



**MELHORES PRÁTICAS PARA
A PRESERVAÇÃO DE PROVAS DIGITAIS
NO RELACIONAMENTO
ENTRE A INSTITUIÇÃO FINANCEIRA
E A SOCIEDADE DIGITAL**



Presidente

Hilgo Gonçalves

Diretor Superintendente

Antonio Augusto de Almeida Leite (Pancho)

Coordenador das Comissões

Carlos Alberto Marcondes Machado

Consultora Jurídica

Dra. Cintia M. Ramos Falcão

Direção de Arte

Rogério Callamari Macadura
(Purim Comunicação Visual)

Elaboração

Junho/2017

Impressão

DuoGraf



Autoria:

Victor Auilo Haikal

Coordenação:

Patricia Peck Pinheiro

Créditos:



PATRICIA PECK PINHEIRO
Advogados Especialistas em Direito Digital

Este Guia foi elaborado com base na legislação brasileira e regulações institucionais em vigor até 12 de outubro de 2016.





ÍNDICE

- 7** Apresentação
- 8** Introdução
- 9** **CAPÍTULO I - Conceito de prova e sua utilidade à instituição financeira na sociedade digital**
- 14** **CAPÍTULO II - Provas digitais – Principais características e cuidados**
- 20** **CAPÍTULO III - Confiabilidade das provas digitais**
- 27** **CAPÍTULO IV - Condições para formação de provas lícitas**
- 33** **CAPÍTULO V - O ônus da prova e suas hipóteses de inversão**
- 37** **CAPÍTULO VI - Produção de documentos nos sistemas de informação da instituição financeira**
- 45** **CAPÍTULO VII - Preservação e uso das provas digitais dos sistemas de informação da instituição financeira – compliance da atividade em meio digital**
- 50** **CAPÍTULO VIII - Guarda e preservação das provas digitais de sistemas de informação de terceiros**
- 56** **CAPÍTULO IX - A forma de apresentação da prova digital**
- 62** **CAPÍTULO X - Check-list para produção de provas seguindo as regras de compliance em vigor**
- 65** **CAPÍTULO XI - Check-list para coleta e uso de provas de acordo com a situação prática enfrentada pela instituição financeira**
- 70** Referências Bibliográficas





APRESENTAÇÃO

A velocidade com que a era digital passou a fazer parte de nossas vidas exige cada vez mais atenção às mudanças que as inovações tecnológicas trazem ao cotidiano. Essa é uma realidade que abrange todos os segmentos e que impacta diretamente também todos nós que trabalhamos no mercado financeiro.

Com o crescimento em velocidade espantosa da utilização de sistemas de informação nas transações, é preciso atenção redobrada para ter um nível de segurança que reduza os riscos operacionais nas operações financeiras, sem esquecer de dar praticidade aos clientes. É pensando nessa realidade que a ACREFI apresenta este Guia, que é uma ferramenta de suporte ao ecossistema de crédito nesse intrincado e por muitas vezes pouco conhecido mundo digital.

O Guia centra-se na orientação, de forma didática e de fácil compreensão, para a formação e a apresenta-

ção adequada de provas nos processos judiciais em que as instituições financeiras estiverem envolvidas em transações que envolvam o mundo digital. São recomendações abrangentes que incluem, entre outros pontos, características, formação, uso e ônus das provas. E ao final o Guia inclui dois check-lists: um para produção das provas dentro das regras de compliance e outra para coleta e uso de acordo com situações práticas.

Trata-se, enfim, de mais uma iniciativa da ACREFI para colaborar com o aprimoramento do setor, ainda mais quando se trata do mundo virtual. Esperamos que esse Guia seja mais uma ferramenta importante no processo de constante aperfeiçoamento do nosso setor, que tem papel fundamental a cumprir no crescimento sustentável da economia brasileira.

Boa leitura!

Hilgo Gonçalves
Presidente da ACREFI

INTRODUÇÃO

O uso de dispositivos digitais para contratação e relacionamento é realidade inseparável da sociedade digital, cada vez mais fazendo parte do cotidiano de todos, afetando a forma de realização de operações bancárias e financeiras, inclusive.

Tal cenário implica em cuidados técnicos e jurídicos adicionais às Instituições Financeiras durante a disponibilização de sistemas de informação para que seus clientes executem as mais diversas operações de modo prático, em mobilidade e com segurança.

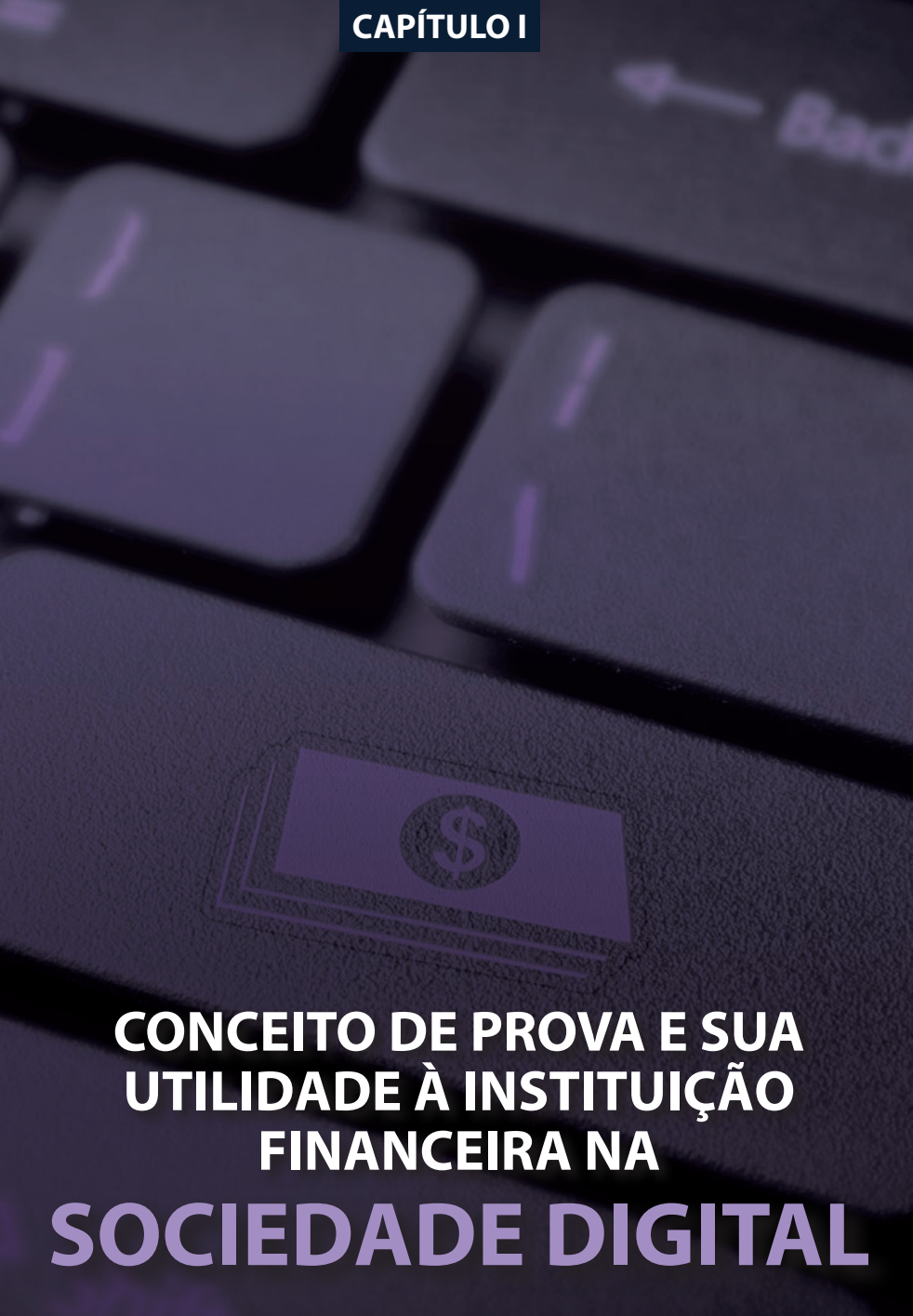
Além disso, as Instituições Financeiras devem se cercar de controles de segurança e rotinas para mitigar seus riscos operacionais e reunir recursos para melhor defender seus interesses caso haja algum incidente ou prejuízo envolvendo as atividades de seus clientes que forem praticadas por meio digital.

Dentre esses controles e rotinas destacaremos a formação adequada de provas e a maneira adequada de apresentá-las nos processos judiciais ou administrativos que a Instituição Financeira vier a enfrentar, de modo

a transmitir a confiabilidade dos sistemas de informação que utiliza e se resguardar com documentos adequados a comprovar a veracidade e autenticidade da prova produzida.

Para chegar em tais recomendações, este Guia explorará diversos conteúdos de gestão documental digital e de segurança da informação indispensáveis para o tratamento seguro de dados e informações, com o resgate de conceitos fundamentais do Direito Processual além da análise legal dos textos em vigor que estão relacionados ao tema, sobretudo de origem regulatória.

Depois de apresentadas as recomendações e fundamentos técnicos e legais, indicaremos dois *check-lists* práticos: um destinado a garantir à Instituição Financeira que produza documentos de acordo com o exigido em lei que servirão como provas; e outro de como proceder em situações em que há prejuízos sofridos pela Instituição em virtude do relacionamento digital que possui com clientes e sua visibilidade nas diversas redes de informação existentes.



**CONCEITO DE PROVA E SUA
UTILIDADE À INSTITUIÇÃO
FINANCEIRA NA
SOCIEDADE DIGITAL**

A expressão *provar* contém diversos significados possíveis pela aplicação prática e social que possui.

Dentre eles, destacamos:

1-) A ideia de se demonstrar algo que tem como fim a obtenção da verdade sobre:

- Fatos; ou
- Afirmações ou negações.

Ex.: Provar que houve um imprevisto no trânsito, que a pessoa realmente comprou a peça de roupa que se pretende a troca dentro do prazo, que o e-mail foi enviado ‘sem querer’, ou ainda que determinada teoria está errada.

2-) A ideia de experimentar algo:

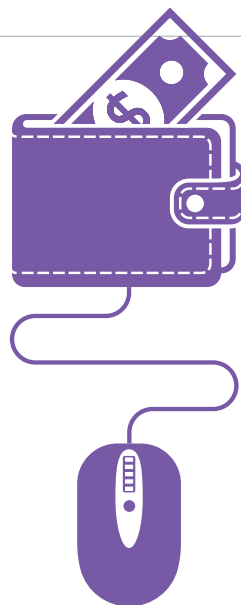
- Para descobrir novos efeitos ou sensações; ou
- Como possível demonstração.

Ex.: Provar uma receita nova de bolo ou a utilização de novo aplicativo como método mais exato para medir velocidade de conexão à internet.

Diante destes possíveis significados da palavra ‘provar’, utilizaremos a aplicação da primeira ideia ao longo deste Guia, pelo peso jurídico na combinação de dois postulados históricos do Direito que dizem respeito aos fatos:

“Contra fatos não há argumentos.”

“Dos fatos decorre o Direito.”



Com base nessas duas expressões, é possível dizer que as provas possuem extrema relevância na harmonização jurídica de situações que possam causar prejuízos à instituição financeira das mais diversas maneiras, pois **a demonstração da ocorrência, ou não, de certos fatos pode afastar ou reduzir os prejuízos que vier a sofrer conforme a circunstância.**

Tais prejuízos decorrem do cotidiano da instituição financeira, podendo ser causados por:

- Falhas internas da instituição;
- Eventos externos;
- Descumprimentos de contrato;
- Condenações judiciais;
- Sanções administrativas.

Como decorrência imediata da possibilidade de prejuízos acima indicada, esta condição foi fixada como **risco operacional** pela Resolução nº 3.380 de 2006 do Banco Central do Brasil:

*“Art. 2º Para os efeitos desta Resolução, define-se como **risco operacional a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos.***

*§ 1º A definição de que trata o caput inclui **o risco legal associado à inadequação ou deficiência em contratos firmados pela instituição, bem como a sanções em razão de descumprimento de dispositivos legais e a indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição.**”*

Por mais que haja dedicação, cuidado, atenção e zelo pela instituição financeira e seus colaboradores é impossível evitar, afastar ou repelir todos os possíveis incidentes que decorrem dos mais diversos riscos e, por conseguinte, seus prejuízos.

