NÃO CONSEGUIMOS IDENTIFICAR O INCIDENTE PORQUE FOI CREDENCIAL PRIVILEGIADA

QUANDO UMA CREDENCIAL VÁLIDA VIRA UMA DESCULPA PARA EXPLICAR UM INCIDENTE

Existe uma frase que deveria acender um alerta imediato em qualquer investigação de incidente de segurança envolvendo dados pessoais:

“Não conseguimos identificar o incidente porque o acesso foi realizado com uma credencial privilegiada. ”

Uma credencial privilegiada explica como o acesso ocorreu. Ela não explica, por si só, quem utilizou a credencial, de onde ocorreu o acesso, quando ocorreu, quais sistemas foram acessados, quais operações foram realizadas, quais recursos foram consultados, quais alterações foram efetuadas e por que os mecanismos de monitoramento não detectaram a atividade.

E existe uma diferença fundamental entre essas duas coisas. Uma credencial válida pode dificultar a atribuição da identidade humana por trás do acesso. Isso não significa que a atividade seja necessariamente invisível, não registrada ou impossível de investigar

Se o serviço foi contratado justamente para monitorar e detectar eventos de segurança, a pergunta correta é: *“Quais eventos relacionados à utilização dessa credencial foram efetivamente registrados, coletados, correlacionados, alertados e analisados durante o período do incidente? ”*

Durante o tratamento de incidentes de segurança tenho ouvido regularmente a respostas de alguns Operadores: “*Não Conseguimos Identificar o Incidente Porque foi Credencial Privilegiada. ”*

Se você é Controlador ou Operador de dados pessoais e já ouviu de um fornecedor de segurança, SOC ou SIEM uma frase parecida com esta *"não conseguimos identificar a ação porque foi usada uma credencial privilegiada"* este artigo é para você. Essa justificativa, quando apresentada sem evidências técnicas que demonstrem a efetiva impossibilidade de rastreamento, é insuficiente para encerrar uma investigação de incidente.”. E o problema não fica só com o fornecedor: ele se espalha, por força de lei, para toda a cadeia de tratamento de dados.

A LGPD não reconhece "terceirização de responsabilidade", o artigo 42 da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) estabelece que o Controlador e o Operador respondem pelos danos causados em razão do tratamento de dados pessoais que viole a legislação. O artigo 43 admite exceções à responsabilização apenas em hipóteses restritas quando o agente prova que não realizou o tratamento que lhe é atribuído, que não houve violação à legislação, ou que o dano decorreu exclusivamente de culpa da vítima ou de terceiro.

Fora dessas hipóteses, a regra é a *responsabilidade solidária***:** se o Operador falha em proteger, monitorar ou rastrear os dados sob sua guarda, o Controlador não se livra da responsabilidade simplesmente por ter contratado um terceiro para isso. Contratar um SOC, um SIEM ou qualquer serviço de segurança gerenciada é uma decisão de governança não é uma transferência de risco jurídico.

Isso significa, na prática, que a frase *"a culpa foi do Controlador ou Operador, que não conseguiu identificar o incidente"* não é uma defesa válida perante a ANPD, perante os titulares de dados ou

perante o Judiciário. O Controlador continua exposto, e o Operador que prestou o serviço de monitoramento também.

Primeiro vamos acabar com essa de *credencial pode tudo*: Credencial privilegiada" não é sinônimo de "invisível nos logs"

O argumento técnico por trás da desculpa também não se sustenta. Um SIEM adequadamente configurado pode coletar e correlacionar eventos de autenticação, origem, horário, ativo, alterações de privilégios e outras atividades registradas pelas fontes integradas ao ambiente. A profundidade da rastreabilidade dependerá da capacidade de auditoria de cada sistema, da integração das fontes e das configurações de logging existentes. Uma conta administrativa possui privilégios elevados. Isso significa que ela pode realizar operações que uma conta comum não poderia realizar.

Não significa que ela seja uma conta sem rastreabilidade.

