Como proteger seu CPF após um vazamento de dados

Especialistas orientam sobre medidas de segurança e explicam os direitos de quem teve informações pessoais comprometidas

O Cadastro de Pessoas Físicas (CPF) é um dos principais documentos de identificação dos brasileiros. Com ele, é possível realizar atividades financeiras, como abertura de contas, solicitação de empréstimos e financiamentos, além de efetuar cadastros governamentais para acesso a serviços públicos nas áreas de saúde, educação e previdência social. Por estar presente em diversas atividades do dia a dia, o documento pode ser utilizado de forma indevida por criminosos em casos de vazamento de dados.

Vertigo3d_CANVA

O maior exemplo registrado no país aconteceu em 2021, quando 223 milhões de números de CPFs, incluindo os de pessoas falecidas, circularam de forma gratuita na internet. Na época, as informações pessoais foram publicadas por um criminoso em um fórum online dedicado à comercialização de bases de dados.

Para Gilberto Reis, COO da Runtalent, empresa de soluções digitais especializada em recrutamento e alocação de profissionais e equipes de tecnologia, o incidente acendeu um alerta sobre segurança digital no Brasil. "Uma exposição massiva de informações sensíveis dessa natureza mostrou que a proteção de dados não é uma preocupação restrita às empresas. Quando informações como CPF acabam expostas, os impactos na vida das pessoas podem se estender por anos, já que esses dados podem continuar circulando e serem utilizados em diferentes tipos de fraudes", afirma.

O que fazer após um vazamento de dados?

Embora nem todo vazamento resulte imediatamente em fraude, Reis recomenda a adoção de medidas para reduzir riscos e identificar rapidamente possíveis irregularidades. "O titular do documento pode realizar o monitoramento frequente da situação cadastral do CPF, utilizando ferramentas como o Registrato, mantido pelo Banco Central, e o Serasa AntiFraude".

O Registrato permite acessar informações sobre o relacionamento de pessoas físicas e jurídicas com instituições financeiras, incluindo contas bancárias, operações de crédito e outros vínculos registrados em seu nome. A plataforma pode ajudar na identificação de movimentações desconhecidas que demandem investigação.

Já o serviço do Serasa disponibiliza recursos de acompanhamento da situação cadastral do CPF e alertas relacionados à exposição de dados pessoais, contribuindo para a identificação precoce de possíveis fraudes.

Contudo, o especialista orienta que a atenção não fique concentrada apenas no CPF exposto. "Os criminosos costumam combinar diferentes informações obtidas em vazamentos para acessar contas, aplicar golpes e se passar por outras pessoas. Por isso, é importante revisar a segurança de todos os serviços digitais utilizados, especialmente e-mails, aplicativos bancários e redes sociais, por meio da criação de senhas fortes e exclusivas para cada serviço, além da ativação da autenticação em dois fatores sempre que possível".

Quais são os direitos de quem teve dados vazados?

Além dos cuidados para evitar fraudes, a população também conta com direitos garantidos pela Lei Geral de Proteção de Dados (LGPD). A legislação estabelece regras para a coleta, o armazenamento e o tratamento de informações pessoais, além de prever responsabilidades para organizações que não adotem medidas adequadas de segurança.

Raquel Grieco, advogada e sócia do escritório Bosque & Grieco Advogados Associados, ressalta que os titulares de dados têm o direito de ser informados sobre incidentes que possam representar riscos relevantes às suas informações pessoais. "A LGPD prevê mecanismos para garantir maior transparência e proteção aos cidadãos. Dependendo da gravidade do incidente, as organizações podem ser obrigadas a comunicar o vazamento às autoridades competentes e aos titulares afetados, permitindo que adotem medidas para reduzir possíveis danos", explica.

A advogada explica que os cidadãos que sofrerem prejuízos em decorrência do uso indevido de seus dados também podem buscar a responsabilização dos envolvidos. "Cada situação deve ser analisada individualmente, mas a legislação brasileira prevê a possibilidade de reparação quando há comprovação de danos relacionados à falha na proteção das informações pessoais. Por isso, é importante guardar registros, documentos e evidências que possam auxiliar na apuração do caso", conclui.

Como registrar um BO?

Caso identifique movimentações financeiras desconhecidas, abertura de contas, contratação de empréstimos ou qualquer outro indício de uso indevido do CPF, a recomendação é registrar um boletim de ocorrência (BO). O documento ajuda a formalizar o fato e pode ser utilizado para comunicar instituições financeiras, instruir investigações e resguardar o titular em eventuais disputas relacionadas à fraude.