Tais prejuízos podem ter de ser indenizados ou ressarcidos pela Instituição Financeira conforme o caso, em virtude do instituto da responsabilidade civil aplicada ao próprio descumprimento do contrato da Instituição Financeira com seus clientes ou do contato social que houver dentre as demais pessoas no contexto de

interconexões da sociedade digital.

Isso ocorre porque a legislação fixou a obrigação de aquele que deu causa ao prejuízo deve indenizar a vítima, assim descrita pelo artigo 927 do Código Civil como regra geral, ou ainda pelo risco da atividade executada, independentemente de intenção ou culpa:

*“Art. 927. **Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.***

*Parágrafo único. **Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.**”*

Quando existe contrato entre os envolvidos, o Código Civil fixou as disposições de responsabilidade do descumprimento do contrato no artigo 389:

*“Art. 389. **Não cumprida a obrigação, responde o devedor por perdas e danos, mais juros e atualização monetária segundo índices oficiais regularmente estabelecidos, e honorários de advogado.**”*

Se existir relação de consumo entre as partes, o descumprimento contratual é descrito e pelo artigo 20 do Código de Defesa do Consumidor, em que apresenta possíveis medidas a remediar o cenário de inadimplemento ou de falta de adequação do que é fornecido em relação às normas vigentes que devem ser cumpridas:

*“Art. 20. **O fornecedor de serviços responde pelos vícios de qualidade que os tornem impróprios ao consumo ou lhes diminuam o valor, assim como por aqueles decorrentes da disparidade com as indicações constantes da oferta ou mensagem publicitária, podendo o consumidor exigir, alternativamente e à sua escolha:***

I - a reexecução dos serviços, sem custo adicional e quando cabível;

II - a restituição imediata da quantia paga, monetariamente atualizada, sem prejuízo de eventuais perdas e danos;

III - o abatimento proporcional do preço.

§ 1º A reexecução dos serviços poderá ser confiada a terceiros devidamente capacitados, por conta e risco do fornecedor.

*§ 2º **São impróprios os serviços que se mostrem inadequados para os fins que razoavelmente deles se esperam, bem como aqueles que não atendam as normas regulamentares de prestabilidade.”***

Adicionalmente, o Código de Defesa do Consumidor prevê a responsabilidade que independe de culpa (objetiva) em caso de danos provocados pelo conjunto de atividades que resultam no oferecimento do serviço bancário ou financeiro à sociedade, podendo atingir seus clientes ou quaisquer terceiros, de acordo com seus artigos 14 e 17:

*“Art. 14. **O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.***

*§ 1º **O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:***

I - o modo de seu fornecimento:

II - o resultado e os riscos que razoavelmente dele se esperam:

III - a época em que foi fornecido.”

“Art. 17. Para os efeitos desta Seção, equiparam-se aos consumidores todas as vítimas do evento.”

Como fator adicional para responsabilização da Instituição Financeira nos casos de danos sofridos por seus clientes, independentemente da origem, temos o conteúdo Sumular nº 479 do Superior Tribunal de Justiça, que indica:

“As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.”

No entanto, é possível combater a responsabilização da Instituição Financeira demonstrando que não deve suportar a carga da indenização

quando não existir defeito no serviço ou houver culpa exclusiva do consumidor para ter experimentado os prejuízos, pelo §3º e seus incisos do artigo 14 do próprio Código de Defesa do Consumidor:

“Art. 14. (...)

§ 3º O fornecedor de serviços só não será responsabilizado quando provar:

I - que, tendo prestado o serviço, o defeito inexiste;

II - a culpa exclusiva do consumidor ou de terceiro.”

Para tanto, é indispensável que a Instituição Financeira possua recursos documentais e probatórios suficientes para ter respaldo em tais argumentações e em outras que buscam defender direitos legítimos que possui.

Portanto, as provas são demonstrações de fatos, afirmações ou negações que tem como utilidade dar apoio à defesa dos interesses da instituição financeira caso ocorra alguma perda financeira.

March

April

July

Aug

Sept

PROVAS DIGITAIS

PRINCIPAIS CARACTERÍSTICAS E CUIDADOS

Feb

Sept

Recuperando a ideia de que a prova é demonstração da verdade sobre determinado fato, afirmação ou negação, temos que é possível transmitir tal apresentação ao juiz do processo ou a quem avaliará determinada situação jurídica por meio de prova oral ou escrita.

De tal sorte, cuidaremos de orientar a utilização da prova digital fundada em documentos digitais, isto é, aqueles que serão criados, processados, armazenados, acessados e excluídos por sistemas de informação, assim chamadas as soluções tecnológicas que dependam de um dispositivo digital para rodar.

Ex.: Computador, telefone celular, tablets, notebooks, terminal de auto atendimento (ATM), etc.

Vale dizer que a legislação brasileira já admite amplamente as mídias digitais para produção de documentos eletrônicos, seguindo o previsto pelo artigo 225 do Código Civil:

“Art. 225. As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão.”

Dentre as características das provas digitais, é possível destacar as mais relevantes para a produção, guarda e uso destas:

- Possuem ordem de volatilidade (OVV), isto é, dependendo do meio onde os dados são processados, armazenados e acessados, as chances de terem a disponibilidade e integridade preservadas podem diminuir drasticamente pela continuidade do uso de tal meio.

Ex.: Memória RAM >>> Disco Rígido >>> DVD-R.

Tipo	Tempo de Degradação
Registradores	Nanossegundos
Memória RAM	10 nanossegundos
Informações de Rede	Milissegundos
Processos em execução	Segundos
Memória flash	100.000 ciclos de gravações
CDs e DVDs	De 3 a 5 anos

Por isso, alguns tipos de dados e informações somente podem ser coletados por especialistas em forense computacional e atendendo a padrões de procedimento já estabelecidos, por exemplo, na ABNT NBR ISO/IEC 27037:2013;

- Têm alta capacidade de replicabilidade da prova original sem comprometimento de sua integridade, autenticidade, confidencialidade, autenticidade e legalidade;

- Que independentemente da metodologia utilizada para avaliação das provas e evidências, o resultado final deverá ser o mesmo – Reprodutibilidade;

- Que independentemente de quantas vezes forem feitas as avaliações sobre a mesma prova utilizando o mesmo método, o resultado final será sempre o mesmo – Repetibilidade.

Ao utilizar provas digitais, deve-se sempre buscar preservar o **documento original** (normalmente um arquivo de computador), pois somente estes estarão aptos a serem submetidos a perícia direta, ou seja, que estão nos formatos nativos em que foram criados, preservando os seguintes atributos:

- **Integridade**, que indica a não alteração de seus dados desde a criação ou última modificação desejada;

- **Confidencialidade**, somente permite acesso aos dados a quem seu criador estipulou;

- **Disponibilidade**, descreve que os dados estarão aptos para acesso e processamento no momento em que for necessário;

- **Autenticidade**, que determina a condição de autoria do documento;

- **Legalidade**, a produção, manuseio e guarda dos dados está em conformidade com a lei.

No entanto, nem sempre o documento poderá ser apresentado como prova em seu formato original, em virtude da linguagem computacional empregada, que dependerá de programa ou solução específica para traduzir o que está lá registrado para compreensão humana.

Por isso, é comum que exista a captura de como o documento eletrônico original é exibido para juntada nos processos judiciais ou administrativos.

Quando houve a validação do processo eletrônico no Brasil pela Lei nº 11.419 de 2006, seu artigo 11 determinou que os documentos trazidos aos processos digitais pela parte do processo **são considerados originais**, reedição confirmada pelo Código de Processo Civil, artigo 425, inciso VI:

“Art. 11. Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais.”

§ 1º Os extratos digitais e os documentos digitalizados e juntados aos autos pelos órgãos da Justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pelas procuradorias, pelas autoridades policiais, pelas repartições públicas em geral e por *advogados* públicos e *privados têm a mesma força probante dos originais, ressalvada a alegação motivada e fundamentada de adulteração antes ou durante o processo de digitalização.*

“Art. 425. *Fazem a mesma prova que os originais:* (...)

VI - as reproduções digitalizadas de qualquer documento público ou particular, quando juntadas aos autos pelos órgãos da justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pela Defensoria Pública e seus auxiliares, pelas procuradorias, pelas repartições públicas em geral e por *advogados, ressalvada a alegação motivada e fundamentada de adulteração.*

Esses extratos e reproduções são reconhecidos pela legislação como produzindo efeitos legais idênticos aos originais por presunção, admitindo-se a sua desconstituição por meio de oposição à sua **autenticidade** ou **integridade**.

Quando houver dúvida sobre a autenticidade de determinado documento particular, quem o apresentou ao processo deverá comprovar que tais condições são fidedignas, sob pena de o conteúdo trazido pela da prova ser perdido, de acordo com os artigos 428, inciso I e 429, inciso II também do Código de Processo Civil:

“Art. 428. *Cessa a fé do documento particular quando:*

I - *for impugnada sua autenticidade e enquanto não se comprovar sua veracidade;*

“Art. 429. *Incumbe o ônus da prova quando:* (...)

II - *se tratar de impugnação da autenticidade, à parte que produziu o documento.*

Por outro lado, a prova que se funda em documento digital também poderá perder sua fé quando for provado que as alegações ali retratadas não são verdadeiras ou foram alvo de alteração em relação ao original, nos termos do artigo 427 do Código de Processo Civil:

*“Art. 427. **Cessa a fé do documento público ou particular sendo-lhe declarada judicialmente a falsidade.***

Parágrafo único. A falsidade consiste em:

I - formar documento não verdadeiro;

II - alterar documento verdadeiro.”

Neste caso, todavia, a falsidade deve ser comprovada por quem alega tal condição do documento, de acordo com o disposto no artigo 429, inciso I do Código de Processo Civil, seguindo o texto do artigo 225 do Código Civil:

*“Art. 429. **Incumbe o ônus da prova quando:***

I - se tratar de falsidade de documento ou de preenchimento abusivo, à parte que a arguir;”



Assim, é dever de diligência da parte que levar a reprodução de documento digital original ao processo **preservar o arquivo de origem**, pois caso haja necessidade de perícia ou avaliação mais cuidadosa, especialmente se houver questionamento sobre sua autenticidade ou integridade, será possível fundamentar a força jurídica da prova produzida e evitar que sua fé seja comprometida.

Além desta condição para guarda dos originais, há a possibilidade de o vencido ingressar com ação rescisória no caso (revisão judicial de sentença



transitada em julgado) em até dois anos do trânsito em julgado da última decisão do processo, de acordo com os artigos 425 e 975 do Código de Processo Civil:

“Art. 425. (...)”

§ 1º Os originais dos documentos digitalizados mencionados no inciso VI deverão ser preservados pelo seu detentor até o final do prazo para propositura de ação rescisória.”

“Art. 975. O direito à rescisão se extingue em 2 (dois) anos contados do trânsito em julgado da última decisão proferida no processo.”

Haja vista que tais sistemas de informação possuem linguagem própria para criação, operação, guarda e exclusão de dados, devemos avaliar alguns cuidados determinantes para que a produção específica de determinadas provas eletrônicas seja feita adequadamente.



**CONFIABILIDADE DAS
PROVAS DIGITAIS**

Como ponto de partida para entendermos a confiabilidade das provas digitais, é necessário compreender o que são **sistemas confiáveis**, pois a partir destes que tais evidências serão geradas.

“Uma base computacional confiável (BCC) contém hardware e software além de vias de comunicação confiáveis (VCC) entre várias bases computacionais. Em termos leigos, Os sistemas de informação são considerados confiáveis quando há proteção encapsulando os equipamentos físicos, os programas e os dados em determinada área de processamento e protegendo as transações entre usuários utilizando canais seguros” LEWIS, Theodore Gyle. Critical infrastructure protection in homeland security: defending a networked nation. Second Edition. New Jersey: John Wiley & Sons, 2015, p. 145 (Tradução do autor)

Quando existir a utilização de provas digitais em determinado processo judicial ou administrativo, o juiz ou aquele que decidirá sobre o caso com base nas evidências trazidas ao expediente terá de avaliar o teor do documentos que for apresentado representando o conteúdo de determinado documento digital, especialmente porque foi apre-

sentado pela parte que o produziu.

Sob estas condições, **é imprescindível que haja exposição de características de confiabilidade do sistema em que a prova foi produzida**, em que há retratação genuína de fatos praticados por terceiros e não de declaração unilateral de vontade.