Quando um fornecedor afirma que não consegue identificar uma ação só porque a credencial era privilegiada, isso revela uma:

- As fontes de log daquele ativo não estavam integradas ao SIEM;
- O log deixa de existir?;
- Não há necessidade de monitoramento?
- A granularidade de auditoria daquele sistema estava desabilitada.

Nenhuma pergunta é uma "limitação natural" da tecnologia. São falhas de configuração do serviço contratado e *falhas de configuração de um serviço de segurança são, elas mesmas, um possível incidente de tratamento inadequado, já que comprometem a capacidade de detectar e responder a violações de dados pessoais.*

Vale repetir: O acesso ter sido realizado com credencial privilegiada não significa que o acesso não poderia ter sido detectado ou auditado. Credencial legítima explica a *forma* de acesso; não explica, por si só, a ausência de rastreabilidade, monitoramento ou detecção da atividade realizada com essa credencial.

Uma credencial válida pode ser utilizada de forma indevida após seu comprometimento, e essa utilização indevida costuma gerar eventos de segurança perfeitamente registráveis: autenticações fora de padrão, acessos atípicos, movimentação lateral, alterações de privilégio, acesso a recursos sensíveis. Tudo isso é matéria-prima para correlação e alerta se o serviço estiver de fato operando como contratado ou como é sempre vendido.

Quem se sustenta na isenção do incidente em contas privilegiadas deveria pensar justamente o contrario: *contas privilegiadas pedem MAIS monitoramento, não o contrário*

A norma ISO/IEC 27001, trata especificamente da gestão de acesso privilegiado e exige que a organização identifique, documente e controle rigidamente todos os direitos de acesso privilegiado, junto com os papéis e responsabilidades associados.

Ou seja: contas admin/superuser são reconhecidas pelo próprio mercado de segurança como as de *maior risco* e por isso deveriam ter monitoramento *reforçado*, não reduzido. Isso inclui, entre outras práticas:

- Gravação de sessão;
- MFA obrigatório;
- Log de comandos executados;
- Alertas de uso anômalo em tempo real.

Se um fornecedor certificado ISO 27001 não tem essas capacidades para as contas mais críticas do ambiente, isso não é uma "limitação intransponível da tecnologia" é um erro de controle que contradiz a própria certificação apresentada como garantia de qualidade. Vale a pergunta direta ao fornecedor: *como a certificação de vocês trata o controle de acesso? Existe log de sessão privilegiada? Como isso foi validado pela certificadora?*

Por esse motivo tenho entrado em atrito com muitos fornecedores ao aplicar a *Due Diligence*, quando digo que Certificação e contrato não são prova de que o monitoramento funcionou são somente documentos, diferente de evidência.

Um ponto que costumam esquecer: a certificação ISO 27001 de um fornecedor, ou a simples existência de um contrato de SOC/SIEM, não prova que uma atividade específica foi de fato monitorada ou que um alerta correspondente foi gerado no momento do incidente.

Certificação atesta processo. Contrato atesta escopo contratado. Nenhum dos dois, isoladamente, atesta execução efetiva no momento em que mais importava. Por isso, diante de um incidente, a pergunta certa não é "vocês têm SIEM?" é:

- Quais registros foram efetivamente coletados e analisados durante o período do incidente?
- Quais regras e correlações estavam configuradas para credenciais privilegiadas?
- Quais alertas foram gerados?
- Quais ações foram tomadas pelo serviço de monitoramento diante desses alertas?

A ausência de resposta objetiva a essas perguntas não fortalece a defesa do fornecedor, fragiliza.

É nesse memento que aparece o ponto que diferencia *compliance documental de efetividade de controle.*

Como auditor em LGPD e resposta de incidente sempre defendo:

Checklist prático que muitos vão descobrir a importância quando o incidente acontecer e os agentes de tratamento sumirem ou tentarem se eximir de responsabilidades.

