

SERVIÇOS PROFISSIONAIS

CYBERDETETIVE

Investigação digital, inteligência em fontes abertas e análise técnica de evidências.

Informação organizada para esclarecer fatos, documentar ocorrências e apoiar decisões.

Inteligência OSINT

Perícia e computação forense

Relatórios técnicos

01 • APRESENTAÇÃO

Informação organizada para esclarecer fatos e apoiar decisões

O **CyberDetetive** é a frente de investigação digital da Gestão de TI. Utilizamos uma plataforma baseada em **inteligência em fontes abertas (OSINT)**, com **mais de 90 ferramentas** e painel de buscas por dados como CPF, telefone, nome, e-mail, RG e placa, sempre com finalidade legítima e base legal.

O trabalho começa a partir das informações e dos materiais iniciais fornecidos pelo cliente, como prints e documentos, e termina em um relatório técnico com metodologia, fontes, evidências e conclusões.

+90

ferramentas de investigação em fontes abertas

8

frentes de serviço para pessoas, empresas e profissionais

4

etapas do material inicial ao relatório técnico

PARA QUEM ATUAMOS

Empresários e executivos

Due diligence, background check com consentimento, pegada digital e reputação.

Empresas

Fraudes e golpes digitais, fraude interna e vazamentos, com autorização formal.

Escritórios de advocacia

Pesquisa em fontes abertas, preservação de provas e relatórios técnicos.

Vítimas e famílias

Assédio e perseguição digital, golpes e riscos online para crianças e adolescentes.

28 anos

de experiência da Gestão de TI no mercado corporativo

Liderança

Felippe Britto, Head de TI e CISO

Todo o Brasil

remoto em todo o país; presencial em São José dos Campos (SP)

02 • SERVIÇOS

Decisões empresariais com base em fatos verificáveis

Frentes para executivos, empresas e escritórios de advocacia que precisam verificar informações antes de fechar negócios, contratar ou instruir uma ação.

01

Due diligence de empresas e parceiros

Análise de sócios, estrutura societária, processos judiciais públicos, reputação e histórico de inadimplência antes de fechar negócios, contratar fornecedores ou investir.

RECURSOS

OSINT empresarial; investigação de empresas e sócios.

02

Background check com consentimento

Verificação de informações profissionais e públicas de candidatos, parceiros ou locatários, com autorização expressa do avaliado e finalidade definida.

RECURSOS

Busca de pessoas, Google Dorks e análise de redes sociais.

03

Apoio a escritórios de advocacia

Pesquisa em fontes abertas para instruir ações, localizar bens ou partes por meios públicos e organizar provas de forma documentada.

RECURSOS

Fluxo do caso ao relatório final; ferramentas OSINT.

04

Relatórios técnicos de investigação

Entrega padronizada com metodologia, fontes, evidências e conclusões, para uso interno ou jurídico.

RECURSOS

Workflow do caso ao relatório.

FINALIDADE DEFINIDA, CONTRATAÇÃO FORMAL

Todo trabalho parte de uma finalidade legítima e de uma contratação formal. Quando envolve dados de terceiros, exige autorização expressa do avaliado ou da empresa.

03 • SERVIÇOS

Proteção, reputação e resposta a incidentes

Frentes para quem precisa agir rápido diante de golpes, exposição indevida, vazamentos ou perseguição digital, com evidências preservadas e encaminhamento correto.

05

Investigação de fraudes e golpes digitais

Análise de perfis falsos, e-mails, sites, imagens e mensagens fraudulentas para apoiar vítimas, empresas e registros de ocorrência.

RECURSOS

Análise de e-mails e imagens; investigação de WhatsApp, Telegram e redes sociais.

06

Pegada digital e reputação

Mapeamento do que existe publicamente sobre uma pessoa, executivo ou marca, com recomendações para reduzir a exposição.

RECURSOS

Trilhas de investigação e área de ferramentas.

07

Verificação de vazamentos do próprio cliente

Verificação, a pedido e em nome do titular, da presença de e-mails, senhas ou dados em bases vazadas, com orientação sobre medidas de proteção.

RECURSOS

Bases vazadas; anonimato e criptografia.

08

Apoio a vítimas de assédio online

Documentação e preservação de evidências de ameaças e perseguição digital, com encaminhamento às autoridades competentes.

RECURSOS

Investigação em redes sociais e relatórios.

PRESERVAR ANTES QUE SEJA APAGADO

Prints, URLs, áudios e conversas podem desaparecer a qualquer momento. A coleta e a preservação organizada do material que você já possui é o primeiro passo de todo caso.

04 • INVESTIGAÇÃO DIGITAL

Da coleta de vestígios à documentação

A investigação digital reúne atividades de coleta, preservação e análise de vestígios encontrados na internet e em dispositivos eletrônicos, com o objetivo de esclarecer fatos, identificar elementos relacionados a uma conduta e produzir documentação que possa apoiar um processo.

01

Pesquisa em fontes abertas (OSINT)

Busca e cruzamento de informações públicas, como redes sociais, sites, registros de domínio e processos judiciais, para compreender quem pode estar por trás de um perfil, empresa ou golpe.

02

Perícia e computação forense

Coleta e preservação de evidências digitais (conversas, prints, e-mails, arquivos e registros de dispositivos) com técnicas voltadas à integridade da prova e à cadeia de custódia.

