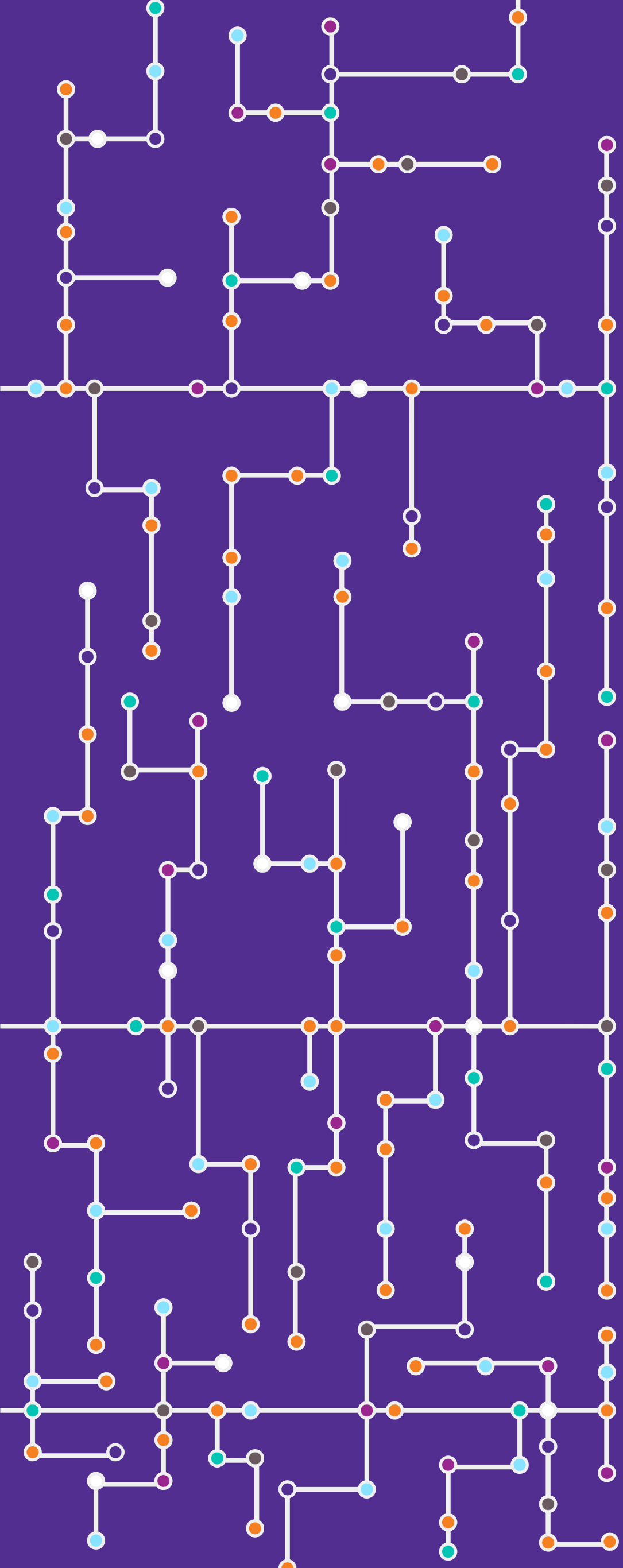
Segurança da Informação

[Cartilha de Boas Práticas para Advogados]

Comissão de Tecnologia e Inovação
[OAB - SP]

OAB SÃO PAULO
ITS



[Presidente]

Ronaldo Lemos

[Vice-Presidente]

Renato José Cury

[2° Vice-Presidente]

Renato Tadeu Rondina Mandaliti

[Secretária]

Celina Bottino

[Colaboração Especial]

José Antonio Milagre
Karina Kaehler Marchesin
Yuri Nabeshima

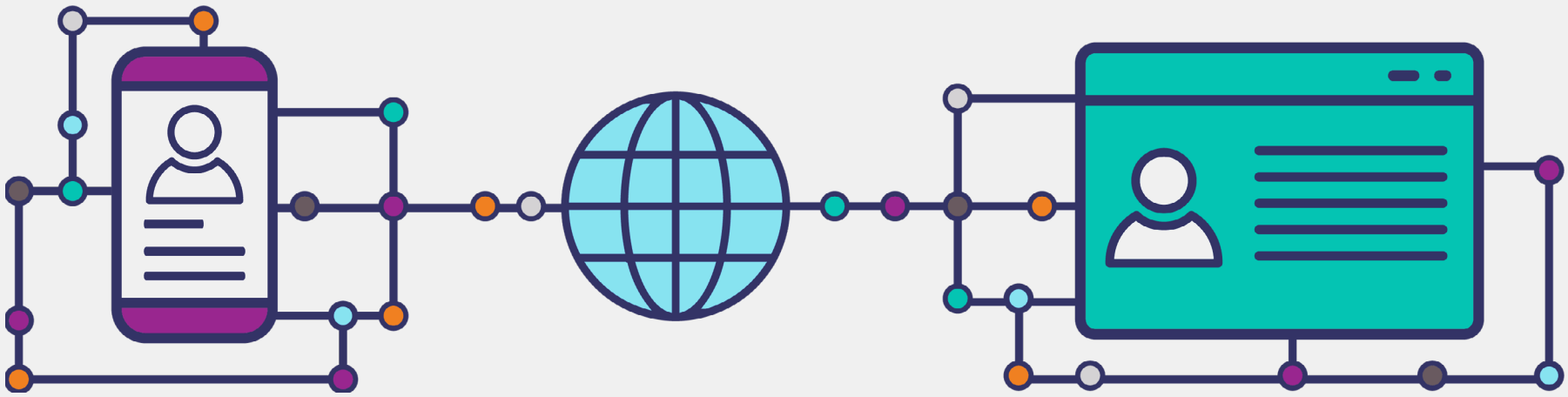
[Revisão]

Celina Bottino
Janaína Costa
Pedro Gueiros

[Diagramação e Ilustração]

Cecilia Quental

São Paulo
2023



[Identidade Digital]

A identidade digital está diretamente ligada a processos de autenticação de pessoas. E como se sabe, a autenticação é um processo indispensável para vida em sociedade. A todo o momento precisamos comprovar nossa identidade para usufruir de serviços públicos e privados, até mesmo nas atividades mais rotineiras, como votar, ingressar em um ambiente forense ou adentrar em salas de audiência (ainda que em uma audiência virtual). Para nós, operadores de Direito, comprovar a identidade é igualmente fundamental.