Durante a investigação de um incidente

1. Peça log de autenticação, IP de origem, timestamp e comandos executados mesmo que a granularidade da ação em si seja limitada, o evento de logon já ajuda a delimitar a janela temporal do incidente.
2. Solicite a política de Gestão de Acesso Privilegiado (PAM) do fornecedor e evidências de revisão periódica dessas contas.
3. Exija evidências operacionais do período do incidente: registros, alertas, correlações e eventos de autenticação não apenas a alegação de que "o sistema não registrou".

4. Trate qualquer lacuna de integração de logs ao SIEM como falha do prestador, e não como limitação técnica inerente ao uso de credenciais privilegiadas.

Ao contratar (ou renovar) serviços de SIEM/SOC

- Escopo de logging obrigatório**:** contas privilegiadas devem gerar logs de autenticação, autorização e execução de comandos idealmente com gravação de sessão (PAM).
- Retenção mínima de logs compatível com o tempo real de detecção de incidentes hoje praticado no mercado, tipicamente medido em meses, não em poucas semanas.
- Correlação de eventos privilegiados**:** alertas específicos para uso de contas admin fora do padrão (horário, localização, volume).
- Cláusula de responsabilização por gaps de monitoramento: se uma fonte de log não estava integrada ao SIEM no momento do incidente, isso deve ser expressamente tratado como falha do prestador, com consequência contratual definida.
- Auditoria periódica independente do escopo real de cobertura do SIEM quais ativos e contas estão de fato sendo monitorados, e não apenas o que consta na proposta comercial.

A pior situação é descobrir a limitação somente depois do incidente

Existe uma pergunta que deveria ser feita antes da contratação: “Se ocorrer um incidente amanhã, quais evidências vocês conseguirão me entregar?

Se a resposta só aparece depois do incidente, talvez o problema não seja apenas o ataque, pode existir um problema de governança, arquitetura, contratação, configuração ou gestão de riscos anterior ao ataque

Quando seu fornecedor diz *“O hacker utilizou uma credencial válida. ”,* isso é apenas uma parte da história. Nesse momento uma investigação deixa de ser uma explicação do ataque e passa a ser uma verdadeira análise de segurança e conformidade.

A ANPD orienta que os agentes adotem medidas para prevenir danos aos titulares e que o controlador avalie o incidente considerando, entre outros aspectos, a natureza, categoria e quantidade de dados e titulares afetados e as consequências concretas e prováveis. A Autoridade também orienta que, havendo dúvida sobre a relevância dos riscos e danos, o controlador adote uma postura cautelosa.

Além disso, a Resolução CD/ANPD nº 15/2024 regulamenta a comunicação de incidentes de segurança, atualmente vigente.

A própria ANPD informa que, diante de incidente não comunicado que possa acarretar risco ou dano relevante, pode instaurar procedimento de apuração, requisitar informações ao controlador e, constatada a ocorrência, determinar a comunicação à Autoridade e aos titulares, além de poder instaurar processo administrativo sancionador nas hipóteses previstas no regulamento.

Portanto, uma investigação incompleta não deveria ser tratada como justificativa automática para concluir que não houve incidente ou que não houve impacto.

A falta de informação é, em si, uma situação que precisa ser administrada, documentada e tecnicamente explicada.

Existe uma diferença fundamental entre: **"***Não conseguimos identificar" e "Com as evidências disponíveis, não foi possível determinar X, porque Y; os seguintes registros foram analisados; os seguintes controles estavam ativos; os seguintes controles não estavam disponíveis; e essas são as limitações técnicas que impedem uma conclusão mais precisa.* **"** Essa é uma conclusão técnica, já a primeira é apenas uma afirmação.

Em incidentes envolvendo dados pessoais, especialmente aqueles que envolvem operadores, fornecedores de tecnologia, SOC, SIEM, infraestrutura ou contas privilegiadas, conclusões precisam ser sustentadas por evidência

Controlador e Operador formam, para efeitos da LGPD, uma cadeia solidária de responsabilidade sobre o tratamento de dados pessoais. Delegar a execução técnica do monitoramento a um terceiro é uma escolha operacional legítima e, muitas vezes, necessária. Mas essa delegação não transfere a responsabilidade legal ela apenas adiciona mais um agente de tratamento à cadeia que pode ser chamado a responder.