03

Relatório técnico

Documento com metodologia, fontes e conclusões, destinado ao cliente, ao advogado ou às autoridades para apoiar medidas legais, boletins de ocorrência ou decisões internas.

FRENTES ESPECIALIZADAS

Perfis falsos e perseguição online

Preservação de provas e pesquisa OSINT em fontes públicas, com dossiê para advogado ou polícia.

Preservação de evidências digitais

Coleta organizada de URLs, prints, áudios e conversas que o cliente já possui, com registro de data, hora e captura completa.

Investigação empresarial e fraude interna

Análise de suspeitas de vazamento, concorrência desleal ou fraude interna, mediante autorização formal e dentro das políticas da empresa.

Fraudes e golpes digitais

Análise de phishing, golpes por WhatsApp e Pix, sites e perfis fraudulentos, com relatório para apoiar o registro de ocorrência.

Questões familiares e segurança de menores

Documentação de condutas digitais direcionadas ao cliente e de riscos online para crianças e adolescentes sob sua guarda.

Dossiê técnico de inteligência

Relatório com metodologia, fontes, evidências e conclusões para apoiar o trabalho jurídico ou eventual investigação oficial.

05 • FLUXO DE INVESTIGAÇÃO

Quatro etapas, do material inicial ao relatório técnico

Um processo organizado e documentado, que preserva a integridade da prova em cada fase.

1

ETAPA 1

Coleta de evidências iniciais

Organizar e preservar materiais fornecidos pelo cliente, como URLs, prints e áudios, antes que conteúdos possam ser apagados.

2

ETAPA 2

Análise de pegadas digitais (OSINT)

Cruzar dados públicos de e-mail, telefone e nome de usuário em fontes abertas e verificáveis.

3

ETAPA 3

Análise técnica dos vestígios

Examinar cabeçalhos de e-mail, metadados de imagens e arquivos, datas e padrões de comportamento, identificando quais provedores poderão ser acionados judicialmente.

4

ETAPA 4

Relatório técnico de inteligência

Entregar um dossiê com os elementos documentados para apoiar o cliente, o advogado e, quando pertinente, as autoridades.

O QUE VOCÊ RECEBE

Metodologia

Como cada achado foi obtido.

Fontes

Públicas e verificáveis.

Evidências

Com registro de data, hora e captura completa.

Conclusões

Para uso interno, jurídico ou junto às autoridades.

06 • GOVERNANÇA E CONFORMIDADE

Atuação dentro da lei, com ética e rigor

Nossa atuação respeita a legislação aplicável, a finalidade legítima de cada consulta e os limites de acesso a dados e dispositivos. Esses compromissos protegem o cliente e a validade das provas.

Proteção de dados

LGPD

Consultas a dados pessoais exigem finalidade legítima e base legal. Informações obtidas em vazamentos não se tornam lícitas apenas por estarem acessíveis.

Contra a perseguição

Art. 147-A do Código Penal

Não realizamos rastreamento ou monitoramento reiterado que ameace a liberdade ou a privacidade, nem aceitamos demandas para localizar ex-parceiros ou pessoas que interromperam contato.

Dispositivos e contas

Art. 154-A do Código Penal

Não acessamos contas, aparelhos ou comunicações sem autorização.

Detetive particular

Lei nº 13.432/2017

Observamos as regras da atividade, incluindo contratação formal e coleta de dados de natureza não criminal.

Sigilo de dados telemáticos

Decisão judicial

A quebra de sigilo depende de decisão judicial. Reunimos elementos para que o advogado possa requerer as providências cabíveis, e não prometemos quebra de sigilo.

Sem rastreamento ativo

Privacidade e validade da prova

Links monitorados para capturar IP ou geolocalização geram riscos de privacidade, LGPD e validade da prova. Essa prática não integra o nosso escopo.

Dados vazados

Fontes verificáveis

Evitamos usar dados de vazamentos para vincular um perfil a uma identidade. Priorizamos fontes públicas e verificáveis.

PRINCÍPIO DE ATUAÇÃO

Trabalhamos com informações e materiais acessados legitimamente, documentamos a metodologia e não prometemos acesso a dados protegidos por sigilo nem a identificação garantida de pessoas por meios não autorizados.

07 • PRÓXIMOS PASSOS

Vamos conversar?

Conte-nos o contexto do seu caso. Avaliamos a finalidade, o escopo e o material disponível e indicamos o caminho mais adequado, com total clareza sobre o que o serviço entrega e o que não entrega.

COMO INICIAR

1

Conversa inicial

Você apresenta o contexto, a finalidade da consulta e os materiais que já possui, como prints, URLs e documentos.

2

Contratação formal

Definição de escopo e finalidade, com autorização expressa do avaliado ou da empresa quando aplicável.

3

Investigação e relatório

Execução em quatro etapas e entrega do relatório técnico com metodologia, fontes, evidências e conclusões.

CONTATO

E-MAIL

contato@gestaodeti.net

TELEFONE E WHATSAPP

(11) 94255-5354

SITE

gestaodeti.net

ATENDIMENTO

Segunda a sexta, das 8h às 18h. Trabalhamos de forma remota para todo o Brasil e oferecemos atendimento presencial para empresas em São José dos Campos (SP).



Este documento tem caráter informativo. Os serviços não incluem quebra de sigilo, rastreamento ativo ou acesso a dados protegidos, e os resultados dependem das informações e das fontes disponíveis em cada caso.