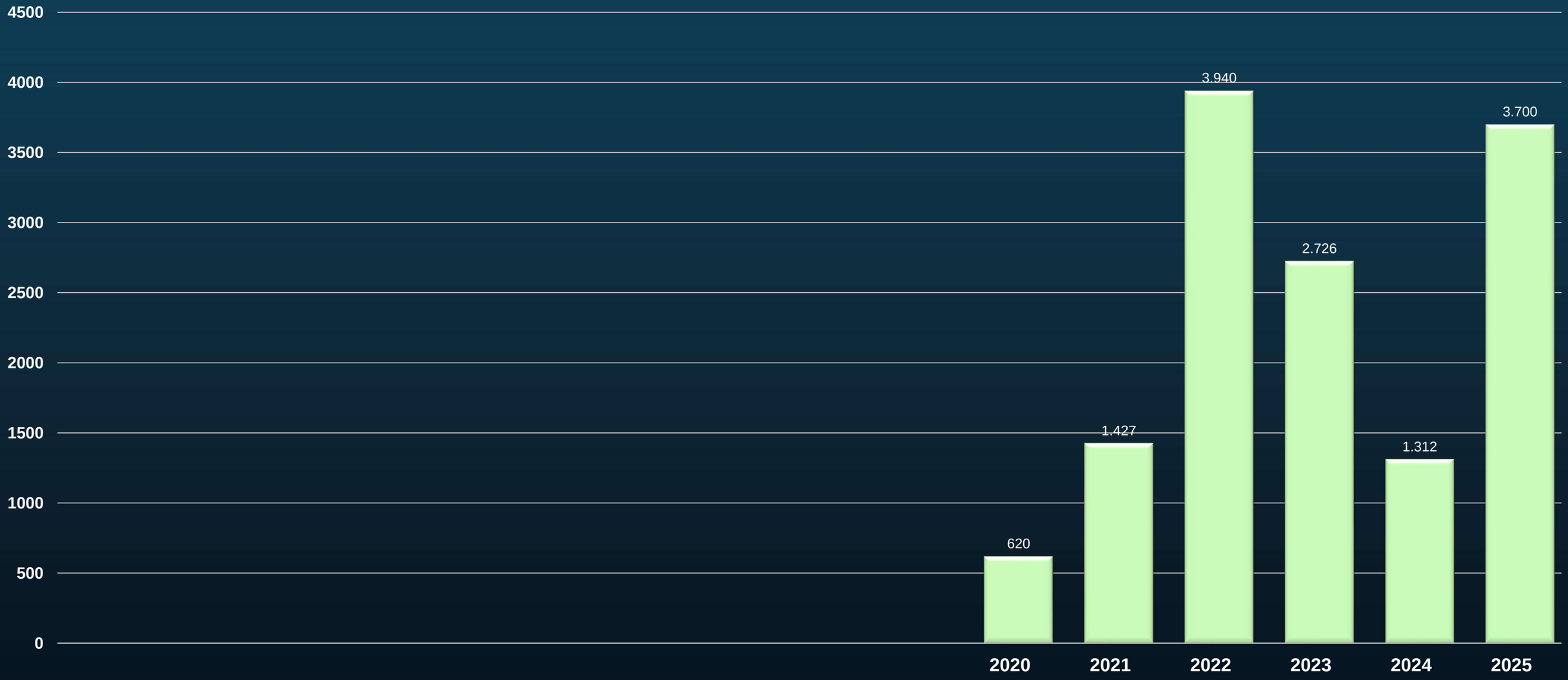
Evolución temporal

	< 1 SEMANA	8 A 31 DÍAS	1 A 6 MESES	6 MESES a 1 AÑO	> de 1 AÑO
2021	37,4%	17,7%	26,2%	10,7%	0,3%
2022	42%	16%	24%	7%	0%
2023	43,3%	22,7%	22,3%	5,4%	0,2%
2024	45,1%	17,6%	23,9%	5,9%	7,5%