Identidade é, assim, o processo para se demonstrar que uma pessoa é de fato a que está se apresentando e obtendo serviços físicos ou virtuais. Quando em uma audiência, por exemplo, apresentamos a carteira da OAB, estamos através do documento, nos autenticando frente ao servidor da justiça. Com a carteira, ele poderá confirmar os dados e saber que estamos habilitados a praticar os atos de representação. De maneira bem simples, ao lado direito, podemos entender que:

[Identidade]

Conceito complexo e dinâmico, que envolve as subjetividades do indivíduo, que pode entender a si de maneiras muito diferentes.

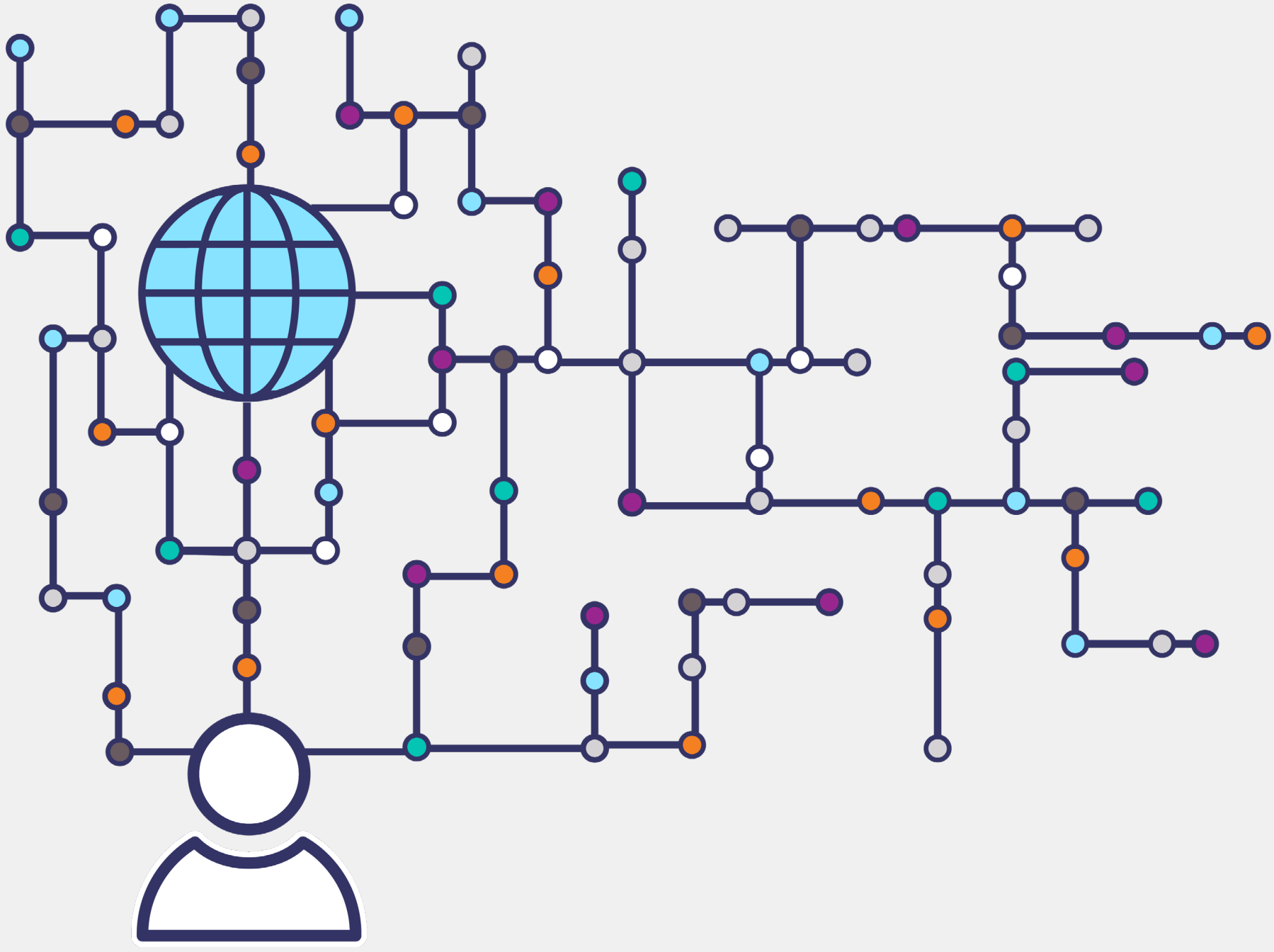
[Identificação]

Diz respeito ao processo de se identificar, em que uma pessoa atesta que a outra é quem ela diz ser.

[Credencial]

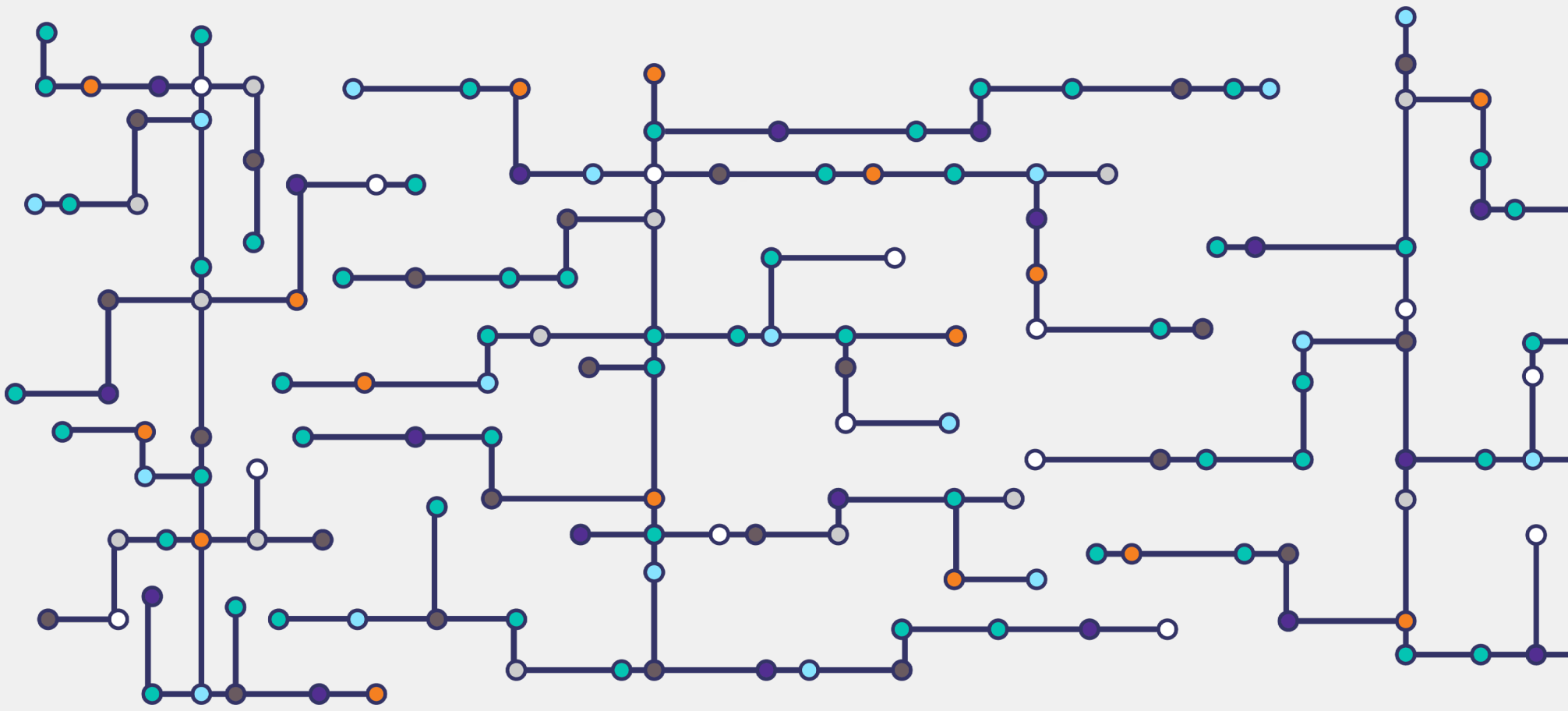
É o documento em si, ou seja, passaporte, carteira da OAB, RG, CPF, crachá, fichas de identificação, dados cadastrais etc..