O registro pode ser feito presencialmente em uma delegacia da Polícia Civil ou de forma online, nos estados que oferecem o serviço. Ao preencher o BO, é importante descrever detalhadamente o ocorrido e anexar documentos que possam comprovar a fraude, como extratos bancários, comprovantes de transferências, protocolos de atendimento, e-mails, mensagens e capturas de tela. Essas informações auxiliam na análise da ocorrência e na investigação do caso.

Vibe coding: a nova "Shadow IT" e os riscos para as empresas

João Paulo Costa Pereira (*)

Cerca de 380 mil aplicações web criadas com ferramentas de inteligência artificial estavam publicamente acessíveis na internet, sem qualquer controle de acesso ou autenticação. Desse total, aproximadamente cinco mil vazavam dados corporativos e pessoais sensíveis, incluindo escalas de trabalho de hospitais com informações de identificação de médicos, estratégias comerciais de empresas, registros de incidentes de segurança e conversas privadas entre pacientes e profissionais de saúde.

Essa descoberta, feita em maio de 2026 por uma empresa israelense de cibersegurança e verificada de forma independente por veículos como Axios e Wired, expõe uma realidade que poucos líderes de tecnologia estavam preparados para enfrentar: o vibe coding, prática de criar software por meio de comandos em linguagem natural a ferramentas de IA generativa, está produzindo uma crise de exposição de dados em escala comparável à dos buckets de armazenamento em nuvem mal configurados que atingiu empresas entre 2017 e 2020.

A diferença fundamental é que, naquele período, era necessário algum grau de conhecimento técnico para criar e configurar um servidor na nuvem. Agora, qualquer funcionário com acesso a um navegador e uma conta gratuita em plataformas de desenvolvimento assistido por IA pode construir uma aplicação funcional em minutos, sem compreender o mínimo sobre controles de acesso, validação de dados ou criptografia.

As plataformas de vibe coding, por padrão, publicam as aplicações como acessíveis a qualquer pessoa, a menos que o usuário altere manualmente essa configuração. Muitas dessas aplicações acabam indexadas por mecanismos de busca, o que significa que qualquer pessoa pode encontrá-las com uma pesquisa simples.

Vibe coding: facilidade levanta alertas

Uma pesquisa publicada pela DX em fevereiro de 2026 revelou que 92,6% dos desenvolvedores já utilizam algum assistente de IA para programação ao menos uma vez por mês, e cerca de 75% o fazem semanalmente. Mas o problema vai além dos profissionais de tecnologia. O vibe coding democratizou a criação de software para pessoas que nunca escreveram uma linha de código, e esse é precisamente o ponto em que a produtividade colide com o risco.

Segundo dados do GitHub, a IA já é responsável por 46% de todo o código novo produzido na plataforma, e a projeção é que esse percentual chegue a 60% até o fim do ano. Uma consultoria global de tecnologia prevê que 90% dos engenheiros de software corporativos utilizarão assistentes de IA para codificação até 2028, contra menos de 14% no início de 2024. A mesma consultoria alerta que a abordagem de construção por prompt utilizada por desenvolvedores cidadãos, aqueles que não são profissionais de TI, pode aumentar defeitos de software em 2.500% até 2028 caso não haja governança adequada.

O que torna o vibe coding uma ameaça distinta da Shadow IT tradicional é a natureza bidirecional da exposição. Quando um funcionário utilizava um serviço de armazenamento em nuvem não autorizado, o risco principal era guardar arquivos fora do perímetro corporativo.

No vibe coding, o movimento é mais amplo: o funcionário constrói uma aplicação inteira que pode processar dados de clientes, conectar-se a sistemas internos e expor informações sem que a equipe de segurança sequer saiba que essa aplicação existe.

Do ponto de vista técnico, a fragilidade do código gerado por IA é consistente e bem documentada. Testes de fabricantes diferentes do setor apontam que 45% das amostras de código gerado por IA introduziam vulnerabilidades presentes na lista OWASP Top 10, a referência global de riscos em aplicações web. O índice de falha não apresentou melhora neste último ano, apesar das promessas dos fornecedores.

A consequência prática já é mensurável em termos de vulnerabilidades catalogadas. O projeto Vibe Security Radar, mantido pelo Systems Software & Security Lab da Georgia Tech, rastreou 35 novas entradas de CVE, o registro internacional de vulnerabilidades, diretamente atribuídas a código gerado por IA apenas em março de 2026, contra seis em janeiro e quinze em fevereiro. Os pesquisadores estimam que o número real de vulnerabilidades introduzidas no ecossistema de código aberto é de cinco a dez vezes maior do que o registrado formalmente, dado que muitas aplicações construídas por vibe coding jamais passam por auditoria de segurança.