Isso se deve porque o sistema de informação está sob controle e supervisão da parte que quer se utilizar de documento por ele produzido para obter sucesso em disputa judicial ou administrativa, então, se presume que possui total controle e manipulação de tais registros, **fator que pode comprometer a prova.**

No entanto, a prova ganhará força sempre que existir comprovação que o sistema:

- Produz registros de atividade (*logs*) indicando qual usuário praticou qual ação, quando a praticou e por quanto tempo a executou como forma de representar trilha de auditoria de como o sistema de informação foi utilizado. Tais registros não devem ser acessados por usuários não administradores e não devem ser passíveis de edição ou exclusão, sob nenhuma hipótese;
- Possui diretivas de acesso para cada tipo de usuário (*need to know e least privilege*), garantindo que a prova eletrônica apresentada não sofreu adulteração desde sua criação;

- Possui controles de permissões adequados com as diretivas de acesso (*need to know e least privilege*) e não podem ser revogados por usuários que não sejam administradores;

- Possui controles de proteção à toda estrutura, compreendendo registros de acesso das atividades de permissões, travas contra alteração de metadados de arquivos e registros de atividade por quaisquer usuários ou exigência de dupla ou tripla autenticação para tarefas destinadas aos administradores.

Como regra abrangente das atividades de comércio eletrônico, o artigo 4º do Decreto que promoveu sua regulamentação, 7.962 de 2013, o artigo 4º e inciso VII indica a **necessidade de recursos seguros e confiáveis para fluxos de pagamento e tratamento de dados pessoais**, diretamente vinculados a links seguros de **transmissão de dados via internet com algoritmos assimétricos fortes** (SHA-384 ou 512) ou de **guarda de dados em repouso utilizando além de algoritmos simétricos fortes** (AES-256 ou Twofish), técnicas de obfuscação de dados à base respectiva:

“Art. 4º Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá:

VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.”

Nesse sentido, o artigo 3º da Resolução nº 3.964 de 2009 do Banco Central do Brasil estabeleceu parâmetros em que a prestação de serviços bancários por meios alternativos deverão ser fornecidos, o que inclui as interfaces digitais:

“Art. 3º (...)

*§ 2º A opção pela **prestação de serviços por meios alternativos aos convencionais é admitida desde que adotadas as medidas necessárias para preservar a integridade, a confiabilidade, a segurança e o sigilo das transações realizadas, assim como a legitimidade dos serviços prestados**, em face dos direitos dos clientes e dos usuários, **devendo as instituições informá-los dos riscos existentes.**”*

Então, como ponto de partida deve-se construir sistema de informação que atenda aos requisitos técnicos de

segurança adequados para que sejam preservados os atributos da **Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade** dos processos e dados pela leitura do artigo acima de modo a reduzir os riscos operacionais, de acordo com o estabelecido pela família de normas técnicas ABNT NBR ISO/IEC 27000.

Nesse mesmo sentido verificamos o texto regulatório do BACEN ao publicar **as condições para abertura e encerramento de contas de depósito exclusivamente por meios eletrônicos** na Resolução nº 4.480 de 2016, artigo 5º:

“Art. 5º Os procedimentos e as tecnologias utilizados na abertura e no encerramento de contas de depósitos por meio eletrônico devem assegurar:

*I - **integridade, autenticidade e confidencialidade** das informações e dos documentos eletrônicos utilizados;*

*II - **proteção contra o acesso, o uso, a alteração, a reprodução e a destruição não autorizados das informações e documentos eletrônicos;***

*III - **produção de cópia de segurança das informações e dos documentos eletrônicos;** e*

*IV - **rastreamento e auditoria dos procedimentos e das tecnologias empregados no processo.**”*

Depois de construído sistema atendendo a esses critérios e controles de segurança da informação, caso a parte tenha de apresentar prova produzida por sistema que ela própria controla, **podará contar com a obtenção de certificações de segurança da informação expedida por peritos ou auditores independentes que transmitirão ao julgador veredito técnico sobre a confiabilidade do sistema que se extraíram as evidências digitais e não se confundam com declarações unilaterais de vontade,** que possuem pouca força de prova.

A rigor, os documentos digitais terão **força probante contra terceiros quando assinados com certificado digital ICP-Brasil,** conforme descrito no artigo 10º, § 1º da Medida Provisória nº 2.200-2 de 2001:

“Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1º de janeiro de 1916 - Código Civil.” (N.A. Atual 219)

Quando não houver uso do certificado digital ICP-BRASIL, mas procedimento eletrônico que garanta autenticidade dos documentos produzidos, haverá pleno efeito legal entre as partes envolvidas em tal operação caso tenham aceito tal procedimento como válido e eficaz, **como contratações digitais de modo geral**, valerá o disposto no § 2º do mesmo artigo da referida Medida Provisória:

“§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.”

Por outro lado, quando for apresentada prova que foi gerada por um sistema de informação oficial ou perfil de aplicação de internet fidedigno, a autenticidade da prova é de difícil contestação, já que ocorrerá presunção de veracidade estabelecida pelo Código Civil em seu artigo 219 e o Código de Processo Civil em seu dispositivo 412:

“Art. 219. As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários.”

“Art. 412. O documento particular de cuja autenticidade não se duvida prova que o seu autor fez a declaração que lhe é atribuída.”

Pela aplicação da **Teoria da Aparência**, tal presunção de que o conteúdo é genuíno por todos os elementos envolvidos apontarem que as informações são fidedignas e que partiram de quem se diz controlar tal sistema ou interface **ganha ainda mais força, pois todos os elementos gráficos e indicativos de que pertence àquela parte levam a crer que esta é a verdade real dos fatos.**

Quando esses **conteúdos vão contra os interesses de quem publicou a**

prova recebe mais relevância, sendo classificada como confissão, submetendo quem divulgou determinadas informações ou conteúdos às consequências deles decorrentes, seguindo o disposto pelos artigos 374 e 389 do Código de Processo Civil:

“Art. 374. Não dependem de prova os fatos:

I - notórios;

II - afirmados por uma parte e confessados pela parte contrária;

III - admitidos no processo como incontroversos;

IV - em cujo favor milita presunção legal de existência ou de veracidade.”

*“Art. 389. **Há confissão**, judicial ou extrajudicial, **quando a parte admite a verdade de fato contrário ao seu interesse e favorável ao do adversário.**”*

Contudo, se provada a existência de defeito na autenticidade do material que foi divulgado e utilizado contra a parte que o fez, a prova poderá ser des-

considerada, sobretudo nos casos de erro ou coação, conforme exposto pelo artigo 393 do Código de Processo Civil:

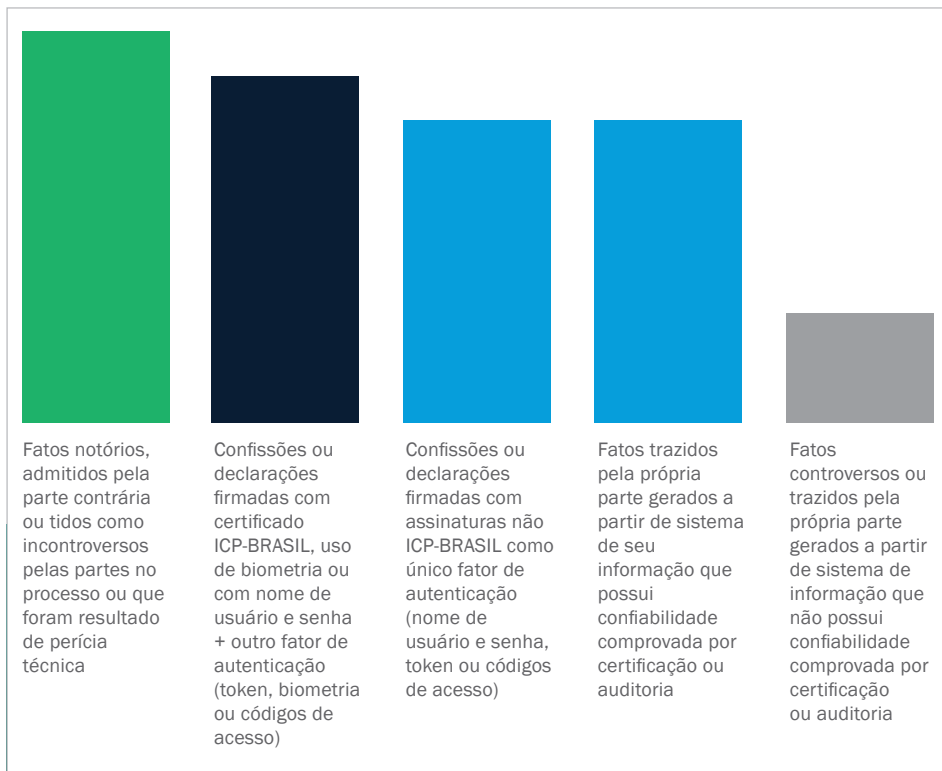
*“Art. 393. **A confissão é irrevogável**, mas pode ser **anulada se decorreu de erro de fato ou de coação.**”*



Neste capítulo identificamos a importância da confiabilidade das provas digitais e da força probante que possuem, tanto daquelas que foram produzidas

por quem as irá utilizar ou por evidências disponibilizadas por terceiros.

No gráfico abaixo temos panorama de força das provas acima mencionadas:





CONDIÇÕES PARA FORMAÇÃO DE PROVAS LÍCITAS

De acordo com a legislação em vigor no Brasil, as provas somente serão aceitas em procedimentos administrativos ou judiciais se forem **lícitas**, ou seja, **quando não forem obtidas violando direitos**, de acordo com o inciso LVI do artigo 5º da Constituição Federal:

“Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)

LVI - são inadmissíveis, no processo, as provas obtidas por meios ilícitos;”

Complementarmente, o Código de Processo Civil em seu artigo 369 permite livre produção da prova desde que atendam suas condições morais de legitimidade e sua produção não seja ilícita:

*“Art. 369. **As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz.**”*

Apesar de a utilização de provas ser livre pelas partes, deve existir bom senso para que sejam relevantes ao processo, pois, se não for capaz de interferir na convicção do juiz, esta poderá ser negada ou desconsiderada por ser **prova inútil**.

Dada a condição primordial para que não se violem direitos na obtenção da prova, qual seja de que seu sigilo não seja comprometido no momento de sua colheita, ou seja, deve ser acessível, requisito que depende de um dos atributos de segurança da informação: a **confidencialidade**.

A **confidencialidade** de determinada informação pode ser imposta pela lei ou decorrer de garantia legal, o que inclui o desejo de seu proprietário em não divulgá-la, fazendo com que somente sejam apresentadas mediante ordem judicial específica.

De modo amplo, existe confidencialidade por todos os dados de particulares (pessoas naturais ou jurídicas), pois decorre da combinação do direito à propriedade (dispor, usar e fruir) e de legítima expectativa de privacidade, de acordo com a leitura do inciso XXII do artigo 5º da Constituição Federal conjuntamente com os incisos X e XII, respectivamente:

“Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)”

*X - **são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;** (...)*

*XII - **é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;** (...)*

*XXII - **é garantido o direito de propriedade;**”*

A lei reforça alguns casos de tais dados confidenciais:

- Informações bancárias ou financeiras, artigo 1º da Lei Complementar nº 105 de 2001:

“Art. 1º As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados.”

- Dados de ordem fiscal, artigo 198 da Lei nº 5.172 de 1966, o Código Tributário Nacional:

“Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades.”

- Segredos de negócio e industriais, artigo 206 da Lei nº 9.279 de 1996:

“Art. 206. Na hipótese de serem reveladas, em juízo, para a defesa dos interesses de qualquer das partes, informações que se caracterizem como confidenciais, sejam segredo de indústria ou de comércio, deverá o juiz determinar que o processo prossiga em segredo de justiça, vedado o uso de tais informações também à outra parte para outras finalidades.”

- Sigilo nas comunicações telefônicas, telemáticas, privadas, artigo 1º da Lei nº 9.296 de 1996:

“Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob sigredo de justiça.

Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.”

- Registros de conexão à internet e registros de acesso às aplicações de internet, artigo 10º, §§ 1º e 2º;

“Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.”

No entanto, são somente exemplos, sobrevalendo a regra geral indicada pela tríade de incisos do artigo 5º da Constituição Federal já apresentada, em que **é indispensável ordem judicial específica para obtenção de tais dados.**

Ainda que exista a solicitação extrajudicial desses dados ao detentor, este somente poderá fornecê-los se for o proprietário dos dados, não podendo fornecê-los se pertencerem a terceiro, todavia, **sob pena de ser considerada**

prova com vício insanável, pois pode violar o dever de sigilo imposto pela Constituição Federal, uma vez que deveria preservar sua confidencialidade.