Acredita-se que no futuro será possível nos autenticar nesses e em muitos outros serviços sem a necessidade de memorizar “senhas”, tudo, através da identidade digital. Mas, por ora, ter cuidado com elementos que formam nossa identidade digital é fundamental. **Imagine se alguém tem acesso aos dados de sua identidade, permitindo que entre em serviços públicos, de empresas, bancários ou até mesmo serviços jurídicos que deveriam ser seus? O que poderia acontecer? Grandes danos!**



Da mesma maneira que nos atentamos com documentos físicos que comprovam nossa identidade, também devemos ter cuidado com nossos dados, senhas, aplicativos de autenticação, *selfies* e assinaturas digitais, que, por excelência, atestam nossa identidade nos serviços online.

Não incomuns são os casos de advogados que tiveram comprometidos seus dados de *login* (acesso) a tribunais e atos foram praticados sem seu consentimento.
A exemplo, nos sites de alguns tribunais, é possível se autenticar apenas com um CPF e senha. Outros tribunais exigem a troca de documentos por e-mail. Nesses casos, o comprometimento desses dados pode permitir que pessoas se passem pelo advogado ou advogada na internet.



[Dicas importantes para proteger sua Identidade Digital]

— Não compartilhe dados e documentos além do necessário. Questione sempre a real necessidade de se compartilhar fotos de rosto, documentos ou demais dados;

— Questione o serviço e a empresa sobre qual segurança atribuem aos dados que serão compartilhados e com quem compartilham os dados;

— Jamais deixe suas senhas salvas em navegadores (repositório de senhas), evitando que terceiros que usem um computador compartilhado, acessem sites e serviços com sua identidade;

— Não compartilhe a chave privada ou o arquivo do seu certificado digital com terceiros. De posse do arquivo e da senha PIN, pessoas poderão praticar atos processuais em seu nome;

— Procure se atentar com o que compartilha online, em especial em serviços públicos e redes sociais;

— Pesquise sempre por seus dados em sites de buscas como o Google e, encontrando dados pessoais que podem ser usados para falsear sua identidade, solicite o apagamento desses dados e de sua pegada digital;

— Nos peticionamentos eletrônicos, apresente somente documentos necessários, e use os recursos, quando possível, para manter os documentos como “sigilosos”;

— Verifique sempre se o site do Tribunal de Justiça é, efetivamente, o site correto, e se a criptografia está ativada. Fique atento pois criminosos podem publicar sites falsos e clonados, inclusive indexando-os nos buscadores;

— Ative apenas *cookies* fundamentais no navegador. *Cookies* são pequenos pacotes de dados que são gerados por sites, gravados no computador do usuário e que são usados por outros sites para que lembrem de preferências dos usuários e até mesmo para autenticação em serviços. Criminosos podem sequestrar *cookies* e tentar autenticar serviços, como se fossem a vítima;

— Cuidado com sua carteira da OAB. Ela também é um token que permite autenticação em serviços de Tribunais;

— Altere suas senhas e o PIN do seu certificado digital pelo menos a cada 6 (seis) meses;

— Quando for compartilhar documentos físicos ou digitalizados, como cópia da sua carteira de identidade, carteira da OAB ou passaporte, você pode utilizar aplicativos que adicionam marca d’água onde pode informar o nome do aplicativo ou serviço que solicitou os documentos, como por exemplo “Registro válido para o Serviço TJ/SP”. Assim, fica mais difícil ao fraudador que eventualmente tenha acesso aos dados, utilizá-lo para outras finalidades.