Evolución del Cibercrimen



Evolución del Cibercrimen



Evolución del Cibercrimen: la cifra negra

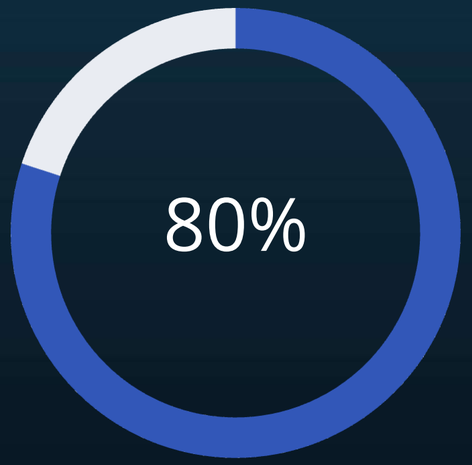
Las estadísticas oficiales representan solo una fracción de la realidad. La enorme brecha entre víctimas reales y denuncias formales revela la verdadera magnitud del problema.

Estimación UNODC

Total estimado de víctimas: 2.360.625

Solo el 20% denuncia → 472.125 denuncias

Cifra negra: 1.888.500 víctimas sin registrar



No denuncia

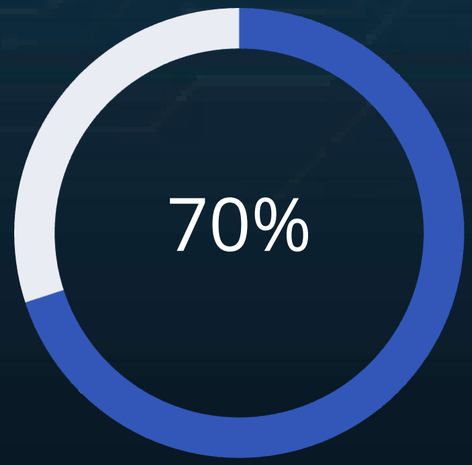
4 de cada 5 víctimas no reportan el incidente a las autoridades