A velocidade com que aplicações são construídas e publicadas por meio de vibe coding supera em ordens de magnitude a capacidade das equipes de AppSec de revisá-las. Os pipelines de análise estática de código, desenhados para avaliar software desenvolvido por profissionais dentro de ambientes controlados, não foram projetados para detectar aplicações criadas por áreas de negócio que utilizam plataformas externas e publicam diretamente na internet. O resultado é um ponto cego operacional que cresce a cada semana.

O caminho para enfrentar essa realidade não passa por proibir o uso de IA para desenvolvimento de software. Pesquisas demonstram consistentemente que quase metade dos funcionários continuaria utilizando ferramentas pessoais de IA mesmo após uma proibição formal, o que apenas empurraria a prática para camadas ainda mais invisíveis.

A resposta eficaz exige tratar o vibe coding como um problema de arquitetura, não de política. Isso significa implementar varredura de descoberta nos domínios das principais plataformas de vibe coding, exigir revisão de segurança antes da publicação, estender o pipeline de segurança de aplicações para cobrir software criado por áreas de negócio e incluir esses domínios nas regras de prevenção de perda de dados. O líder de segurança que tratar o vibe coding como uma questão de conscientização escreverá um memorando. O que tratá-lo como questão de arquitetura implementará controles antes que a próxima exposição vire manchete.

(*) CEO da Solo Network.

BMG SEGURIDADE S.A. - CNPJ/MF nº 48.263.272/0001-00 - NIRE nº 35.300.607.392

ATA DE ASSEMBLEIA GERAL EXTRAORDINÁRIA REALIZADA EM 28 DE MAIO DE 2026

Data, hora, local: 28.05.2026, 10hs, na sede social, Avenida Presidente Juscelino Kubitschek, nº 1.830, 10º andar, Bloco 04, Condomínio Edifício São Luiz, São Paulo/SP. **Presença**: única acionista. **Mesa**: Presidente: Flávio Pentagna Guimarães Neto, Secretário: Carlos André Hermesindo da Silva. **Deliberações aprovadas**: **1.** A declaração e o pagamento de juros sobre capital próprio pela Companhia, calculados nos termos do artigo 9º da Lei nº 9.249/95, no valor bruto de R$ 6.000.000,00, com retenção de 17,5% de Imposto de Renda na Fonte, resultando no valor líquido de R$ 4.950.000,00. Os juros sobre capital próprio ora declarados serão imputados ao valor dos dividendos mínimos obrigatórios relativo ao exercício social a ser encerrado em 31.12.2026, nos termos do artigo 9º, § 7º da Lei nº 9.249/95. O pagamento dos juros sobre capital próprio ora declarados será efetuado ao único acionista da Companhia até 30.06.2026, sem qualquer atualização monetária ou remuneração correspondente entre a presente data e a data do seu efetivo pagamento. **2.** Nos termos da Cláusula 8ª, 'xiii' do Estatuto Social, a orientação do voto a ser proferido pela Companhia na Reunião de Sócios da BMG Participações em Seguradoras a ser realizada nesta data, favorável à declaração e ao pagamento de juros sobre capital próprio pela Bmg Participações em Seguradoras, calculados nos termos do artigo 9º da Lei nº 9.249/95, no valor bruto de R$ 1.000.000,00, com retenção de 17,5% de Imposto de Renda na Fonte, resultando no valor líquido de R$ 825.000,00 pagos à sua única sócia até 30 de junho de 2026, sem qualquer atualização monetária ou remuneração correspondente entre a data da declaração e a data do seu efetivo pagamento. **Encerramento**: Nada mais. São Paulo, 28.05.2026. Acionista: **Banco BMG S.A.** Por: Flávio Pentagna Guimarães Neto, - Diretor Executivo Vice-Presidente e de Relações com Investidores, e Carlos André Hermesindo da Silva - Diretor sem Designação Específica. JUCESP nº 294.115/26-2 em 17.07.2026. Marina Centurion Dardani - Secretária Geral.

Osvaldo Fernandes S.A. Artes Gráficas

CNPJ: 61.407.060/0001-18 - NIRE: 35300063341

Edital de Convocação - Assembleia Geral Ordinária (AGO)