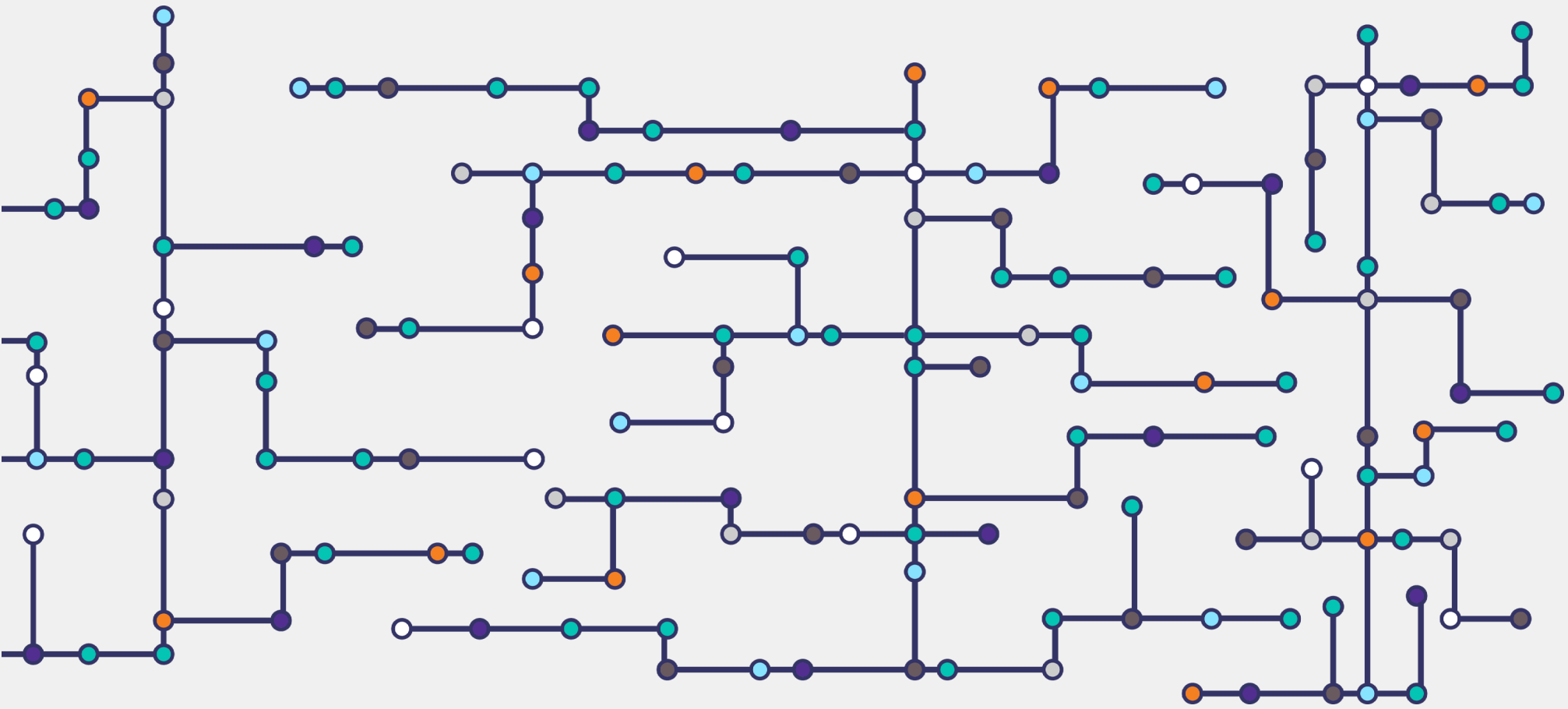
[Gestão de dados na prática]

Por que o advogado ou advogada deve se preocupar com a proteção dos seus dados pessoais? O cibercrime atinge uma receita de R$ 43 trilhões e se torna a terceira economia do mundo. Dentre os golpes mais praticados estão violação de dados, *phishing* ataques de *ramsomware* (sequestro de dados) e espionagem cibernética.

Especificamente em relação à advocacia, diariamente novos golpes surgem com vistas a prejudicar advogados e representados. Um dos golpes mais comuns é o do "falso advogado". Conforme a nota da OAB/SC, os golpistas entram em contato com clientes de escritórios de advocacia por meio de aplicativos e pedem dinheiro para o pagamento de serviços prestados, se passando por advogados e advogadas.

Em alguns casos ainda, os criminosos se passam por “atendentes dos tribunais”, e informam que os valores “foram liberados em determinado processo” e que para isso, o cliente precisa falar com seu “advogado”. Ao fazer contato acreditando que está falando com o advogado, o cliente acaba pagando para o fraudador, acreditando que estava pagando uma “taxa” para ter acesso aos valores do processo.

Esse é apenas um de inúmeros golpes que podem prejudicar clientes e advogados, razão pela qual preparamos orientações importantes para gestão de senhas e dados pessoais que comumente circulam por escritórios de advocacia. Fique atento às dicas e implemente imediatamente as medidas.



[Melhores práticas com gestão de senhas]

— Utilize senhas fortes como letras, números, caracteres especiais;

— Cuidado onde venha a salvar suas senhas. Evite papéis, blocos de notas. Prefira utilizar programas seguros para a custódia de senhas. Nesse site, podemos ver um dos melhores e mais seguros gerenciadores de senhas disponíveis;

— Prefira sempre se autenticar em serviços por meio do certificado digital (*token* ou arquivo .pfx) e não apenas com nomes de usuários e senhas;

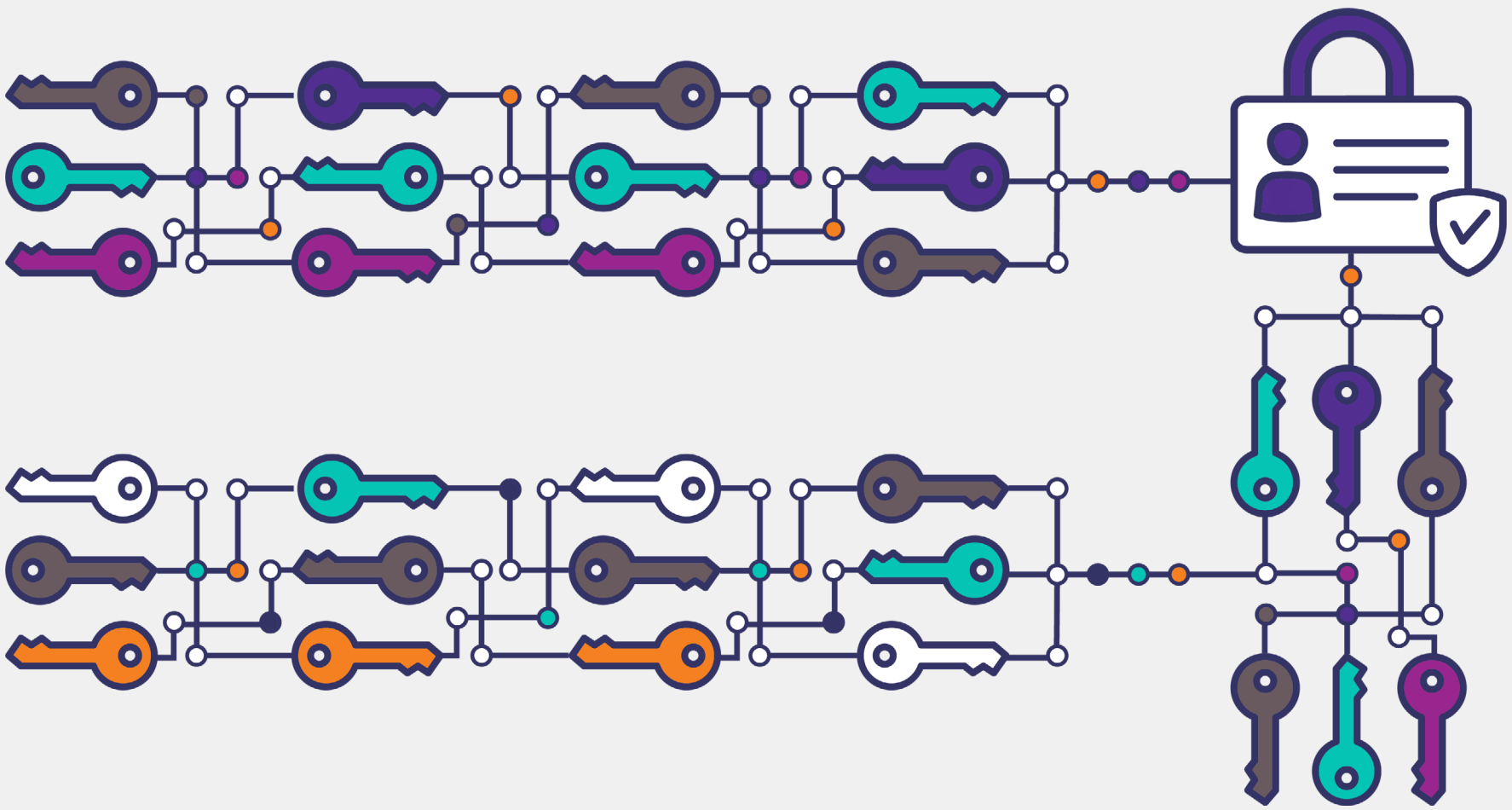
— Evite usar dados pessoais como CPF e número telefônico como chaves de PIX. Se for usar e-mail como chave, utilize um que não é autenticado em serviços e contas. Prefira as chaves aleatórias;