Adicionalmente, os dados que tiverem o Estado como seu proprietário ou controlador possuem diretiva específica apresentada pela Lei nº 12.527 de 2011, a Lei de Acesso à Informação, em que indica a diretiva padrão como sendo o acesso público, mas passível de restrição conforme sua classificação pelo órgão responsável, seguindo o texto do artigo 3º, inciso I:

“Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:

I - observância da publicidade como preceito geral e do sigilo como exceção;”



Dentre as classificações possíveis e o tempo de restrição, temos que o artigo 24 da lei apresentou quais são as indicações possíveis por parte do Estado:

“Art. 24. A informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada como ultrassecreta, secreta ou reservada.

§ 1º Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista no caput, vigoram a partir da data de sua produção e são os seguintes:

I - ultrassecreta: 25 (vinte e cinco) anos;

II - secreta: 15 (quinze) anos; e

III - reservada: 5 (cinco) anos.”

Para ter acesso a tais dados sob controle do Estado, é necessário que haja pedido específico ao órgão que for proprietário ou gestor da informação, de acordo com o previsto no artigo 10º da já mencionada lei:

“Art. 10. Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades referidos no art. 1º desta Lei, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida.”

Em contrapartida, quando os dados forem da Instituição Financeira e estiverem sob controle de terceiros, há total legitimidade para sua utilização e apresentação como prova, pelos princípios **de uso e fruição** que estão contidos no direito à propriedade, a exemplo de e-mails trocados, que estarão o remetente e os destinatários como donos de seus respectivos arquivos da mensagem.

Também, quando os os dados não são de propriedade da Instituição e forem publicados ou disponibilizados por terceiro, **a boa-fé em seu acesso é presumida desde que não exista violação aos dispositivos legais do sigilo acima descritos** (texto, imagem, áudio, vídeo ou a combinação entre eles nas mais diversas mídias sociais), isto é, se não pertencerem a outros e não forem sigilosos por força de lei (dados bancários, fiscais, etc).



O ÔNUS DA PROVA E SUAS HIPÓTESES DE INVERSÃO

Constatada a importância da prova para que a Instituição Financeira possa buscar defender seus interesses caso ocorram perdas financeiras e sua licitude na produção, é indispensável que haja domínio sobre o ônus da prova que lhe recai.

Quando esta for pleitear algum direito que entender possuir, deverá apresentar suas razões de fato para que lhe seja identificada legitimidade no que foi apresentado, especialmente em âmbito judicial.

Esta é a regra geral do ônus da prova, fixada pelo artigo 373, inciso I do Código de Processo Civil:

“Art. 373. O ônus da prova incumbe:

I - ao autor, quanto ao fato constitutivo de seu direito;”

Contudo, quando estiver na posição oposta, isto é, em que alguém promove ação em seu desfavor, poderá existir o fenômeno de **inversão do ônus da prova**, conforme estabelece o artigo 6º, inciso VIII do Código de Defesa do Consumidor (CDC), desde que configurada relação de consumo entre o cliente e a Instituição Financeira e se constate um dos seguintes critérios: **que as alegações são plausíveis e se presumem verdadeiras** ou **que o consumidor for hipossuficiente:**

“Art. 6º São direitos básicos do consumidor: (...)

*VIII - **a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente**, segundo as regras ordinárias de experiências;”*

Tal situação se aplicará também às vítimas de fatos que foram praticados pela Instituição, ainda que não sejam clientes, nos termos do artigo 17 também do CDC:

“Art. 17. Para os efeitos desta Seção, equiparam-se aos consumidores todas as vítimas do evento.”

Na prática, sempre que a parte invocar o direito à inversão do ônus da prova quando ingressar com ação indenizatória, **o juiz deverá o preenchimento dos requisitos para tal inversão**, isto é, se os fatos narrados possuem força suficiente para serem considerados verdadeiros ou que o consumidor sofra de **limitações para produzir a prova**

por sua condição social, capacidade econômica, de acesso às informações ou de educação, hipótese que a Instituição Financeira deverá apresentar provas para afastar os pedidos feitos, ainda que o autor não tenha apresentado nenhuma.

O Código de Processo Civil também conferiu **poderes ao juiz para determinar a distribuição do ônus da prova de acordo com a capacidade de cada parte em produzi-la,** podendo assumir o caráter de inversão de ônus da prova quando não existe relação de consumo entre as partes em litígio, de acordo com o artigo 373, § 1º.

“Art. 373. O ônus da prova incumbe: (...)

§ 1º Nos casos previstos em lei ou diante de peculiaridades da causa relacionadas à impossibilidade ou à excessiva dificuldade de cumprir o encargo nos termos do caput ou à maior facilidade de obtenção da prova do fato contrário, poderá o juiz atribuir o ônus da prova de modo diverso, desde que o faça por decisão fundamentada, caso em que deverá dar à parte a oportunidade de se desincumbir do ônus que lhe foi atribuído.”

Ou seja, ainda que não haja relação de consumo entre a Instituição Financeira e as partes de eventual processo judicial, a Instituição poderá ser compelida a apresentar provas de determinados fatos em virtude de deter a maior porção das documentações dos serviços prestados em seus sistemas, sobretudo por força regulatória.

Esta hipótese não atribui a carga de fazer prova em favor das outras partes, mas de facilitar a compreensão dos fatos que são trazidos pelos litigantes, em que o juiz determinará a juntada de determinada evidência conforme o caso concreto que solucione determinada questão de fato, sobretudo quando atendidas as condições de encargo excessivo ou que **a produção da prova é impossível** (prova diabólica).

Além desta possibilidade de inversão do ônus da prova em processos judiciais, o Código de Defesa do Consumidor impõe **a carga de provar fatos àquele que patrocinar conteúdo publicitário quando alguém contestar que tal material não diz a verdade ou não está correto** pela leitura de seu artigo 38.

“Art. 38. O ônus da prova da veracidade e correção da informação ou comunicação publicitária cabe a quem as patrocina.”

Por isso, o artigo 36 do CDC **determina àquele que for realizar veiculação de publicidade que guarde as evidências de fato, dados técnicos e científicos que assegurem o caráter fidedigno do material publicitário.**


“Art. 36. A publicidade deve ser veiculada de tal forma que o consumidor, fácil e imediatamente, a identifique como tal.

Parágrafo único. O fornecedor, na publicidade de seus produtos ou serviços, manterá, em seu poder, para informação dos legítimos interessados, os dados fáticos, técnicos e científicos que dão sustentação à mensagem.”

Assim, em virtude de a legislação impor facilitação dos direitos de defesa do consumidor na relação de consumo, por este ser parte mais fraca, como já mencionamos anteriormente, temos que esta se encontra em posição de desvantagem em eventual ação judicial por ter recebido mais obrigações processuais pelos comandos de lei e a jurisprudência.

Então, o cumprimento adequado do ônus da prova por parte da Instituição Financeira é condição mínima para que esteja em condições de igualdade de disputa judicial e minimizar as ocorrências de indenizações ilegítimas pleiteadas, haja vista a condição da carga probatória ser atribuída a ela.



A green credit card is the central focus, tilted at an angle. It features a pen resting on it. The card has the text 'CREDIT BANK' at the top, a card number '2319 9860 1535 9007', and a name 'MR. YOUR NAME HERE'. The background is filled with binary code (0s and 1s) and a grid pattern.

**PRODUÇÃO DE DOCUMENTOS NOS
SISTEMAS DE INFORMAÇÃO DA
INSTITUIÇÃO
FINANCEIRA**

Existem diversas obrigações legais e regulatórias para a produção de registros de operações por parte das Instituições Financeiras que terão fins de auditoria, fiscalização e controle, que também deverão ser executadas quando houver uso dos meios digitais, se revelando como outra forma possível de prática de atos de natureza creditícia ou financeira.

Isso significa que a realização de guarda de determinados registros somente mudou de formato, mas a proteção de **autenticidade** e **integridade** de tais documentos permanece a mesma, por isso os sistemas de informação que a Instituição Financeira adotar deverão estar aptos de cumprir com os deveres legais de registros de auditoria já fixados pela lei e por normas regulamentares, especialmente pela **preservação de seus originais**.

Adicionalmente, a Instituição deve aplicar medidas de proteção à confidencialidade de modo a cumprir com o estabelecido na Lei Complementar nº 105 de 2001, em seu artigo 1º (vide capítulo 4).

Então, é mandatário que a Instituição Financeira adote **técnicas de segregação de bases de dados, criptografia com algoritmos fortes (simétricos AES-256 ou maior e Twofish; assimétricos SHA-384 ou 512), diretivas de segu-**

rança e sistemas de monitoramento e controle em suas redes para que consigam assegurar o sigilo das operações dos clientes e dos registros de atividade que os documentarem (*logs*).

Sob tais cuidados a Instituição Financeira deverá realizar a geração de documentos digitais que comprovarão as operações realizadas em seus sistemas de informação, atendendo ao já disposto na lei e demais normativos que regulam a atividade bancária e financeira.

Uma dessas obrigações de produção de documentos digitais que são previstas pela legislação bancária pode ser exemplificada pela Carta Circular nº 3.454 de 2005 do BACEN, que determina a forma de composição de arquivos contendo informações de clientes solicitadas para investigação de crimes previstos na lei nº 9.613 de 1998 (lavagem de dinheiro).

No entanto, há obrigações legais impostas às Instituições Financeiras que utilizarem de aplicações da internet como **meio alternativo** para a prestação de seus serviços, assim identificados os sistemas de informação ou tecnologias que permitem ao cliente realizar operações bancárias ou financeiras, a exemplo de aplicações de internet, terminais

de auto atendimento 24horas (ATM), ligação telefônica ou via mensagem de texto curta (torpedo-SMS).

Muito embora algumas disposições sejam aplicáveis quando existe relação de consumo entre o cliente e a Instituição Financeira, o que afastaria sua incidência sobre o relacionamento bancário e financeiro com pessoas jurídicas, **é recomendável que a produção de documentos ocorra de modo uniforme para todo o público da Instituição, evitando assimetrias no sistema e complicações para configuração de determinados serviços,** além de **maximizar o acesso à informação e transparência como sinal de boas práticas.**

A primeira regra para produção de documentos digitais que merce desta que é a **confirmação de determinada operação ou contratação de serviço solicitados pelo cliente à Instituição Financeira** tão logo haja recebimento de tal comando via sistema de informação, de acordo com as regras impostas pelo Decreto nº 7.962 de 2013, artigo 4º, III:

“Art. 4º Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá: (...)

III - confirmar imediatamente o recebimento da aceitação da oferta;”

Tal providência exigida pela legislação faz com que a Instituição Financeira comunique de modo ativo seus clientes submetendo mensagens de que houve recebimento do seu pedido de contratação de serviço com sucesso ou de operações em sua interface, com vistas a manter o cliente sempre informado sobre o que efetivamente foi firmado durante o fluxo de atividades no sistema.

Adicionalmente, **a Instituição também deverá manter o histórico dos contratos e das operações realizadas por seus clientes, permitindo que possam verificar as operações realizadas a qualquer tempo, de acordo com o inciso IV do mesmo artigo 4º do Decreto nº 7.962,** cumprindo com os deveres de transparência já fixados no Código de Defesa do Consumidor:

“IV - disponibilizar o contrato ao consumidor em meio que permita sua conservação e reprodução, imediatamente após a contratação;”

Sob as mesmas premissas de informação ao cliente **há disposição legal que obriga a Instituição Financeira a confirmar o recebimento de requisições de atendimento a dúvidas, dificuldades ou inadequações sobre dos**

serviços prestados, realizando prova positiva de que efetivamente tomou conhecimento da requisição e que dela se esperam providências.

“VI - confirmar imediatamente o recebimento das demandas do consumidor referidas no inciso, pelo mesmo meio empregado pelo consumidor;”

Todas as operações acima devem gerar documentos eletrônicos registrando a operação que foi realizada ou mensagem recebida por parte do cliente, podendo compreender mais de um tipo de sistema de informação e gerando mais de uma prova de sua ocorrência.

Além de obrigações com vistas a documentar as operações de contratação e atendimento do cliente nas plataformas digitais da Instituição Financeira, a legislação em vigor também impõe a obrigação de registro de determinadas atividades quando for utilizada aplicação de internet como sistema de informação.

Conforme previsto na lei nº 12.965 de 2014, o Marco Civil da Internet, há disposições em que se tem como necessário o registro documental de diversos momentos específicos na utilização dessas interfaces.

O primeiro deles é a **concordância com os Termos de Uso de tal ambiente digital**, exposta pela necessidade de publicidade e clareza de tais regras, o que se presume com a declaração de vontade do usuário que está de acordo com as disposições apresentadas, conforme aplicação prática do artigo 7º, inciso XI da lei:

“Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...)