Estimación UE

Total estimado de víctimas: 1.573.750

El 30% denuncia → 472.125 denuncias

Cifra negra: 1.101.625 víctimas sin registrar



No denuncia

Escenario conservador: 7 de cada 10 víctimas permanecen en silencio

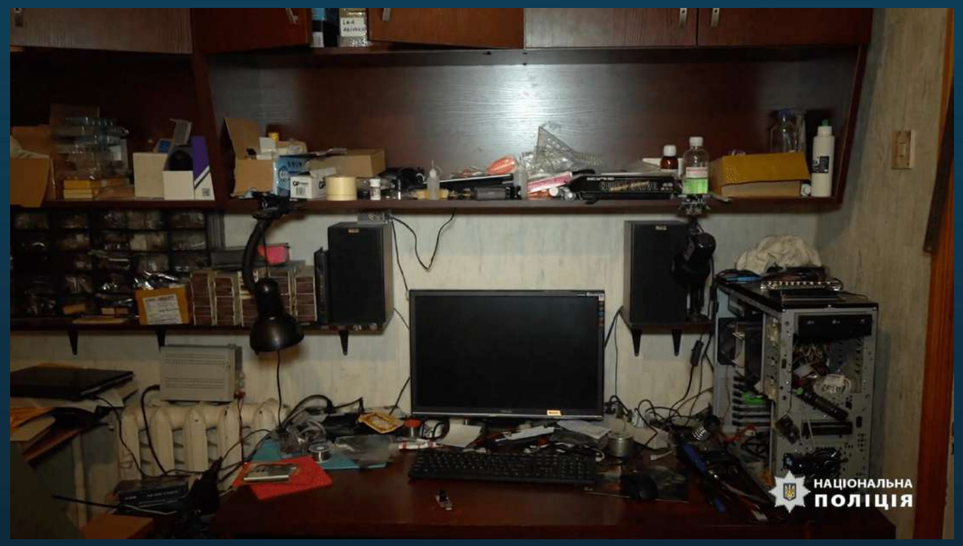
02

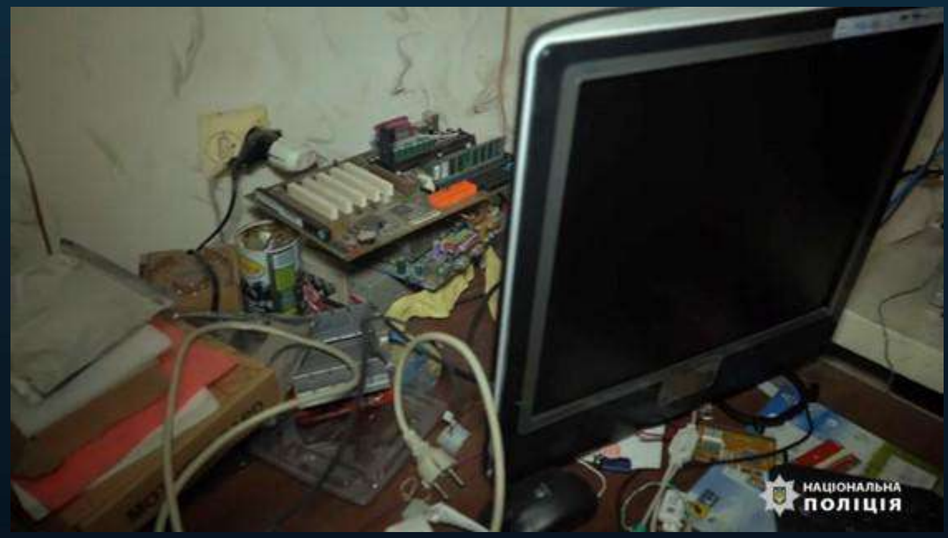
CARACTERÍSTICAS DEL CIBERCRIMEN

PERCEPCIÓN DEL ATACANTE

COSTE ECONÓMICO

COSTE ECONÓMICO





HERRAMIENTAS

UBICUIDAD

HIPERCONECTIVIDAD

CRIME AS A SERVICE