— Ative sempre a autenticação em duas etapas, não se contentando apenas com um único fator de autenticação, como nome de usuário e senha, mas no mínimo, dois fatores de autenticação, a exemplo: para acessar no serviço você precisa digitar o nome do usuário e senha e um código do seu aplicativo autenticador;

— Jamais confirme códigos ou links que receber por e-mail ou mensagens, em processos de autenticação que você não reconhece.

Para reforçar o aprendizado, é importante destacar que o NIST, órgão de padronização estadunidense, tem uma publicação muito interessante, denominada *Easy Ways to Build a Better P@$5w0rd* (Melhores caminhos para se fazer uma senha melhor). O documento fornece importantes dicas de proteção de senhas.

O mesmo órgão, ainda, tem uma norma técnica de número 800-63, que estabelece melhores práticas sobre identidade digital. Também vale a pena aprofundar nos estudos sobre como proteger sua identidade, senhas e dados pessoais.



[Melhores práticas na atuação jurídica]

— Não faça mais sua “assinatura física” em documentos do processo eletrônico. Estes documentos já foram assinados digitalmente;

— O advogado não precisa, via de regra, anexar documentos pessoais ao distribuir um processo;

— Classifique, sempre que possível, documentos pessoais do cliente como “Documentos sigilosos” ou alternativa similar;

— Procure “borrar” de documentos ou provas eventuais dados pessoais desnecessários à prova do ato (sempre que viável e informando ao juízo);

— Fique atento às situações em que pode pedir para que o processo tramite em segredo de justiça;

— Sempre que um processo segredo de justiça eventualmente for indexado em sites ou buscadores, com base em identificações em despachos no corpo do documento ou texto, informe o juízo para pseudonimização;

— Alguns sistemas, como o “PJ-e”, permitem saber o nome de outros advogados consultando os autos. Fique atento a quem, externo a relação processual, tem pesquisado seus processos;

— Adote um sistema jurídico que permita cadastro de usuários e permissionamento, impedindo que os dados de clientes sejam acessados por pessoas sem permissão no escritório de advocacia. Prefira um sistema que registre “*logs*” das atividades de usuários;

— Mantenha uma solução de *backup* (cópias de segurança) dos dados pessoais sempre ativas, evitando que em caso de destruição ou criptografia de dados, os mesmos possam ser recuperados. Proteja os *backups* com senhas ou outros recursos, evitando-se acesso indevido;

— Remova credenciais (e-mails, comunicadores e acesso a arquivos) de membros do corpo jurídico quando desligados do escritório e adote sistemas que adotam cópias indevidas de arquivos;

— Identifique os fluxos de dados pessoais do escritório e adote medidas para proteção e segurança destes dados;

— Caso seu escritório permita que o cliente consulte seu processo em "Área do cliente" no site, certifique-se que o site passou por um "teste" de intrusão que certifique que o mesmo não possui vulnerabilidades que possam ser exploradas por eventuais ataques;

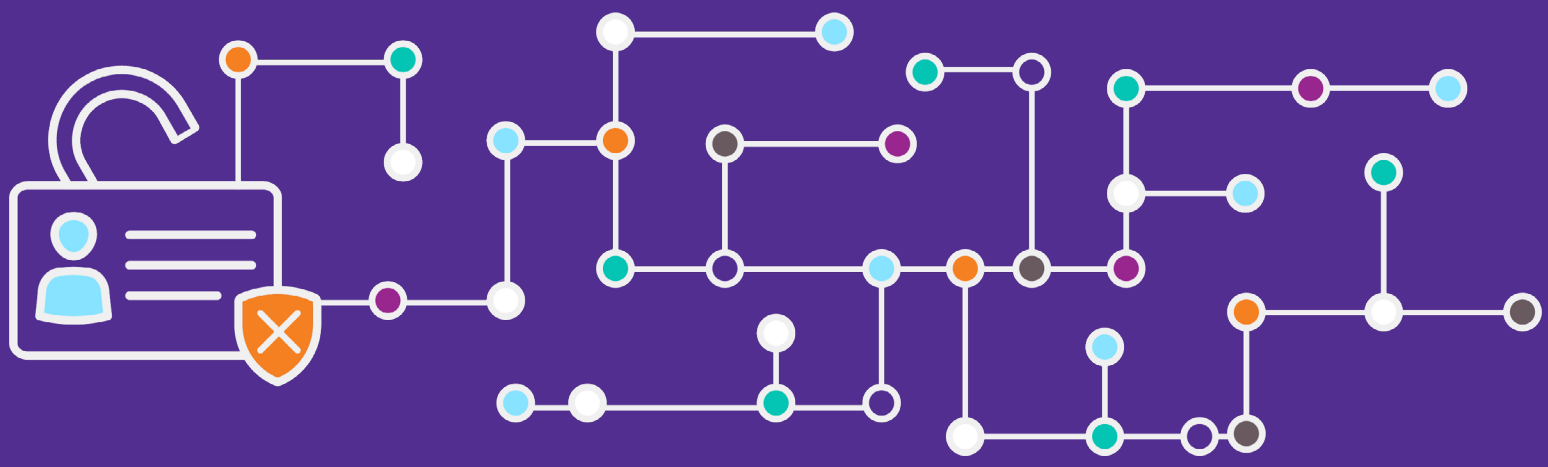
— Capacite constantemente o time jurídico para que conheçam as ameaças internas e externas e adotem posturas que fortaleçam a segurança de dados pessoais e de senhas;

