INSIGHT PERICIAL

ADRIANO PENEDO DE ATHAYDE VALLIM

Perito Forense, com 30 anos de carreira em tecnologia e 25 anos de atuação pericial, uma trajetória singular construída na intersecção entre tecnologia, direito e administração. Perito especialista em crimes digitais, com atuação nas áreas da forense computacional (tecnologia), grafotécnica e documentoscopia (análise de assinaturas e documentos físicos e digitais) e fonética forense (identificação de falantes), acumula uma combinação de credenciais técnicas, acadêmicas e institucionais que o posiciona como uma das referências mais completas da área no Brasil.

▶ PERÍCIA

Insider Threat: como a perícia prova o vazamento que veio de dentro

Quando o vazamento nasce dentro de casa, a prova técnica é o que separa a suspeita da demonstração.

O comunicado chega ao jurídico quase sempre com a mesma frase: os dados vazaram, é preciso descobrir quem invadiu. Em parte relevante dos casos, ninguém invadiu. A informação saiu pela porta da frente, com crachá, login válido e senha própria. O relatório Cost of Insider Risks, do Ponemon Institute, estimou em 2025 um custo médio anual de US$ 17,4 milhões por organização para gerenciar incidentes de origem interna. O Data Breach Investigations Report, da Verizon, aponta que cerca de 60% das violações de dados envolvem o elemento humano. Os números confirmam o que a prática pericial observa há anos: o insider não é exceção, é hipótese obrigatória. Toda investigação séria de vazamento precisa testar, com método, a possibilidade de a origem estar dentro de casa antes de apontar para fora.

O direito já mapeou as consequências: LGPD, justa causa, responsabilidade civil, comunicação à autoridade. Todas dependem de um fato demonstrado. E o fato, em ambiente digital, se demonstra por vestígios. É nesse ponto que o trabalho jurídico encontra o trabalho técnico.

Os rastros que o colaborador deixa

Todo acesso deixa registro. Logs de autenticação mostram quem entrou, quando, de qual máquina e por qual rede. Trilhas de auditoria dos sistemas de gestão registram consultas, exportações e relatórios gerados. O sistema operacional da estação de trabalho guarda artefatos de cada dispositivo USB conectado: modelo, número de série, data e hora da conexão, além de vestígios dos arquivos manipulados. Servidores de e-mail registram encaminhamentos para contas pessoais; registros de rede documentam uploads para serviços de nuvem; servidores de impressão guardam o histórico do que foi enviado para o papel.

Há um limite que a honestidade pericial exige declarar: a fotografia da tela feita com o celular pessoal não gera registro no ambiente corporativo. Nesses casos, o exame se desloca do ato de captura para o comportamento ao redor dele. Consultas em volume atípico, acessos a registros sem relação com a função, sessões em horários incomuns e navegação sequencial por cadastros formam, correlacionados no tempo, o indício que a captura isolada tentou esconder.

Como o rastro vira prova

O rastro só se converte em prova quando é preservado com método, e a preservação precisa acontecer antes de qualquer confronto com o suspeito. O procedimento começa pela imagem forense da estação de trabalho e pela cópia dos logs relevantes, ambas autenticadas por código hash que comprova a integridade. Sobre o material preservado, o exame reconstrói a linha do tempo: o que foi acessado, exportado, conectado, enviado e apagado, evento a evento. A força do resultado está na correlação de fontes independentes: quando o log do sistema, o artefato da estação e o registro de rede apontam para o mesmo evento, a conclusão resiste ao contraditório.

> **"A prova do vazamento interno nasce nos primeiros minutos da suspeita. O que a empresa faz antes do confronto define o que ela consegue demonstrar depois."**

A prova pelos erros idênticos

Uma técnica recorrente em casos de concorrência desleal merece destaque. Toda base de clientes carrega imperfeições: um sobrenome digitado errado, um endereço desatualizado, um dígito trocado. Quando a base vazada reaparece no concorrente, quem a recebeu raramente refaz o trabalho, e os mesmos erros reaparecem, nas mesmas posições. A coincidência de erros idênticos entre a base de origem e a base encontrada no destino demonstra o reaproveitamento com altíssimo grau de segurança técnica. Empresas maduras vão além e inserem sementes deliberadas: registros fictícios criados para rastrear cópias. Se o cliente que não existe recebe uma proposta do concorrente, a rota do vazamento está exposta.

O método de captação do insider também evoluiu. Casos recentes de grande repercussão no mercado de aplicativos de entrega expuseram o esquema das falsas pesquisas remuneradas: consultorias abordam gerentes e diretores por redes profissionais oferecendo pagamento por entrevistas sobre o mercado, sem perguntar nada sobre a empresa. Os valores crescem a cada rodada, as perguntas se tornam específicas e, quando o entrevistado resiste, há registros de ameaça de envio das gravações ao empregador. O que parecia consultoria era coleta estruturada de segredo de negócio, com casos que evoluíram para extorsão.

O erro clássico: a TI investiga primeiro

O roteiro se repete nas empresas. Surge a suspeita, a equipe de TI liga o computador do colaborador, abre os arquivos, imprime e-mails e monta um dossiê. O gesto parece diligente e destrói o caso. Cada arquivo aberto altera metadados; cada login na máquina sobrescreve vestígios; a cópia sem hash não comprova integridade. No contraditório, a defesa não precisa provar inocência: basta demonstrar que a evidência foi manuseada sem cadeia de custódia. O resultado conhecido é a justa causa revertida na Justiça do Trabalho, com verbas rescisórias e eventual indenização, em um caso cujo fato de fundo era verdadeiro.

Os primeiros minutos da suspeita

A conduta do RH e do jurídico nos primeiros minutos vale mais que meses de investigação posterior:

- Não confrontar o suspeito nem alterar sua rotina antes da preservação das evidências;
- Impedir o uso da estação de trabalho envolvida; se estiver desligada, mantê-la desligada;
- Suspender rotinas de expurgo automático de logs e backups do período sob análise;
- Registrar por escrito quem soube da suspeita, quando e por qual meio;
- Acionar o jurídico e um perito forense antes de qualquer medida técnica interna.

Prevenção e o papel do laudo

A prevenção é menos tecnológica do que parece. Monitoramento legítimo, previsto em política interna e comunicado com clareza ao colaborador, sustenta a validade da prova e desestimula o desvio. Avisos explícitos de que o ambiente corporativo é auditável eliminam a zona cinzenta que o insider explora. E a cultura pesa: a equipe que entende o valor da informação e conhece as consequências do vazamento é a primeira camada de defesa.

Quando a prevenção falha, o desfecho depende do laudo. O laudo pericial documenta o método, comprova a cadeia de custódia, declara as limitações do exame e apresenta conclusões reproduzíveis por outro perito. É esse documento que sustenta a justa causa na Justiça do Trabalho, fundamenta a ação cível de reparação e instrui a notícia-crime quando a conduta configura ilícito penal. O vazamento interno se resolve com fatos demonstrados. E fato, em ambiente digital, é vestígio preservado a tempo.

A PROVA DO VAZAMENTO INTERNO NASCE NOS PRIMEIROS MINUTOS DA SUSPEITA. O QUE A EMPRESA FAZ ANTES DO CONFRONTO DEFINE O QUE ELA CONSEGUE DEMONSTRAR DEPOIS

© 2026 VALLIM Perícias · Reprodução autorizada com crédito ao autor