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;”

Em seguida, **é indispensável que haja a documentação do consentimento dado pelo usuário às atividades de tratamento de dados pessoais que serão realizadas de acordo com a Política de Privacidade ou documento de igual valor** apresentado pela Instituição Financeira, seguindo o disposto pelo inciso IX do mesmo artigo, comprovando-se que houve exercício deste direito a contento pelo cliente:

*“IX - **consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;**”*

Seguindo as mesmas orientações jurídicas, **deve-se realizar registro do pedido de apagamento dos dados pessoais do cliente quando houver encerramento de relação de serviços com a Instituição Financeira e da comunicação do recebimento deste pedido com sucesso.** consoante estabelece o inciso X do artigo 7º do Marco Civil da Internet:

“X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;”

Além da produção desses documentos, o Marco Civil da Internet estabeleceu obrigação de guarda dos seus registros de acesso à determinada aplicação de internet (logs) pelo prazo de 6 seis (meses) e sob controles de segurança e sigilo, conforme determinado pelo artigo 15 da lei:

“Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.”



Como não houve descrição do que se consideraria efetivamente acesso à aplicação, é recomendável que se registrem todas as atividades do cliente nos ambientes digitais disponibilizados pela Instituição Financeira que utilizarem a internet, **dada a importância de compliance com tal disposição**, a exemplo, mas não se limitando a:

- Abertura da conta;
- Leitura dos Termos de Uso da aplicação de internet e sua respectiva Política de Privacidade, além de outros contratos que forem exibidos ao usuário;
- Concordância com os Termos de Uso da aplicação de internet e sua respectiva Política de Privacidade;
- Registro do fator de autenticação na plataforma (uso de senha, *token* ou dados biométricos);
- Alteração de dados cadastrais ou de autenticação (senhas, *token* ou dados biométricos);
- Autenticação bem sucedida no sistema;
- Autenticação mal sucedida no sistema;
- Inserção, edição ou exclusão de dados para recuperação de senha ou acesso à conta (e-mail alternativo, número de telefone celular, etc.)
- Realização de transferências, pagamentos e operações em geral;
- Tomada de créditos;
- Contratação de serviços adicionais;
- Renegociação de eventuais débitos;

- Geração de relatórios;
- Recuperação de comprovantes;
- Cancelamento de serviços ou operações;
- Encerramento da conta.

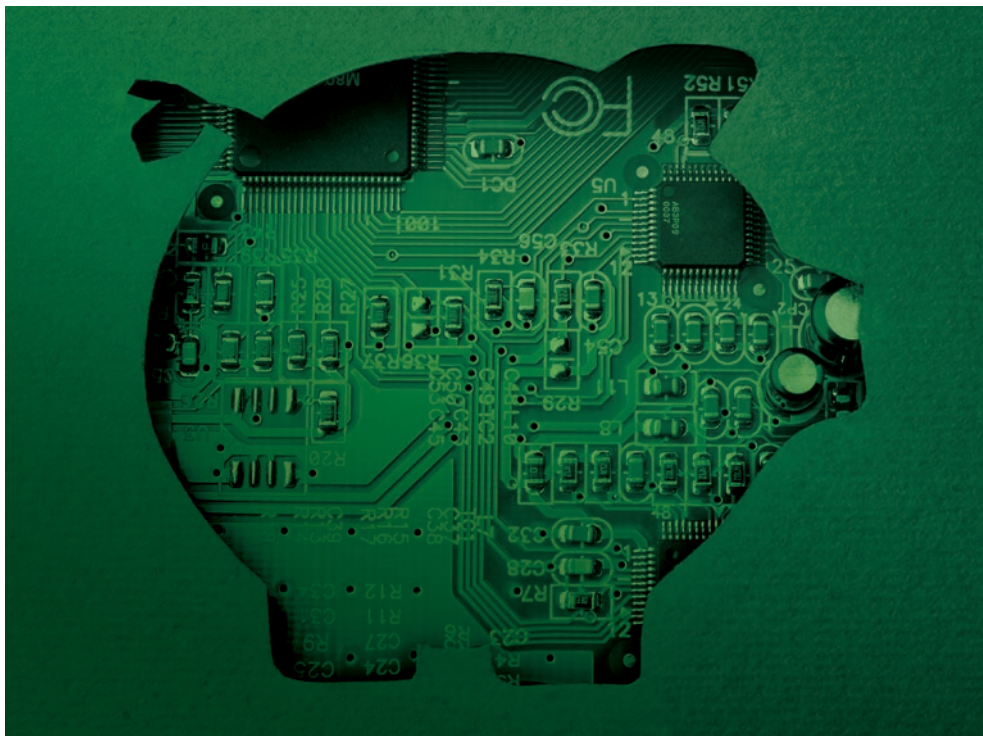
Para a guarda desses registros o Marco Civil da Internet estabelece como obrigatória a anotação do **endereço de IP do usuário** que utiliza a aplicação, **data, hora e fuso respectivo**, conforme o inciso VIII do artigo 5º da lei:

“Art. 5º Para os efeitos desta Lei, considera-se: (...)

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.”

Contudo, pelo esgotamento dos endereços de internet disponíveis devido à limitação de sua arquitetura na versão 4 (IPv4), a ANATEL formalizou alternativa às empresas de telecomunicação para manter seus clientes com acesso à internet, que é a utilização de recurso de agrupamento de diversos acessos num mesmo endereço de origem, adotando fracionamento por **portas lógicas de conexão**.

Por isso, é recomendável que a Instituição Financeira prepare seus sis-



temas de aplicação de internet para realizar o registro também deste componente de acesso por parte do usuário, como medida de cumprimento adequado às próprias orientações da ANATEL para permitir a identificação adequada dos terminais de rede em caso de investigação de autoria por atos ilícitos ou fraudes, ou para que consiga alcançar os melhores resultados de tal atividade de identificação caso necessário, conforme prescrito em seu Relatório Final de Atividades do GT-IPv6:

*“para que a identificação unívoca de usuário seja possível a partir da implantação do CG-NAT44, será necessário que as entidades com poder requisitório informem, além do (1) **endereço IPv4 de origem** e (2) do período de **tempo em que foi realizado o acesso (acompanhado do fuso horário aplicável)**, passem também a **informar (3) a porta de origem.**”*

Além desses dados, a Instituição Financeira poderá obter e registrar outros detalhes de autenticação e uso de seus ambientes digitais disponibilizados a seus clientes, a exemplo de:

- **Informações sobre o dispositivo utilizado para as operações (marca, modelo, número do telefone utilizado e IMEI, de dispositivo móvel, ou fingerprints de um computador por exemplo)**, em que será possível comparação quando houver repúdio de algum ato praticado; ou
- **Informações de geolocalização no momento da operação.**

Uma vez produzidos, os documentos anteriores deverão atender o prazo de guarda que lhes for determinado para cumprimento das disposições em lei e normas regulatórias, sendo certo que o prazo de 6 (seis) meses previsto no Marco Civil da Internet é insuficiente para atender aos melhores interesses da Instituição Financeira, dada a força jurídica que possuem e versatilidade na combinação de outras evidências para formar o conjunto de provas.

O tempo exigido para guarda de registros na Circular nº 3.461 de 2009, artigo 11, varia de 5 (cinco) a 10 (dez) anos, complementado pelo prazo de 5 (cinco) anos de prescrição de ação por prejuízos sofridos pelo consumidor

previsto no artigo 27 do CDC, em que a Instituição poderá ser compelida a apresentar evidências em juízo pela **inversão do ônus da prova** (vide capítulo 2) e, se não o fizer, haverá fundada expectativa de perda da ação.

*“Art. 11. **As informações e registros de que trata esta circular devem ser mantidos e conservados durante os seguintes períodos mínimos, contados a partir do primeiro dia do ano seguinte ao do término do relacionamento com o cliente permanente ou da conclusão das operações:***

*I - **10 (dez) anos, para as informações e registros de que trata o art. 7º;***

*II - **5 (cinco) anos, para as informações e registros de que tratam os arts. 6º, 8º e 9º.”***

“Art. 27. Prescreve em cinco anos a pretensão à reparação pelos danos causados por fato do produto ou do serviço prevista na Seção II deste Capítulo, iniciando-se a contagem do prazo a partir do conhecimento do dano e de sua autoria.”

**PRESERVAÇÃO E USO DAS PROVAS
DIGITAIS DOS SISTEMAS DE INFORMAÇÃO
DA INSTITUIÇÃO FINANCEIRA**

**COMPLIANCE DA
ATIVIDADE EM
MEIO DIGITAL**

Após a criação dos documentos digitais elencados no capítulo anterior, é imprescindível que estes sejam preservados de modo adequado para estarem disponíveis quando for necessária a utilização destes como prova em algum procedimento judicial ou administrativo.

Isto é, devem atender ao sigilo necessário, estar íntegros e acessíveis pelo tempo de guarda estabelecido pela Instituição, adotando-se os recursos tecnológicos apropriados para tanto.

Muito embora existam normas técnicas que indiquem os controles adequados a serem tomados para que esses atributos sejam preservados, a lei somente fixou obrigações nesse sentido para os registros de conexão à internet e acesso às suas aplicações no Decreto regulamentador do Marco Civil da Internet nº 8.771 de 2016, estabelecendo diretrizes em seu artigo 13 e incisos.

O primeiro controle apresentado é a necessidade de aplicação de restrições de acesso a tais documentos, em que as permissões devem ser concedidas de acordo com as responsabilidades e funções a serem desempenhadas por cada usuário:

“Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:

I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;”

Em seguida é apresentado o controle de adoção de múltiplos fatores para autenticação do usuário que for ter acesso a tais registros de aplicação à internet, de modo a reforçar a garantia de que realmente foi o usuário respectivo que os acessou, **já que o procedimento de autenticação é considerado forte quando envolve ao menos dois fatores.**

São fatores de autenticação todas as informações capazes de confirmar a identidade da pessoa correspondente quando utiliza sistemas digitais, sendo classificados por:

- Algo que somente o cliente é ou é capaz de fazer, diretamente ligado à biometria;
- Algo que somente o cliente saiba, como senhas de acesso; ou
- Algo que somente o cliente tenha, a exemplo de *tokens* ou cartões de código.

“II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;”

É recomendável que exista supervisão da Instituição Financeira no momento da emissão do fator de autenticação por parte do cliente, evitando que exista fraude nesse momento, o que compromete a validade do procedimento por atribuição indevida da identidade digital (o sistema confirma que alguém é quem não deveria ser).

Outro controle de segurança exigido pelo Decreto é o **histórico de acesso aos registros de acesso a aplicações na forma de inventário, indicando qual usuário acessou qual arquivo de log, em que data, hora, fuso horário e por quanto tempo o fez:**

“III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014;”

Por fim, há a determinação do **uso de restrições na modificação em tais arquivos de registros de acesso à aplicação, podendo ser aplicados como propriedades de permissão no sistema operacional ou ainda pela utilização de criptografia,** que pode restringir acessos para conferir que o documento criado coincide com seu teor no momento de utilização:

“IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a invariabilidade dos dados, como encriptação ou medidas de proteção equivalentes.”

Como técnica decorrente de utilização de algoritmos criptográficos, **temos que o uso da função hash também é útil para se garantir a inviolabilidade dos dados de registros de acesso à aplicação de internet para a Instituição Financeira cumprir com o descrito no Decreto.**

“Outra aplicação de funções hash criptográficas em sistemas de computação seguros é que elas podem ser usadas para proteger a integridade de arquivos críticos de um sistema operacional. Se armazenarmos o valor hash criptográfico de cada um desses arquivos em memória protegida, podemos verificar a autenticidade desses arquivos apenas calculando seu valor hash criptográfico e comparando esse valor com aquele armazenado em memória segura. Visto que essas funções hash são resistentes a colisões, podemos confiar que, se esses dois valores combinam, é altamente provável que o arquivo não tenha sido adulterado. Em geral, funções hash são aplicáveis sempre que precisarmos de um resumo compacto de informação que seja difícil de falsificar.” (GOODRICH; TAMASSIA, 2013. p. 35.)

Ao mesmo tempo que o *log* é gerado, **o hash respectivo pode ser calculado e adicionado ao histórico de inventário anterior, possibilitando a comparação no momento de sua utilização.**

É recomendável também que se execute a função hash nos documentos recebidos pelos clientes por meio das aplicações de internet, de modo que seja possível atestar que seu conteúdo permaneceu inalterado desde o recebimento até eventual utilização da prova.