— Considere a contratação de um seguro para casos ligados a vazamento de dados pessoais;

— Mantenha sistemas operacionais e softwares sempre originais, atualizados, incluindo antivírus e *antimalware*;

— Estabeleça as regras no tratamento de dados pessoais, por meio de políticas internas e procedimentos, às quais todos devem se vincular;

— Avalie periodicamente os controles de segurança do escritório, preferencialmente por meio de auditorias independentes.

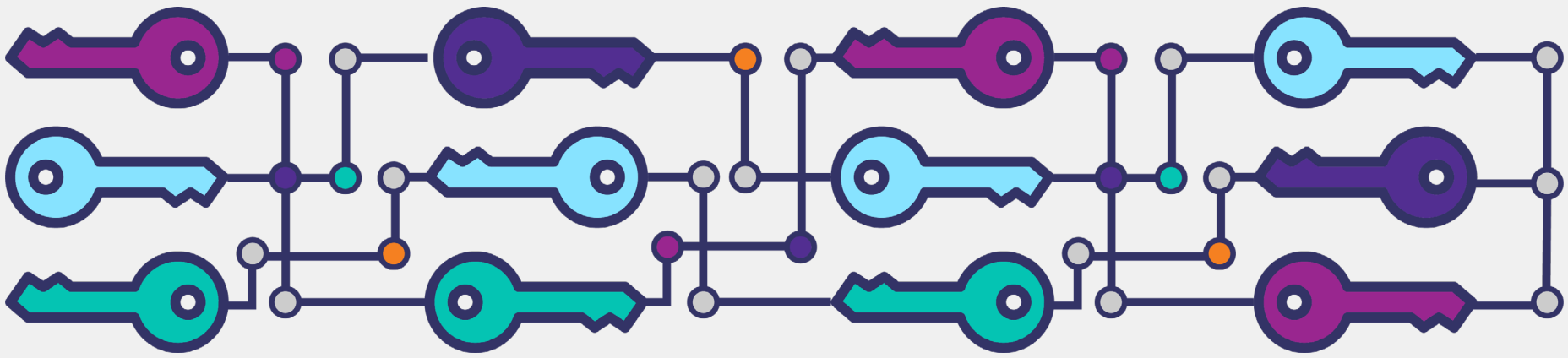


[Como descobrir se seus dados foram vazados?]

— A Avast disponibiliza um serviço muito útil, denominado Avast Check. Nele é possível ver rapidamente se a senha do seu e-mail foi vazada. Acesse o site, digite seu e-mail e clique em *"Check Now"*.

— Muitas vezes, pode ser muito simples identificar dados pessoais vazados. Uma simples pesquisa em buscadores de internet, como o Google, pode revelar muitas informações sobre dados pessoais comprometidos. Por outro lado, às vezes, os dados vazam na *dark web*, área da Internet não acessível por meios convencionais, ou mesmo em repositórios específicos.

— Assim, algumas ferramentas podem ajudar o titular de dados, advogado ou advogada, a descobrir usos indevidos de seus dados pessoais. Um serviço muito útil criado pelo Banco Central do Brasil é o Registrato. No site, é possível consultar empréstimos e financiamentos em seu nome, lista de bancos onde a pessoa tem conta ou outro tipo de relacionamento, consulta de chaves PIX cadastradas em bancos, dentre outras informações. O cadastro e uso são gratuitos.



[Chave Privada]

qual é sua importância?

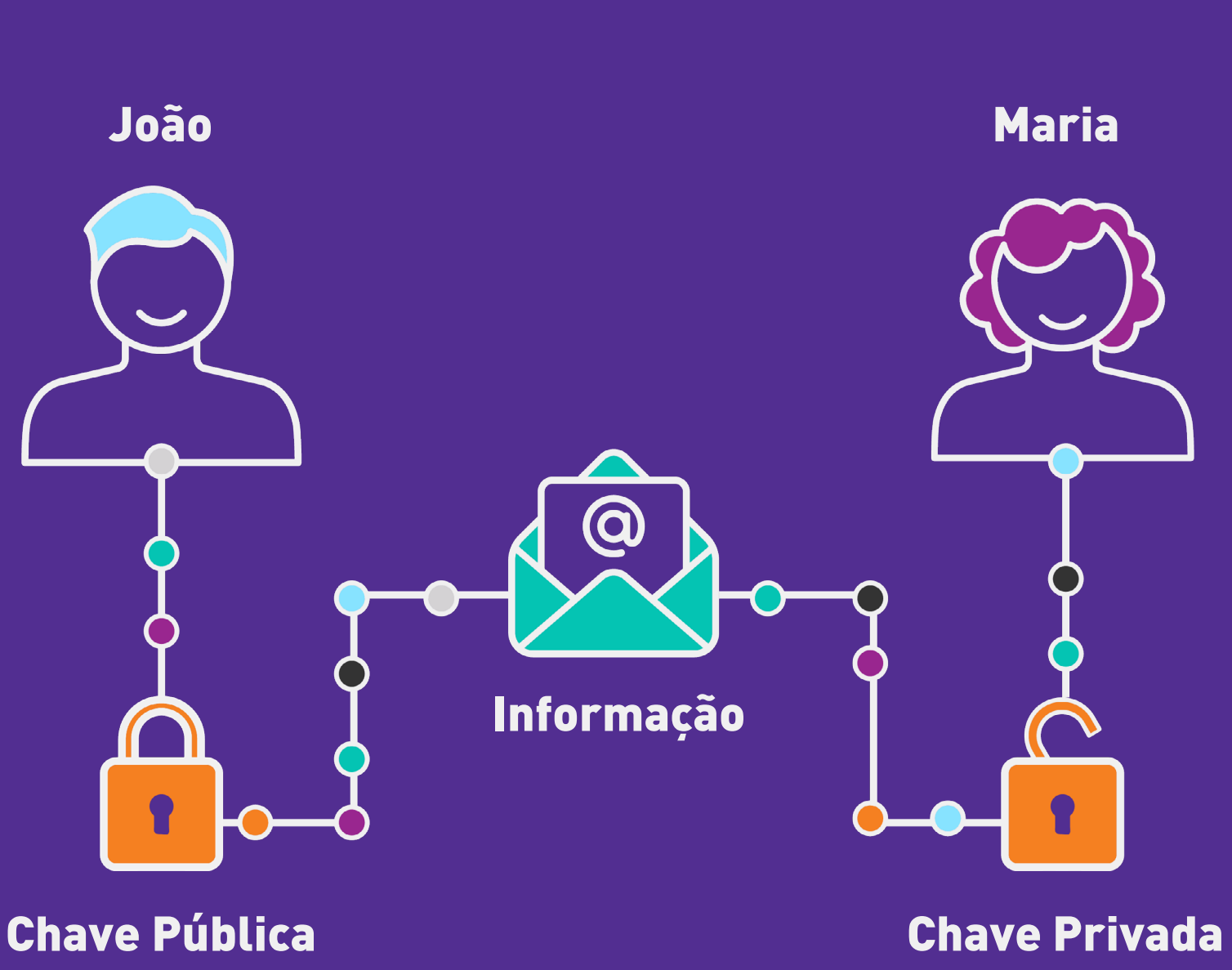
Para falarmos da importância da chave privada, é essencial compreender o que são as chaves públicas e privadas ou criptografia assimétrica.