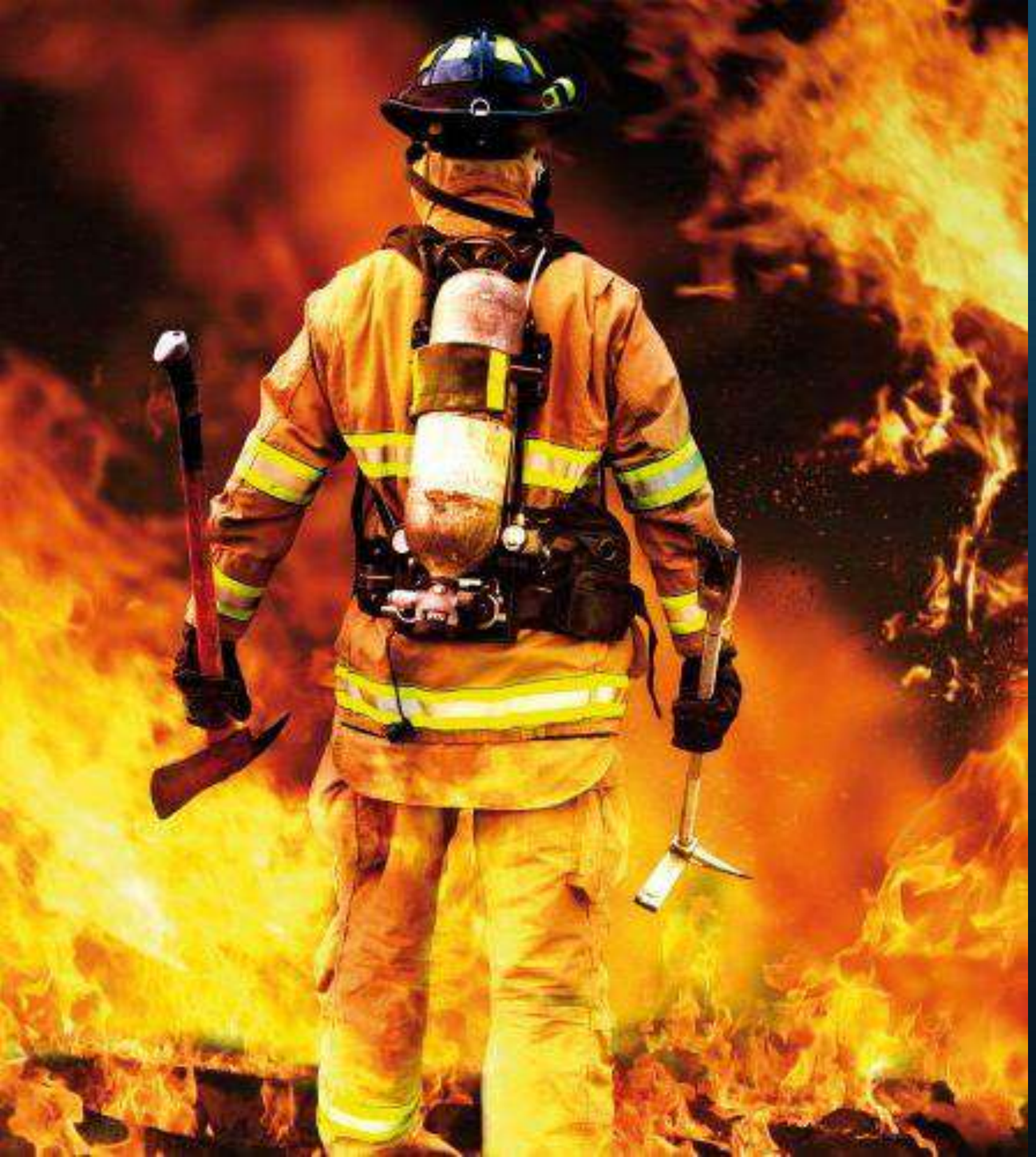
ALTO IMPACTO

REFLEXIÓN CLAVE

Una realidad incómoda

La mayoría de las organizaciones descubre el ataque **demasiado tarde**. Para cuando se activa la alarma, los atacantes ya han tenido tiempo de explorar sistemas, exfiltrar información sensible o preparar acciones de sabotaje contra la infraestructura.

El problema no es únicamente tecnológico: es de visibilidad, anticipación e inteligencia. La detección reactiva ya no es suficiente.