Por isso, diante de qualquer justificativa que soe como "não é possível saber o que aconteceu", o caminho correto não é aceitar a explicação e arquivar o caso. É perguntar, documentar e exigir evidências porque, ao final, é o Controlador (e, junto com ele, o Operador) quem vai precisar demonstrar, para a ANPD e para os titulares de dados, que fez tudo o que era razoavelmente possível para prevenir, detectar e responder ao incidente.

O "O acesso foi realizado com uma credencial privilegiada" não é uma resposta suficiente para encerrar uma investigação de incidente. Temos perguntas a responder mesmo que a credencial seja legítima, o acesso autenticado corretamente e a conta possuído privilégios elevados. Nada disso, permite concluir que a atividade realizada era legítima, que não poderia ser monitorada ou que não existiam mecanismos de rastreabilidade.

Da mesma forma, a existência de SIEM, SOC, EDR, ISO 27001 ou qualquer outra tecnologia ou certificação não significa, por si só, que determinado evento foi efetivamente monitorado ou detectado. É preciso provar.

Uma lição que aprendi tratando e auditando incidente de Agentes de Tratamento junto a ANPD:

Controlador: Não terceirize a tecnologia. Terceirize o serviço, mas mantenha a governança.

Operador: Ao receber uma credencial privilegiada para executar uma atividade não elimina suas obrigações de segurança, rastreabilidade e cooperação.

Um incidente com dados pessoais não é o momento para descobrir quais controles deveriam ter existido

A LGPD estabelece responsabilidades aos agentes de tratamento, e a responsabilidade solidária do operador pode ocorrer nas hipóteses expressamente previstas no art. 42, §1º, I., portanto, nenhum agente deve presumir que poderá simplesmente afastar sua responsabilidade apontando para a credencial utilizada, para o outro agente ou para uma limitação técnica não demonstrada.

Não adianta você dizer documentar ou simplesmente acreditar que responder a Agência Nacional de Proteção de Dados “A credencial era privilegiada? ”. O que se espera em uma resposta de incidente é: “Quais controles deveriam ter permitido prevenir, detectar, registrar, investigar e responder a esse uso indevido e quais evidências demonstram que esses controles estavam efetivamente funcionando quando o incidente ocorreu

Credencial privilegiada explica como o acesso ocorreu. Ela nunca explica, sozinha, por que ninguém percebeu

ALERTA

Muitos agentes de tratamento repetem publicamente que "seguem a LGPD", mas na prática seguem apenas o contrato. Tratam dados pessoais amparados em cláusulas e documentos internos, e esquecem que nenhum instrumento contratual se sobrepõe à lei. Operador nenhum se torna isento de responsabilidade porque assinou um contrato ou porque seu instrumento jurídico diz que "não responde" pelo incidente a LGPD não reconhece essa isenção.

A simples impossibilidade de o titular acessar seus próprios dados já configura, por si só, um incidente. E quem comunica o incidente à ANPD é o Controlador não importa quantas cláusulas o Operador tenha redigido tentando transferir essa obrigação.

Há também um padrão recorrente: agentes afirmam cumprir a LGPD, mas não têm o Encarregado (DPO) formalmente nomeado, com procuração e documentação que comprovem essa nomeação. Só percebem essa ausência quando o incidente já ocorreu e descobrem, tarde demais, que sem essa formalização abrir o processo de comunicação junto à ANPD já é uma dificuldade. .

Quando conseguem abrir o processo e precisam anexar depois os documentos de nomeação e procuração do Encarregado, essa própria conduta já revela que a organização não estava adequada à lei no momento do incidente e essa lacuna, sozinha, se transforma em prova contra o agente de tratamento. Se houvesse Encarregado formalmente nomeado desde o início, esses documentos não precisariam ser incluídos depois: seria o próprio Encarregado quem, desde o primeiro mom

Wendel Babilon
babilon@wendelbabilon.com.br
Escritor, Auditor e Consultor Especializado em
Privacidade e Proteção de Dados