Em linhas gerais, a criptografia de chave pública é qualquer sistema criptográfico que usa pares de chaves públicas, que indicam um determinado endereço a ser livremente divulgado ao público. Já as chaves privadas, são mantidas em sigilo e que são de conhecimento apenas de seu proprietário.

Tecnicamente falando, as chaves públicas e privadas consistem em uma sequência criptográfica de letras e números que permite aos usuários enviar mensagens, realizar transações de criptoativos, assinar documentos eletronicamente, dentre várias outras funcionalidades.

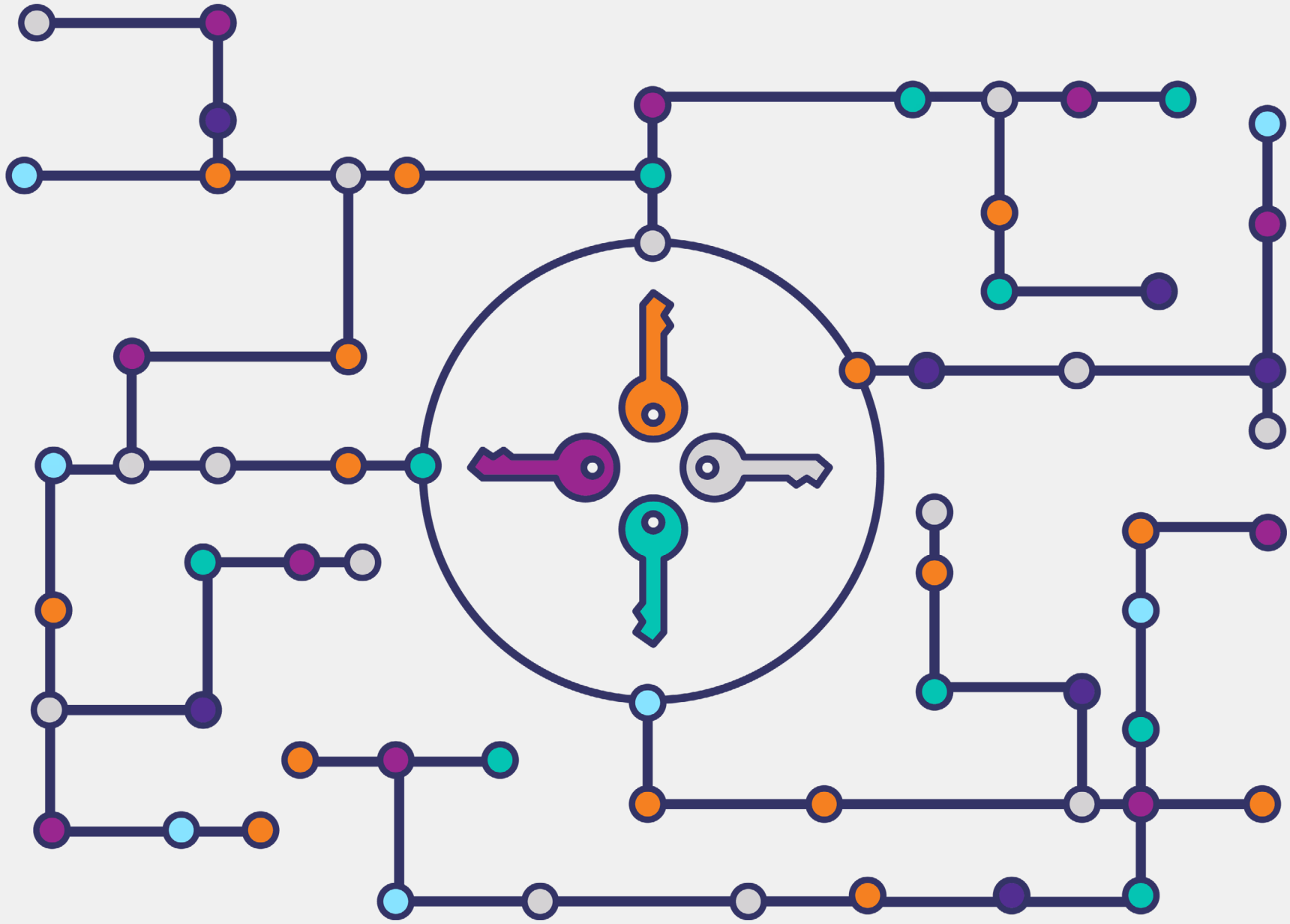
[Como funcionam as chaves privadas?]

João encripta a informação utilizando a chave pública de Maria e, em seguida, a encaminha via internet; Maria, ao receber a transmissão, utiliza sua chave privada para decodificar a informação e compreender seu conteúdo. Da mesma forma, caso Maria queira responder à mensagem de João, ela deve seguir o mesmo processo, encriptando a informação com a chave pública de João, que a desencriptará utilizando sua chave privada.