REACTIVOS

LOS 5 PILARES EN PERSPECTIVA

Ciberseguridad

Intercambio de conocimiento y protección de sistemas críticos

Protección de Datos

Cumplimiento ético y regulatorio en la gestión de la información

Prevención del Fraude

Análisis de tendencias y estrategias activas de mitigación

Seguridad Física

Protección integral de activos tangibles e intangibles

Ética Digital

Políticas responsables que respetan la privacidad y los derechos del usuario

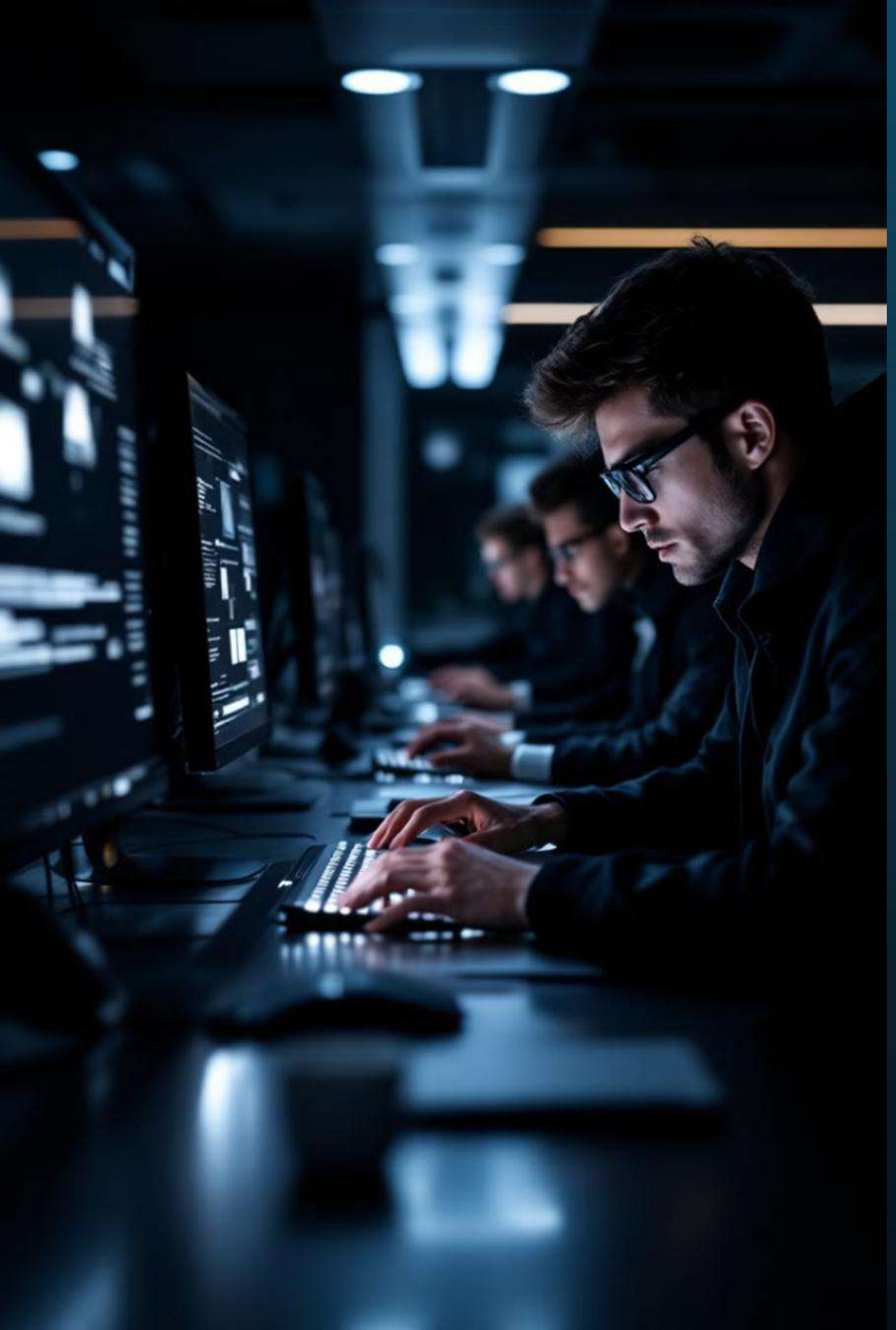
03

IMPACTO FINANCIERO

Un día de parálisis por ciberataque puede costar millones.

Analicemos el desglose para comprender mejor su impacto.

Datos basados en empresa con facturación anual de US$100 millones



Impacto en Diferentes Áreas

Finanzas

Pérdida de ingresos y aumento de gastos

Operaciones

Interrupción de procesos y servicios críticos

Reputación

Daño a la imagen y confianza del cliente

Legal

Posibles multas y sanciones regulatorias

Desglose de Pérdidas Diarias

273.973$

Ingresos Perdidos

Impacto directo en la facturación diaria

33.333$

Costes Operativos

Gastos fijos que continúan acumulándose

¿?

Pérdidas Indirectas

Multas y costes de recuperación

307.306$

Coste Total Diario

Suma de todas las pérdidas

La AEPD multa a Iberdrola con 6,5 millones por desproteger a sus clientes

La AN confirma la multa de 600.000 euros que la AEPD impuso a Air Europa por una brecha de seguridad

La AEPD les multó tras haber quedado al descubierto datos personales y bancarios de 489.000 clientes.