Este procedimento é recomendável caso a Instituição Financeira possibilite abertura de conta ou permitir que se contrate determinado serviço pela via digital com a solicitação de cópia de documentos pessoais, fotografia enviada como meio de autenticação (*selfie*), execução de assinatura no próprio dispositivo e outras informações que o cliente for enviar, como forma de preservar a integridade.

Ainda que esses cuidados sejam impostos pela lei e limitados aos registros de conexão à internet e acesso às suas aplicações, **podem também ser aplicados aos demais documentos eletrônicos criados pelos sistemas de informação da Instituição Financeira, especialmente nos logs que forem gerados em outros sistemas que não sejam o mesmo da aplica-**

ção de internet, de arquivos que resultem de operações específicas e determinadas bases de dados.

Também, a Instituição Financeira poderá dispor de outras informações que coletar em suas estruturas tecnológicas para formar suas provas, especialmente porque o estado da técnica se encontra em cenário de obtenção e criação de dados em grau escalar, assim chamado de big data, desde que atenda aos demais requisitos já impostos pela lei.

Como recomendação final, os documentos digitais que forem produzidos pelos sistemas de informação da Instituição devem ser mantidos em seu **formato original**, preservando os procedimentos de avaliação de metadados e outras características vinculadas à forense computacional caso seja necessário comprovar que o documento foi produzido adequadamente e que é possível se constatar sua autenticidade e integridade.





**GUARDA E PRESERVAÇÃO
DAS PROVAS DIGITAIS
DE SISTEMAS DE
INFORMAÇÃO
DE TERCEIROS**

Quando houver a necessidade de preservação de provas digitais em sistemas de informação de terceiros, a Instituição Financeira deverá se cercar de medidas que permitam o acesso adequado de tais informações conforme o caso específico.

Como já analisado anteriormente, para que determinada prova seja utilizada, quem for produzi-la necessita de **direitos de acesso**, que podem ser livres ou dependerem de ordem judicial ou autorização de órgão de governo.

Quando os dados do sistema de informação estão sob controle de terceiros e não são acessíveis em razão do cumprimento de sigilo legal ou por aplicação de confidencialidade decorrente de seus interesses próprios, **será necessário obter ordens judiciais para que tais informações sejam divulgadas.**

Dentre as provas que necessitam de ordens específicas para acesso, **temos os dados de identificação de usuários da internet, que são formados pela obtenção dos registros de acesso à aplicação de internet para se descobrir o endereço IP+porta lógica de acesso, data e hora de uso do serviço respectivo,** para em seguida requerer ordem judicial para **divulgação dos dados pes-**

soais do usuário correspondente, utilizando como parâmetros os dados obtidos pelo provedor de aplicação.

Conforme com o já exposto no capítulo 6, há obrigação de guarda dos registros de acesso à aplicação de internet por 6 (seis) meses por seu controlador e de acordo com o artigo 13 da referida lei, há dever de armazenamento de registros de acesso à conexão de internet pelos provedores de conexão por 1 (um) ano:

“Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.”

Portanto, para se identificar o real usuário de internet que praticou determinada ação, deve-se seguir o disposto no artigo 22 e incisos da Lei nº 12.965 de 2014, o Marco Civil da Internet, que prevê condições objetivas para que a divulgação seja realizada, quais sejam **as demonstrações de ocorrência de atos ilícitos, legitimidade para obtenção de tais dados e o período que correspondem.**

“Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.”

O pedido judicial deve ter caráter de urgência em razão da volatilidade de tais dados, sobretudo pelo lapso temporal na obtenção da sentença e o prazo de guarda definido no Marco Civil, que pode impossibilitar a produção da prova, 1 (um)

ano para os registros de conexão e 6 (seis) meses para as aplicações.

Por fim, deve-se solicitar sigredo de justiça em tais procedimentos, vez que informações sigilosas serão inseridas no processo e não devem estar abertas ao acesso público, conforme artigo 23 do Marco Civil da Internet, que complementa o artigo 189, III do Código de Processo Civil já exposto:

“Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar sigredo de justiça, inclusive quanto aos pedidos de guarda de registro.”

Admitindo que tal etapa esteja superada, ou seja, a Instituição Financeira possui acesso legítimo às informações que deseja utilizar como prova, deve-se analisar em seguida a **disponibilidade** da prova, isto é, a capacidade de estar acessível quando sua utilização for pretendida.

Quando os dados e informações estiverem sob controle e supervisão de terceiros, deve-se avaliar a capacidade de aquisição de tais dados em seu formato original por quem tem acesso

a eles para preservação adequada das evidências.

Na hipótese de **existir aquisição dos dados em seu formato original**, temos como exemplo o descarregamento de arquivos diretamente da internet, o que prova sua data de criação, hash e assinaturas digitais disponíveis, além do formato nativo estar preservado para eventuais perícias que sejam necessárias.

Algumas aplicações de internet permitem tal atividade, em que é possível realizar aquisição da prova por meio da própria interface computacional, como acontece com os **e-mails**, em **que é possível obter o arquivo da mensagem diretamente do serviço que utiliza a internet**, seja por cliente específico que é executado no dispositivo ou por acesso via *website*.

A aquisição do documento original é possível sempre que a aplicação disponibilizar a função de 'gravar', 'baixar', 'descarregar', 'salvar', 'salvar como' ou comando similar, caso contrário poderá ser necessário programa auxiliar para fazê-lo.

Contudo, algumas aplicações não permitem tal aquisição por padrão, a exemplo de envio e reprodução vídeos, ou ainda, de páginas de conteúdo geradas por mídias sociais, cuja forma-

ção é dinâmica, pois a exibição das informações depende de resultados de algoritmos contidos no código-fonte que são resolvidos em tempo real.

De tal sorte, pode ser necessário utilizar programas auxiliares para se extrair o conteúdo desses ambientes, mas ainda assim a garantia de integridade do que se capturou em relação ao que lá estava não estará livre de dúvidas.

Por isso, **se recomenda que terceiros com fé pública registrem tais ocorrências, uma vez que a percepção do conteúdo em determinada posição do tempo é medida que garante a integridade do estado de dados naquele momento específico.**

Este fator é agravado pelo controle dos dados e informações estar submetido a terceiro, portanto, **sua disponibilidade será incerta, pois a qualquer tempo os dados podem ser perdidos ou simplesmente terem ficado indisponíveis pelas mais diversas circunstâncias, e então, haver comprometimento da prova.**

Além deste fator de risco, **há a possibilidade de alteração dos dados ou informações por seus proprietários, em que não será possível restauração do estado anterior para constatação do que pretendia alegar em tempo real**, sendo o exemplo mais clássico a publicação de conteúdos por meio da internet.

Por isso, é possível identificar **cenário similar a de dados voláteis** (vide capítulo 4), isto é, **o transcurso do tempo pode comprometer o estado dos dados que se pretende preservar**, sobretudo pelas operações de sobrescrição ou capacidade de alteração que são particulares ao meio onde as informações estão presentes.

Nesses casos, é imprescindível que haja o registro da exata condição prova e seu teor em determinada posição do tempo para que sua fidedignidade não seja questionada caso exista alteração posterior.

A legislação prevê dois recursos de documentação de fatos com fé pública, a saber:

- A Ata Notarial:

Ato de o tabelião de notas registrar determinada ocorrência de fatos com fé pública, de acordo com o artigo 6º, III e o artigo 7º, III da lei nº 8.935 de 1994:

“Art. 6º Aos notários compete: (...)

III - autenticar fatos.”

“Art. 7º Aos tabeliões de notas compete com exclusividade: (...)

III - lavrar atas notariais;”

Este procedimento inclui o registro do conteúdo dos fatos que foram autenticados, o que permite a visualização posterior do que foi retratado na Ata, permitindo que haja plena compreensão a quem tal documento for apresentado.

- O Registro Público de Documento particular:

Ato de o tabelião registrar determinado documento a ele entregue ou disponibilizado, cuja transcrição de integral teor e registro de imagem daquilo que lhe foi apresentado reforçam a integridade da prova, de acordo com os artigos 142, 146 e 161, *caput* e § 1º da lei nº 6.015 de 1973:

“Art. 142. O registro integral dos documentos consistirá na trasladação dos mesmos, com a mesma ortografia e pontuação, com referência às entrelinhas ou quaisquer acréscimos, alterações, defeitos ou vícios que tiver o original apresentado, e, bem assim, com menção precisa aos seus característicos exteriores e às formalidades legais, podendo a transcrição dos documentos mercantis, quando levados a registro, ser feita na mesma disposição gráfica em que estiverem escritos, se o interessado assim o desejar.”

“Art. 146. Apresentado o título ou documento para registro ou averbação, serão anotados, no protocolo, a data de sua apresentação, sob o número de ordem que se seguir imediatamente, a natureza do instrumento, a espécie de lançamento a fazer (registro integral ou resumido, ou averbação), o nome do apresentante, reproduzindo-se as declarações relativas ao número de ordem, à data, e à espécie de lançamento a fazer no corpo do título, do documento ou do papel.”

“Art. 161. As certidões do registro integral de títulos terão o mesmo valor probante dos originais, ressalvado o incidente de falsidade destes, oportunamente levantado em juízo.

§ 1º O apresentante do título para registro integral poderá também deixá-lo arquivado em cartório ou a sua fotocópia, autenticada pelo oficial, circunstâncias que serão declaradas no registro e nas certidões.”

Neste procedimento o Cartório armazenará o documento digitalizado permanentemente, estando apto a emitir certi-

dão atestando a veracidade do que lhe foi trazido para registro.

Entretanto, na impossibilidade de realização de quaisquer desses atos de registro, **como contingência é possível que se realize a captura de tela de eventual interface gráfica, seja pelo próprio dispositivo, ou com câmera externa registrando os fatos e com indicação de data e hora, preferencialmente.**

Como vimos, **a integridade das provas é presumida como verdadeira, devendo ser demonstrado que houve violação ou falta de correspondência com os fatos para que perca seu valor, não bastando sua mera alegação para que seja considerada falsa.**

No entanto, pela condição de inversão do ônus da prova que a Instituição pode estar sujeita, por padrão deve-se sempre adotar procedimento mais seguro para a produção da prova e, caso impossível, realizar o registro na forma contingencial.



A FORMA DE APRESENTAÇÃO DA PROVA DIGITAL

De acordo com o já exposto no capítulo 2, **os documentos digitais são formados em linguagem própria para reconhecimento do respectivo sistema de informação, não sendo factível sua apresentação em tais códigos para conhecimento de quem estiver dirigindo o processo administrativo ou judicial, por ficar de impossível compreensão.**

Por isso, **a lei conferiu os mesmos efeitos do documento original à reprodução ou digitalização destes para fins de prova**, resguardando eventuais questionamentos de falsidade ou falta de autenticidade que também estiverem legalmente previstos e permitindo a conversão de interfaces para o processo, seja do documento físico para o processo digital ou do documento digital para o processo físico.

Então, **é adequado apresentar a forma final de como tais arquivos foram processados e ficaram aptos à visualização por parte do usuário respectivo, ou seja, a exibição da imagem, do áudio, vídeo ou texto, pois estarão aptos a cumprir com a função de demonstrar fatos de modo assimilável por quem os julgará.**

Quando existe limitação do formato a ser utilizado para apresentar a prova pela incapacidade de armazenar ou reproduzir o tipo de conteúdo que esta contém, deve-se utilizar outra forma de disponibilização para análise de quem julgará o expediente.

A Lei nº 11.419 de 2006, que regulamentou o processo eletrônico no Brasil, apresentou disposição que **na impossibilidade de juntar aos autos eletrônicos determinado documento ou evidência, seja pela sua extensão ou compreensão, o procedimento adequado deve ser a entrega no cartório correspondente para armazenamento físico para consulta às partes e magistrado**, nos termos de seu artigo 11, § 5º:

“Art. 11. (...)

§ 5º Os documentos cuja digitalização seja tecnicamente inviável devido ao grande volume ou por motivo de ilegitimidade deverão ser apresentados ao cartório ou secretaria no prazo de 10 (dez) dias contados do envio de petição eletrônica comunicando o fato, os quais serão devolvidos à parte após o trânsito em julgado.”

O Código de Processo Civil também deu orientações sobre como armazenar eventuais documentos que sejam relevantes ao processo no parágrafo segundo do artigo 425, em que podem ficar armazenados em cartório para posterior consulta do próprio juiz ou pelas partes mediante requerimento.

“Art. 425. (...)”