A chave privada, como pode se depreender, diz respeito a uma chave que é secreta e que não deve ser compartilhada com terceiros. Ao compartilhar sua chave privada com terceiro, você expõe sua privacidade e segurança.

Com a chave privada, é possível autenticar a identidade dos usuários e garantir a confidencialidade e integridade das transações virtuais, criando eficiência e gerando confiança ao sistema.



[Onde guardar as chaves privadas?]

— Preferencialmente, armazene sua chave privada em *"cold wallets",* que são carteiras não vinculadas à internet, reduzindo drasticamente as chances de que caia em mãos erradas;

— Armazene sua chave privada em locais seguros, em ambientes que não sejam suscetíveis de degradação e/ou perda;

— Evite tirar fotos ou fazer *prints* das chaves privadas, pois ficarão mais expostas em caso de ataques cibernéticos;

— Evite armazenar sua chave privada no *smartphone*, *pen-drives,* disco rígido, dispositivos conectados à internet, ou e-mail;

— Não confie em sua memória: procure fazer *backups* de sua chave privada.

[Ferramentas de Segurança Digital] como adotá-las?

Ameaças à segurança e infecção por vírus, *spywares*, *malwares* são cada vez mais frequentes. Isso, em decorrência da violação e destruição e perda dos arquivos e acesso não autorizado a dados de clientes, pode causar impactos financeiros e reputacionais. Profissionais e escritórios de todos os tamanhos estão sujeitos às ameaças cibernéticas. O uso de ferramentas e tecnologia para *backup* e proteção de documentos e sistemas pode fornecer mecanismos de segurança em caso de violação mas, acima de tudo, seu uso efetivo por todos os envolvidos é crítico.

O caminho para uma prática jurídica segura começa com a criação de um simples documento detalhando quais ativos digitais são usados em sua atividade. Categorias como infraestrutura de rede e sistemas e *hardware* devem ser exploradas. É necessário mapear, por exemplo, qual o tipo de conexão usada, de rede (LAN) ou Wi-Fi, se há rede de visitantes e quem possui acesso às senhas.

Filtros de spam

Movem os e-mails não confiáveis para a pasta de *spam*, protegendo os e-mails recebidos contra *phishing* e *malware*, atuando como a primeira e efetiva linha de defesa. A maioria dos provedores de serviço de e-mail possuem filtros básicos de *spam*. O Gmail, por exemplo, permite aos administradores a personalização das configurações de filtro.

Encriptação

Protege o armazenamento e transmissão de dados em computadores, *laptops*, *smartphones*, *tablets* etc. Embora possa parecer uma ferramenta sofisticada aos olhos dos profissionais do direito, a encriptação é uma medida básica de segurança que pode ser amplamente usada para salvaguardar informações pessoais e proteger especialmente dados sensíveis.

Duplo Fator de Autenticação

Procedimento importante para se proteger os sistemas críticos é habilitar o multifator de autenticação – também conhecido como MFA Múltiplo Fator de Autenticação.

Firewall

Inspeciona as comunicações que entram e saem de seu computador e determina quando permitir ou bloqueá-las.
Os *Firewalls* podem prevenir acessos indesejados a seu computador e dados, além de blindar a disseminação de um *malware* de um computador a outro. Windows e Mac OS têm redes *firewalls* que podem ser configuradas de acordo com as necessidades. o a primeira e efetiva linha de defesa.
A maioria dos provedores de serviço de e-mail possuem filtros básicos de spam. O Gmail, por exemplo, permite aos administradores a personalização das configurações de filtro..

Atualização de sistemas

Uma das maiores ameaças aos seus sistemas internos é o *malware* – software criado especificamente para danificar ou desabilitar computadores e seus sistemas. Muitas ameaças por *malware* operam e se disseminam tomando vantagem dos problemas no software que não foram corrigidos e/ou atualizados. Os sistemas operacionais mais modernos, tais como Windows e Mac OS X suportam instalação automática de instalação de atualizações críticas, sendo apenas se habilitar essa opção.

Limite o acesso de visitantes e de informações

Sua rede de visitantes está lá para manter seus clientes e visitantes em separado de sua rede privada – e sem alcance de sua informação confidencial. Se não houver cuidado pode ser inadvertidamente permitido que seus convidados ganhem acesso. Ao configurar sua rede de visitantes, você pode ver uma opção para permitir o acesso à LAN, rede local ou intranet. Esteja certo de não permitir o acesso à LAN de forma que seus visitantes não possam acessar os sistemas internos que estão conectados diretamente ao roteador.

Proteja sua rede

As redes Wi-Fi facilitam a conexão. No entanto, também podem facilitar o acesso não autorizado a sistemas e dados. Muitas redes são violadas em razão do uso de senhas padrão (*default*) que nunca foram trocadas.

Antivírus para desktop, laptops, e-mails e redes

Clicar em links de e-mail parece legítimo ou fazer a instalação do arquivo de um site que você pensa ser seguro, são ações comuns adotadas diariamente que infectam sistemas com *malware* e os danos vão desde roubo de senhas até sequestro de dados. É possível reduzir consideravel-mente os riscos de ataques através da instalação e configuração de antivírus em todos os sistemas. Uma vez instalados, verifique se a checagem em tempo real está ativada. Também é possível agendar uma varredura completa no computador semanalmente, em momento que não interfira com seu trabalho. Se o sistema operacional é Windows 8 ou posterior, o Windows Defender antivírus já está pré-instalado e necessita somente ser configurado.

[Considerações finais]

Acreditamos que com todas essas considerações a respeito da Segurança da Informação, adotamos um passo importante rumo ao melhor desenvolvimento da advocacia em tempos de profunda digitalização da vida humana. A adoção dessas boas práticas pode significar, portanto, uma nova era em termos de identificação na qualidade de operadores de Direito. A progressiva adaptação aos novos desafios enfrentados no dia a dia da advocacia permite construir novos parâmetros de resiliência e respeitabilidade para o desenvolvimento das atividades e a circulação — física e virtual — perante tantos espaços voltados ao setor jurídico.

A Comissão Especial de Inovação e Tecnologia da OAB-SP tem por objetivo reunir e promover o debate em torno da intersecção entre Direito e desen-volvimento tecnológico, de maneira a avançarmos na construção dessa nova realidade que se apresenta à advocacia. Contamos com seu apoio e participação para seguirmos adiante em busca sempre de melhores resultados.

SÃO PAULO