Blanca Valdés | 01/8/2024 05:30 | Actualizado: 02/8/2024 00:47

elDiario.es

Hazte socio/a Inicia sesión

Política Internacional Economía Opinión Cultura Clima Desalambre Igualdad Vertele Juegos

Multa de 1,3 millones de euros a Telefónica por un ciberataque que afectó a más de un millón de clientes

La brecha, abierta en 2022, permitió el robo de datos como el número de teléfono, el usuario y contraseña de las conexiones wifi de los afectados. Telefónica recurrirá la sanción, impuesta por Protección de Datos

— Fin a la impunidad ante un ciberataque: la alta dirección de las empresas será responsable de las brechas de seguridad

Fachada de la sede de Telefónica, a 7 de noviembre de 2024, en Madrid (España). Eduardo Parra - Europa Press

Carlos del Castillo
5 de diciembre de 2024 -17:43 h Actualizado el 05/12/2024 -17:53 h 2

SEGUIR AL AUTOR/A

La Agencia Española de protección de Datos (AEPD) ha multado a Telefónica con 1,3 millones de euros por un agujero de seguridad descubierto en septiembre de 2022 y que permitió que un ciberatacante se hiciera con los datos personales de más de un millón de clientes de sus

Lo más leído

1

Al Asad huye de Damasco y los rebeldes declaran la victoria mientras las potencias negocian el futuro de Siria

Francesca Cicardi

2

Manuel Marchena, el magistrado que siempre tenía razón

Alberto Pozas / Pedro Águeda

3

Responsabilidad Personal de Directivos

Supervisión Activa

Los directivos deben participar en la implementación de medidas de ciberseguridad.

Consecuencias por Negligencia

Multas individuales e inhabilitación para cargos directivos en casos graves.

Formación Continua

Obligación de mantenerse actualizado en temas de ciberseguridad portuaria.

Magneto INTelligence

Cambio de paradigma

Las organizaciones resilientes no solo protegen…

ANTICIPAN.

04

CiberInteligencia

Entendiendo la Ciberinteligencia

Concepto

La ciberinteligencia implica recopilar, analizar y procesar información sobre amenazas y riesgos cibernéticos.

Objetivo

Su objetivo principal es brindar información útil para la toma de decisiones en materia de ciberseguridad.

Valor

Su valor radica en permitir una defensa proactiva, identificar vulnerabilidades y mitigar riesgos.


Magneto
INTelligence

Magneto INTelligence

Sistema Operativo Multidimensional para Búsqueda y Reconocimiento de Amenazas

Plataforma de Ciberinteligencia multidimensional - SOMBRA

- OSINT
- Dark Web
- Redes sociales
- Señales digitales
- Inteligencia de actores

Todo convertido en información accionable

Qué permite

Detectar:

- Campañas antes de ejecutarse
- Actores hostiles activos
- Targeting de organizaciones
- Manipulación informativa
- Riesgos en cadena de suministro

Qué permite

Transformamos señales dispersas en inteligencia estratégica.

Ayudamos a organizaciones a ver antes lo que otros descubren demasiado tarde.

Vectores Actores	Cadena de Suministro	Desinformación y Manipulación	Inteligencia Artificial y Drones	Tensiones Geopolíticas	Consecuencias Legales	Computación Cuántica	Eventos Climáticos Extremos
Actores Estatales - APT	Muy Alto	Muy Alto	Muy Alto	Muy Alto	Muy Alto	Muy Alto	Alto
Operadores Cibercrimen	Alto	Moderado	Muy Alto	Moderado	Muy Alto	Muy Alto	Alto
Hacktivistas -Activistas	Moderado	Muy Alto	Moderado	Moderado	Moderado	Moderado	Muy Alto
Crimen Organizado	Muy Alto	Moderado	Moderado	Alto	Alto	Alto	Muy Alto
Competidores	Moderado	Alto	Moderado	Moderado	Moderado	Alto	Moderado
Amenazas Internas	Moderado	Moderado	Moderado	Moderado	Moderado	Moderado	Moderado

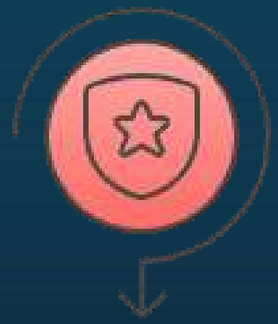
SOMBRA - Áreas de Aplicación

Ciberseguridad

Detección y prevención de ataques cibernéticos, análisis de malware, identificación de vulnerabilidades y gestión de incidentes de seguridad.