§ 2º Tratando-se de cópia digital de título executivo extrajudicial ou de documento relevante à instrução do processo, o juiz poderá determinar seu depósito em cartório ou secretaria.”

Isso se deve em virtude de os fatos se classificarem **como estáticos** ou **em movimento**, cuja representação pode depender de adaptação em razão do formato, isto é, sua captura pode acontecer de **modo único** ou **fracionado**.

Pela representação estática temos a imagem ou texto que podem estar contidos em trechos de registros de operações em sistemas, postagens em aplicações de internet, mensagens instantâneas ou e-mails, códigos fontes de programas ou de páginas de internet, comportamento indesejado de sistema por mensagens de erro, dentre outros.

Nesses casos, basta a representação do conteúdo determinado que consiste na prova para que haja percepção do que se pretende demonstrar ao julgador.

Contudo, **quando a informação que se pretende juntar estiver em movimento, seja áudio ou vídeo, será necessário realizar recortes para a refe-**

rência de conteúdos específicos em determinada posição de tempo reprodução, pois o formato de reprodução das interfaces pode ser estática.

Pela implantação do processo judicial digital é possível pressupor que quem o manuseia também está apto a acessar *links* de internet, dado que a maioria dos dispositivos digitais permite a visualização de arquivos salvos desta forma enquanto se verifica o teor do processo.

Assim, uma das formas a serem utilizadas para facilitar a visualização de determinado conteúdo é realizar **o arquivamento do documento na nuvem com o respectivo link para acesso e eventuais instruções de autenticação (caso o conteúdo seja sigiloso ou sensível)**, o que não dispensa a referência exata do que está contido em tal material nas alegações de fato que forem expostas.

Com apoio nesses recursos para facilitar a visualização dos fatos por quem tiver de julgar o processo, descreveremos as etapas a serem seguidas para produção, preservação e apresentação das provas de acordo com a situação.

- Informações de propriedade da Instituição Financeira ou sob sua custódia:
 - a) Capturar o estado das informações no sistema que forem exibidas na forma de:
 - Prints de tela; ou
 - Extração de relatórios.

b) Salvar tais informações no formato nativo em que o sistema de informação respectivo utiliza ou as exportar de modo que guarde referências confiáveis de auditoria das operações realizadas;

c) Obter os *logs* de operação do determinado sistema que comprovem a ocorrência dos fatos descritos no ambiente informático e que lhes deem sustentação;

d) A guarda dos arquivos acima deve ser seguida da função *hash* para atestar sua integridade quando apresentados como provas, além de implantar regras de limitação de acesso a terceiros não autorizados, utilização de senha ou recursos de criptografia para evitar modificação ou exclusão indesejadas;

e) Apresentar os documentos listados em a) e c) no processo respectivo indicando a correlação com os fatos, suas causas e possíveis resultados com o direito que se busca e mantendo os demais documentos listados em b) para comprovar eventual questionamento de autenticidade e integridade.

São exemplos destes documentos:

- Registros de operações nos sistemas da Instituição Financeira que não descrevam operações de prestação de serviços de crédito, financeiras, dentre outros tipos;
- E-mails trocados entre a Instituição Financeira clientes e não clientes que não descrevam detalhes particula-

res de operações de prestação de serviços de crédito, financeiras, dentre outros tipos;

- Gravações de vídeo e registros fotográficos em suas dependências;
- Registros de atendimento ao público (clientes ou não);
- Textos, imagens, vídeos, áudios e demais conteúdos publicados nas aplicações de internet da Instituição ou por elas acessíveis.
- Informações **sigilosas** de propriedade da Instituição Financeira ou sob sua custódia:

a) Todas as medidas anteriores deverão ser aplicadas, com exceção à letra 'e)', pois dependerá de o sigilo ser decretado no processo, com fundamento no artigo 189 do Código de Processo Civil:

“Art. 189. Os atos processuais são públicos, todavia tramitam em segredo de justiça os processos: (...)

III - em que constem dados protegidos pelo direito constitucional à intimidade;”

Se já houver segredo de justiça aplicado ao processo, pode haver juntada das provas que possuem caráter sigiloso, pois o acesso a terceiros estará resguardado.

Contudo, se não houver tal condição aplicada ao processo físico, recomenda-se o pedido de sigilo em caráter emergencial para que as provas a serem apresentadas não tenham o sigilo comprometido e não se opere a preclusão consumativa.

Se não existir decisão sobre esse pedido ao tempo de juntada da prova, recomenda-se que os documentos sigilosos estejam lacrados em envelope com selo de integridade, cuja abertura somente será possível caso o pedido for deferido pelo magistrado, para posterior guarda em pasta própria.

Por outro lado, se o processo for digital a própria interface do sistema já deve possibilitar ao usuário indicar o encaminhamento de documento sigiloso ou aplicação de sigilo de justiça ao processo.

Caso essa opção não exista e mesmo após provocação de emergência o juiz não decida a tempo de juntada da prova, deve-se depositar o documento em cartório utilizando o envelope lacrado com selo de integridade a ser aberto somente em caso de deferimento para posterior guarda em pasta própria.

Todo cuidado é mínimo para a Instituição Financeira utilizar informações sigilosas que detém poder, uma vez que será ela a dar visibilidade a tais dados no processo.

Além disso, somente deverão ser utilizadas informações ou dados sigilosos

perante pessoa que lhe diz respeito, não sendo recomendado o uso de informações sigilosas de uma pessoa em litígio ou expediente administrativo que não tiver qualquer relação.

São exemplos destes documentos:

- Registros de operações de crédito ou financeiras nos sistemas da Instituição Financeira (*logs*);
- Descritivo de operações de crédito ou financeiras realizadas nos sistemas da Instituição;
- E-mails trocados entre a Instituição Financeira e seus clientes que contenham dados e detalhes bancários, de operações financeiras e outros serviços;
- Registros de acesso à aplicação de internet (*logs*), ainda que hospedados em nuvem;
- Dados pessoais e de cadastro dos clientes;
- Documentos enviados por seus clientes.
- Informações constantes em sistemas de informação sob controle de terceiros:
 - a) Se acessíveis, capturar o estado das informações no sistema que forem exibidas, incluindo registros de data e hora de ocorrência (além do fuso respectivo), identificação do usuário que praticou os atos (ao menos visualmente) na forma de:
 - Prints de tela; ou
 - Extração de relatórios.

b) Salvar tais informações no formato nativo em que o sistema de informação respectivo utiliza ou as exportar de modo que guarde referências confiáveis de auditoria das operações realizadas;

c) A guarda dos arquivos acima deve ser seguida da função *hash* para atestar sua integridade quando apresentados como provas, além de implantar regras de limitação de acesso a terceiros não autorizados, utilização de senha ou recursos de criptografia para evitar modificação ou exclusão indesejadas;

d) Apresentar os documentos listados em a) no processo respectivo indicando a correlação com os fatos, suas causas e possíveis resultados com o direito que se busca e mantendo os demais documentos listados em b) para comprovar eventual questionamento de autenticidade e integridade.

São exemplos destes documentos:

- Textos, imagens, vídeos, áudios e demais conteúdos publicados nas mais variadas aplicações de internet, a exemplo de blogs, mídias sociais, fóruns de discussão, páginas ou aplicativos e programas que exibam tais conteúdos.

- Informações **sigilosas** constantes nos sistemas de informação sob controle de terceiros:

a) Caso os dados não estejam acessíveis em virtude da obrigação de confidencialidade ou por mera liberalidade

do proprietário da informação, antes dos procedimentos acima indicados deve-se buscar sua obtenção pela via judicial adequada e com auxílio de advogados da confiança da Instituição Financeira para tanto, justificando a pertinência, validade jurídica e relevância no acesso a tais informações para uso em eventual processo judicial ou administrativo;

b) Obtido o acesso às provas, será possível utilizá-las de acordo com a intenção da parte que as requereu bastando a demonstração de que tais informações foram fornecidas com ordem judicial respectiva e cujo motivo se manteve para legitimidade no uso;

c) Em razão da utilização de dados e informações que tiveram o sigilo mitigado para o uso da parte, a Instituição Financeira deverá requerer sigilo no feito que for apresentar tais provas, nos mesmos moldes já descritos na 'Conteúdo sigiloso obtido pelos próprios sistemas de informação da Instituição Financeira'.

São exemplos destes documentos:

- Registros de conexão à internet;
- Registros de acesso às aplicações de internet (*logs*);
- Mensagens trocadas entre usuários em aplicações de internet;
- Dados pessoais registrados em aplicações de internet.



**CHECK-LIST PARA PRODUÇÃO
DE PROVAS SEGUINDO
AS REGRAS DE
COMPLIANCE
EM VIGOR**

As regras de produção de provas em conformidade com a legislação em vigor apresentadas ao longo deste Guia foram organizadas na forma de *check*

list para facilitar a visualização e aplicação dos controles adequados pela Instituição Financeira.

CONTROLES PARA PRODUÇÃO DE PROVAS ATENDENDO ÀS NORMAS VIGENTES		
1	Estabelecer sistemas de informação confiáveis (base computacional confiável + canais de transmissão e processamento de dados confiáveis)	<input type="checkbox"/>
2	Logs com acesso restrito e com atributos nativos de somente leitura, não podendo ser alterados, sob nenhuma hipótese	<input type="checkbox"/>
3	Guardar logs de operação por 5 (cinco) ou 10 (dez) anos, conforme o caso específico (capítulo 6)	<input type="checkbox"/>
4	Os sistemas possuem diretivas de acesso para cada tipo de usuário (<i>need to know</i> e <i>least privilege</i>), protegendo os documentos eletrônicos e informações contra o acesso, o uso, a alteração, a reprodução e a destruição não autorizados garantindo que a prova eletrônica apresentada não sofreu adulteração desde sua criação;	<input type="checkbox"/>
5	Os sistemas possuem controles de permissões adequados com as diretivas de acesso (<i>need to know</i> e <i>least privilege</i>) e não podem ser revogados por usuários que não sejam administradores;	<input type="checkbox"/>
6	Os sistemas possuem controles de proteção à toda estrutura, compreendendo registros de acesso das atividades de permissões, travas contra alteração de metadados de arquivos e registros de atividade por quaisquer usuários ou exigência de dupla ou tripla autenticação para tarefas destinadas aos administradores.	<input type="checkbox"/>
7	Os sistemas possuem mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor	<input type="checkbox"/>
8	Os sistemas possuem recursos destinados a preservar a integridade, a confiabilidade, a autenticidade, a segurança e o sigilo das transações realizadas	<input type="checkbox"/>

CONTROLES PARA PRODUÇÃO DE PROVAS ATENDENDO ÀS NORMAS VIGENTES

9	Os sistemas possuem mecanismos de salvaguarda, a exemplo da produção de cópia de segurança das informações e dos documentos eletrônicos	<input type="checkbox"/>
10	Os sistemas possuem mecanismos de rastreamento e auditoria dos procedimentos e das tecnologias empregados no processo	<input type="checkbox"/>
11	Os sistemas exigem autenticação forte pelo utilização de seus usuários (ao menos dois fatores e com emissão supervisionada para evitar fraudes de emissão)	<input type="checkbox"/>
12	Construção de sistemas de informação aptos a gerar relatórios detalhados para identificar operações realizadas pelos usuários internos da Instituição e seus clientes vinculados com registros de acesso à aplicação e utilizando função <i>hash</i>	<input type="checkbox"/>
13	Criação de inventário capaz de registrar o acesso aos registros de acesso a aplicações na forma de inventário, indicando qual usuário acessou qual arquivo de log, em que data, hora, fuso horário e por quanto tempo o fez	<input type="checkbox"/>
14	Registros de acesso de aplicações de internet (<i>logs</i>) contendo identificação do usuário, data, hora, IP+porta lógica de acesso, dados de dispositivo utilizado e geolocalização, se possível	<input type="checkbox"/>
15	Obtenção de consentimento do usuário para guarda de dados pessoais, dados de seu dispositivo e geolocalização	<input type="checkbox"/>
16	Efetuar a guarda de documentos que darão sustentação a eventuais publicidades por 5 (cinco) anos após seu último dia de veiculação	<input type="checkbox"/>
17	Dados em repouso devem ser armazenados criptografados com chaves simétricas fortes (AES-256 ou Twofish)	<input type="checkbox"/>
18	Dados em trânsito devem ser protegidos com chaves assimétricas fortes (SHA-384 ou 512)	<input type="checkbox"/>
19	Executar função hash nos documentos apresentados pelo cliente ou de procedimentos que executar nas aplicações oferecidas pela Instituição Financeira	<input type="checkbox"/>