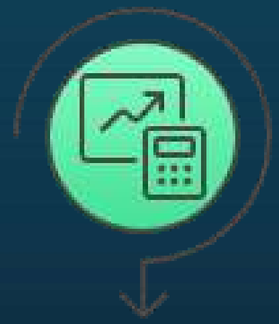
Inteligencia de Amenazas

Monitoreo de amenazas emergentes, identificación de actores maliciosos, análisis de campañas de desinformación y predicción de ataques.



Seguridad Nacional

Detección y prevención de actividades terroristas, crimen organizado y espionaje.



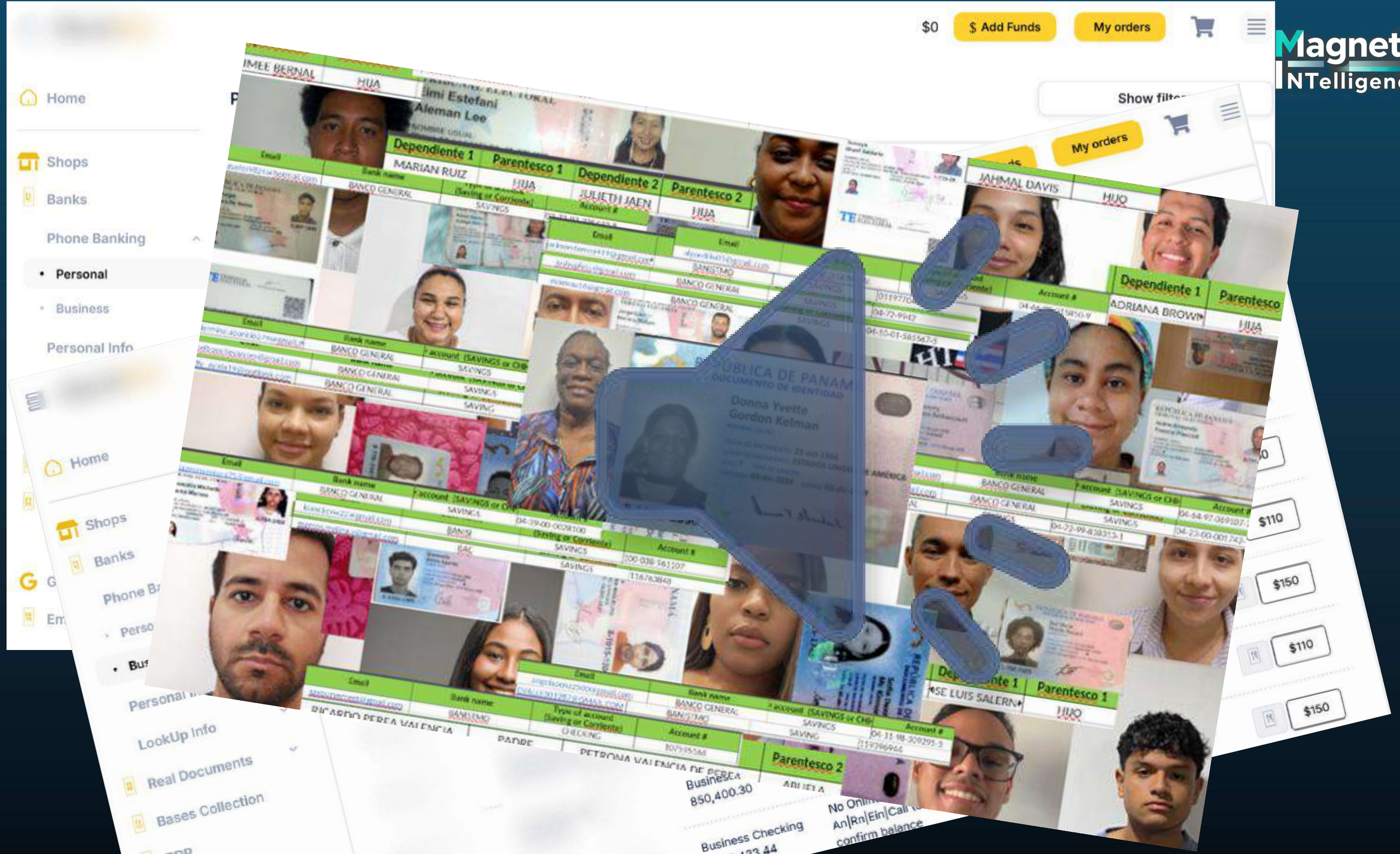
Inteligencia Empresarial

Monitoreo de la reputación de la marca, análisis de la competencia, identificación de oportunidades de mercado y gestión de riesgos.

Investigación Criminal

Investigación de delitos cibernéticos, fraude, lavado de dinero y otras actividades ilícitas.


Magneto
INTelligence


$0
$ Add Funds
My orders
Magneto
INTelligence
Home
Shops
Banks
Phone Banking
Personal
Business
Personal Info
Show filters
Dependiente 1
Parentesco 1
Dependiente 2
Parentesco 2
MARIAN RUIZ
HIJA
JULIETH JAEN
HIJA
JAHMAL DAVIS
HIJO
ADRIANA BROWN
HIJA
Donna Yvette
Gordon Kelman
LookUp Info
Real Documents
Bases Collection
$110
$150
$110
$150
850,400.30
Business Checking

Fuentes

- Redes sociales
- Aplicaciones de mensajería
- Foros de debate
- Listas de spam
- Sitios para compartir código
- Motores de búsqueda
- Feeds de vulnerabilidades
- Feeds de malware
- Canales RSS
- Mercados en línea y Dark Markets
- Tiendas de aplicaciones
- Sitios de ransomware de la Dark Web
- Fugas de credenciales

Servicios asociados

- Ejecución de servicios de DFIR y de seguridad ofensiva
- Integración de API
- Búsqueda activa de amenazas (Hunting)