**CHECK-LIST PARA COLETA E USO
DE PROVAS DE ACORDO COM A SITUAÇÃO
PRÁTICA ENFRENTADA PELA**

INSTITUIÇÃO FINANCEIRA

Como possíveis roteiros para produção de provas em casos específicos in-

dicamos o *check list* abaixo para ilustrar os procedimentos a serem realizados:

A – QUESTIONAMENTO DE AUTENTICIDADE NA TRANSAÇÃO PELO CLIENTE – USO DE APLICAÇÃO DE INTERNET

Objetivo: Provar que o cliente era quem se dizia ser na operação contestada ou que houve sua culpa exclusiva pelo prejuízo sofrido

1	Criar pasta específica para armazenar as informações reunidas do cliente respectivo	<input type="checkbox"/>
2	Coletar os <i>logs</i> de autenticação e acesso contendo o endereço IP, data, hora e fuso	<input type="checkbox"/>
3	Apresentar as condições de segurança e confiabilidade de autenticidade e integridade que foram adotadas pelo sistema no processo	<input type="checkbox"/>
4	Expor os elementos de autenticação biométrica ou de dupla autenticação que foram utilizados para confirmar a identidade do usuário	<input type="checkbox"/>
5	Coletar os dados do dispositivo utilizado e comparar com das transações anteriores para verificar padrão e constatar como transação genuína	<input type="checkbox"/>
6	Buscar dados e informações da operação combatida e das previamente realizadas para identificar padrão e constatar como transação genuína	<input type="checkbox"/>
7	Buscar dados e informações de transações passadas para identificar padrão	<input type="checkbox"/>
8	Apresentar documentos pessoais que forem submetidos eletronicamente à Instituição Financeira além de procedimentos específicos com o resultado da função <i>hash</i> aplicada no momento de recebimento de tais documentos ou na prática dos atos e comparados com o momento de apresentação da prova, demonstrando total integridade	<input type="checkbox"/>
9	Buscar dados de provedor de conexão a partir dos endereços de IP constantes nos <i>logs</i> de acesso	<input type="checkbox"/>
10	Apresentar as provas e realizar a defesa ou ingressar com medida punitiva contra quem se fez passar pelo cliente, requerendo sigilo no processo	<input type="checkbox"/>

B – QUESTIONAMENTO DE AUTENTICIDADE NA TRANSAÇÃO PELO CLIENTE – USO DE TERMINAL DE AUTO ATENDIMENTO (ATM)

Objetivo: Provar que o cliente era quem se dizia ser na operação contestada ou que houve sua culpa exclusiva pelo prejuízo sofrido

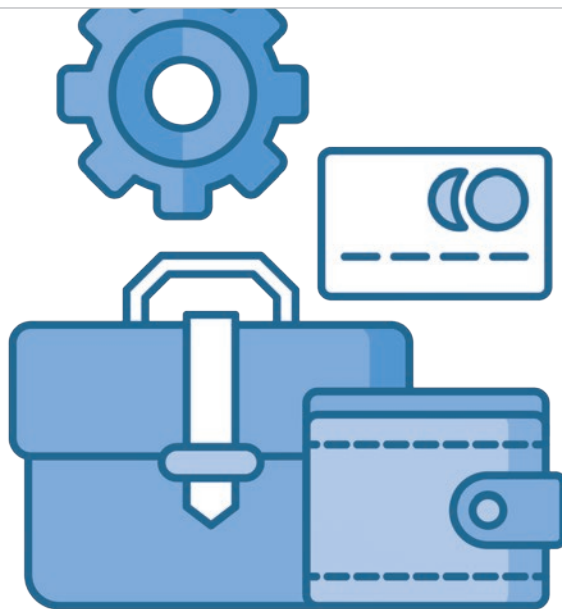
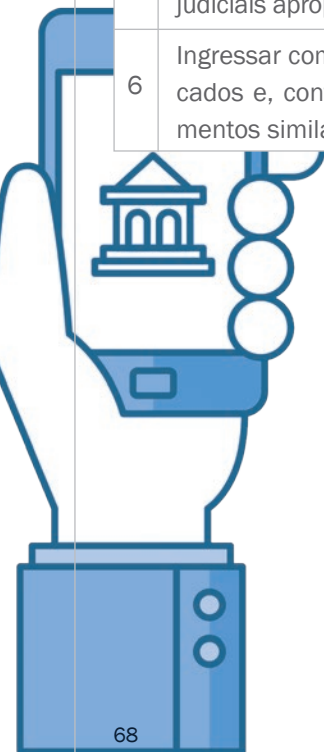
1	Criar pasta específica para armazenar as informações reunidas do cliente respectivo	<input type="checkbox"/>
2	Apresentar as condições de segurança e confiabilidade de autenticidade e integridade que foram adotadas pelo sistema no processo	<input type="checkbox"/>
3	Coletar os <i>logs</i> de autenticação e acesso	<input type="checkbox"/>
4	Apresentar os elementos de autenticação biométrica ou de dupla autenticação que foram utilizados para confirmar a identidade do usuário	<input type="checkbox"/>
5	Buscar dados e informações da operação combatida e das previamente realizadas para identificar padrão e constatar como transação genuína	<input type="checkbox"/>
6	Buscar imagens do ambiente que estava o terminal e do usuário no momento da operação para identificar quem o operava, se possível	<input type="checkbox"/>
7	Apresentar as provas e realizar a defesa ou ingressar com medida punitiva contra quem se fez passar pelo cliente, requerendo sigilo no processo	<input type="checkbox"/>



C – IDENTIFICAÇÃO DE CONTEÚDO DIFAMATÓRIO CONTRA A INSTITUIÇÃO OU QUE A PREJUIQUE

Objetivo: Retirar o conteúdo infringente e buscar indenização e restrição para publicações futuras de mesmo teor ou intenção danosa

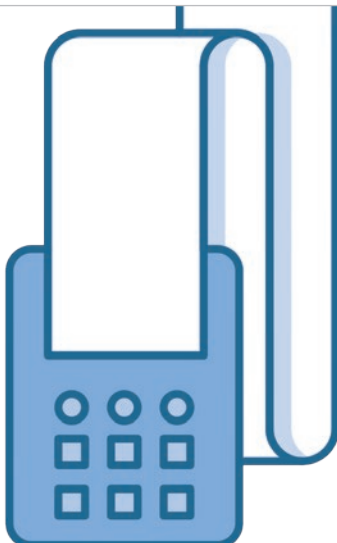
1	Criar pasta específica para armazenar as informações reunidas do incidente respectivo	<input type="checkbox"/>
2	Coletar o conteúdo infringente com prints de tela e salvando o arquivo que os contém no formato nativo	<input type="checkbox"/>
3	Lavrar Ata Notarial ou efetuar Digitalização Registrada sobre o que é exibido	<input type="checkbox"/>
4	Ingressar com medida judicial solicitando a remoção dos conteúdos e a entrega dos registros de acesso da aplicação do usuário que submeteu o material com ordens judiciais apropriadas	<input type="checkbox"/>
5	Solicitar os registros de conexão à internet do provedor correspondente aos dados de acesso à aplicação recebidos anteriormente com ordens judiciais apropriadas	<input type="checkbox"/>
6	Ingressar com medidas de indenização contra os responsáveis identificados e, conforme o caso, requerer medida inibitória para comportamentos similares	<input type="checkbox"/>



D – COMBATE A FRAUDES PRATICADAS CONTRA A INSTITUIÇÃO FINANCEIRA

Objetivo: Buscar ressarcimento pelo prejuízo sofrido pela Instituição e/ou punição de quem executou as fraudes

1	Criar pasta específica para armazenar as informações reunidas do incidente respectivo	<input type="checkbox"/>
2	Coletar os <i>logs</i> de autenticação e acesso	<input type="checkbox"/>
3	Apresentar os elementos de autenticação biométrica ou de dupla autenticação que foram utilizados para confirmar a identidade do usuário	<input type="checkbox"/>
4	Buscar dados e informações da operação combatida e das previamente realizadas para identificar padrão e constatar como transação genuína	<input type="checkbox"/>
5	Ingressar com medida judicial solicitando a quebra de sigilo de e-mails ou mensagens trocadas a partir de determinado serviço que foi utilizado para executar a fraude além da entrega dos registros de acesso da aplicação do usuário que submeteu o material com ordens judiciais apropriadas	<input type="checkbox"/>
6	Solicitar os registros de conexão à internet do provedor correspondente aos dados de acesso à aplicação recebidos anteriormente com ordens judiciais apropriadas	<input type="checkbox"/>
7	Ingressar com medidas de indenização contra os responsáveis identificados e/ou fornecer tais dados na instauração de inquérito policial	<input type="checkbox"/>



REFERÊNCIAS BIBLIOGRÁFICAS

(ISC)². *Official (ISC)² GUIDE TO THE CISSP CBK, 4th Edition*. Taylor & Francis Group: 2015, Boca Raton.

Associação Brasileira de Normas Técnicas. *Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação*. São Paulo, 2011.

Associação Brasileira de Normas Técnicas. *Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação*. São Paulo, 2013.

BUENO, Cassio Scarpinella. *Curso sistematizado de direito processual civil: v.2, tomo I. procedimento comum: ordinário e sumário*. 7 ed. São Paulo: Saraiva, 2014.

BUZAID, Alfredo. Do ônus da prova. In *Revista da Faculdade de Direito da Universidade de São Paulo*. São Paulo. v. 57, 1962. P. 113-140. Disponível em < <http://www.revistas.usp.br/rfdusp/article/viewFile/66398/69008> > Acessado em 14 abr 2016

CASEY, Eoghan. *Digital Evidence and Computer Crime*. Waltham: Elsevier, 2011.

CHIOVENDA, José. *Principios de derecho procesal civil*. Tomo I. 3 ed. Tradução de José Casáis y Santaló. Madri: Editorial Reus S.A., 1922.

COUTO, Camilo José D'Ávila. *Dinamização do ônus da prova: teoria e prática*. 2011. Tese (Doutorado em Direito) – Universidade de São Paulo, São Paulo, 2011

COUTURE, Juan Eduardo. *Fundamentos del derecho procesal civil*. 3 ed. Buenos Aires: Roque Depalma Editor, 1958

ECHANDÍA, Hernando Devis. *Teoria general de la prueba judicial*, tomo I. Buenos Aires: Victor P. de Zavalía, 1970.

GOODRICH, Michael; TAMASSIA, Roberto. In Introdução à segurança de computadores. Porto Alegre: Bookman Editora LTDA, 2013.

GRINOVER, Ada Pellegrini; BENJAMIN, Antonio Herman de Vasconcellos e; FINK, Daniel Roberto; FILOMENO, José Geraldo Brito; WATANABE, Kazuo; NERY JÚNIOR, Nelson; DENARI, Zeno. *Código brasileiro de defesa do consumidor: comentado pelos autores do anteprojeto*. 9. e.d. Rio de Janeiro: Forense Universitária, 2007

LEWIS, Theodore Gyle. Critical infrastructure protection in homeland security : defending a networked nation. Second Edition. Nova Jérсия: John Wiley & Sons, 2015.

MALAGÓ, Fábio Machado. *Distribuição dinâmica do ônus da prova*. 2014. Dissertação (Mestrado em Direito) – Universidade de São Paulo, São Paulo, 2014.

MATOS, Cecília. *Ônus da prova no código de defesa do consumidor*. 1993. 255 f. Dissertação (Mestrado em Direito) – Universidade de São Paulo, São Paulo, 1994.

NEVES, Daniel Amorim Assumpção. Manual de direito processual civil. 7. ed. rev., atual. e ampl. – São Paulo: MÉTODO, 2015.

PACÍFICO, Luiz Eduardo Boaventura. *O ônus da prova no direito processual civil*. São Paulo: Editora Revista dos Tribunais, 2001.

PINHEIRO, Patricia Peck. Direito Digital. 6ª ed. rev. atual. e ampl. São Paulo: Saraiva, 2016.

ROSEMBERG, Leo. *La carga de la prueba*. 2ed. Buenos Aires: BdF, 2002

STRINGHER, Ademar. Aspectos Legais da Documentação em Meios Micrográficos, Digitais e Eletrônicos. São Paulo: CENADEM, 2003.

THEODORO JÚNIOR, Humberto. *Curso de Direito Processual Civil*. Vol.1. 50ª ed. Rio de Janeiro: Editora Forense, 2009



Rua Líbero Badaró, 425 – 28º andar – São Paulo – SP
Tel.: (11) 3107-7177 Fax: (11) 3106-6082
www.acrefi.org.br