- Interacción con los actores de las amenazas
- Eliminación de sitios maliciosos o de phishing
- Eliminación de perfiles falsos en redes sociales
- Eliminación de aplicaciones falsas de las tiendas de aplicaciones
- Consultor senior de CTI asignado al cliente
- Elaboración de informes de inteligencia personalizados

AMENAZAS

Actores Estatales y Grupos APT

Operadores del Cibercrimen

Hacktivistas y Activistas

AMENAZAS

Crimen Organizado

Competidores

Amenaza interna

Vectores Amplificadores


Magneto
INTelligence
PRO
REACTIVE

Ciberinteligencia

Comprender antes de que ocurra:

- Quién ataca
- Qué objetivos tiene
- Qué campañas prepara
- Qué sectores están en su radar

La ventaja estratégica

Cuando entiendes la amenaza:

- anticipas ataques
- reduces impacto
- proteges operaciones críticas
- tomas decisiones informadas

CONCLUSIONES

Un Enfoque Integral e Indivisible

Los **5 pilares** — Ciberseguridad, Protección de Datos, Prevención del Fraude, Seguridad Física y Ética Digital — conforman un sistema donde la debilidad en uno compromete a todos.

La diferencia entre reaccionar y anticipar no es técnica, es **estratégica**.

Las organizaciones que sobreviven a grandes crisis son las que vieron venir la amenaza, por eso, la **ciberinteligencia** no es una opción, es una **ventaja** decisiva.

No gana quien reacciona... gana quien ya sabía lo que iba a pasar.

GRACIAS

Carlos Seisdedos

Fundador / CEO Magneto INTelligence

CONTACTO

@CarloSeisdedos
@MagnetoINT

Carlos Seisdedos
Magneto INTelligence