Ficam **CONVOCADOS** os senhores acionistas da **Osvaldo Fernandes S.A. Artes Gráficas** para se reunirem em **Assembleia Geral Ordinária (AGO),** a ser realizada no dia **6 de agosto de 2026**, na sede do Escritório Alexandre de Morais Advocacia, sito na Alameda Rio Negro, 503, sala 2020, no município de Barueri, Estado de São Paulo, às **10h00** em primeira chamada, e às **10h30** em segunda chamada, a fim de deliberarem sobre a seguinte **Ordem do Dia: 1.** Aprovar as contas dos administradores, examinar, discutir e votar o relatório da diretoria, o balanço patrimonial e as respectivas demonstrações financeiras relativas ao exercício social encerrado em 31 de dezembro de 2025; **2.** Deliberar sobre a proposta de destinação do lucro líquido do exercício de 2025 e a distribuição de dividendos remanescentes (com origem em lucros acumulados), a serem pagos parceladamente a partir do mês de janeiro de 2027; **3.** Ratificação de todos os atos de gestão praticados pela Diretoria desde o encerramento do exercício de 2025 até a presente data; **4.** Outros assuntos de interesse da sociedade. **Aviso Importante (Assembleia Extemporânea):** A presente Assembleia Geral Ordinária é convocada em caráter extemporâneo. Os motivos para a realização fora do prazo legal estabelecido pelo art. 132 da Lei nº 6.404/76 serão devidamente apresentados e registrados em ata durante a reunião. Informamos que, em cumprimento ao disposto no artigo 133 da Lei nº 6.404/76, todos os documentos pertinentes a esta ordem do dia encontram-se à disposição dos acionistas na sede da companhia desde o dia 5 de julho de 2026. Barueri/SP, 24 de julho de 2026. **Patrícia Beltran Fernandes -** Diretora-Presidente.

Registro Civil de Pessoas

CARTÓRIO DE REGISTRO CIVIL

3º Subdistrito - Penha de França

Albert Broday Rodrigues - Oficial do Registro Civil

Faço saber que os seguintes pretendentes apresentaram os documentos exigidos pelo Art. 1525, do Código Civil Atual Brasileiro e desejam se casar:

Faço público a saber que: **RONIFLAVIA PAULINA DA SILVA**, nascida em Juazeiro, BA, em 28/07/1993, filha de José Xavier da Silva e de Maria Paulina da Silva, nos termos do artigo 56 da Lei 6015/73 alterada pela Lei Federal 14.382/2022 promoveu a alteração do seu nome para: **FLAVIA PAULINA DA SILVA**.

Se alguém souber de algum impedimento, oponha-se na forma da lei. Lavro o presente, para ser afixado no Oficial de Registro Civil e publicado na imprensa local Jornal Empresas & Negócios

MARUBENI BRASIL S.A.

CNPJ(MF) nº 60.884.756/0001-72 - NIRE nº 35.300.028.180

Resumo da Ata A.G.E de 26.06.2026

Local, Hora e Data - Na sede da Cia a Av. Paulista, nº 1063, conj. 201, São Paulo - SP, às 10h00 no dia 26.06.2026, reuniram-se os acionistas. **Convocação e Presenças:** Dispensada a convocação, nos termos do artigo 124, § 4º, da Lei 6.404/76 em razão da presença de Acionistas representando a totalidade do Capital Social, conforme assinaturas no Livro de Presença dos Acionistas. **Composição da Mesa -** Presidente - Sr. **Yasunobu Ono,** Diretor Presidente da Cia - Secretário - Sr. **Ryo Furutani,** Diretor da Cia. **Ordem do dia:** Deliberar acerca de: I) a nomeação do Sr. **Koichi Fukunishi** ao cargo de Diretor da Cia. **Deliberações:** Após discussão da matéria da ordem do dia, as Acionistas aprovaram, por unanimidade de votos a nomeação do Sr. **Koichi Fukunishi,** de nacionalidade japonesa, casado, do comércio, portador do passaporte nº TZ2153631, expedido pelo Governo japonês, RMN nº B637880K, inscrito no CPF sob o nº 129.783.431-33, com endereço comercial a Av. Paulista, nº 1063, conj. 201, São Paulo/SP, para o cargo de Diretor da Cia. No ato da nomeação, declara os Sr. **Koichi Fukunishi,** sob as penas da lei, que não estão impedidos, por lei especial, de exercer a administração da sociedade e nem condenados ou sob efeitos de condenação, a pena que vede, ainda que temporariamente, o acesso a cargos públicos, ou por crime falimentar, de prevaricação, peita ou suborno, concussão, peculato; ou contra a economia popular, contra o Sistema Financeiro Nacional, contra as normas de defesa da concorrência, contra as relações de consumo, a fé pública ou a propriedade. **Encerramento -** Nada mais havendo a tratar, foram suspensos os trabalhos pelo tempo necessário para a lavratura da presente ata, no livro próprio, a qual foi lida, aprovada, e assinada por todos os presentes. A Ata em inteiro teor foi registrada na JUCESP sob nº 297.432/26-6 em sessão de 22/07/2026 e publicada neste jornal no formato impresso e digital.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Certisign Assinaturas. Para verificar as assinaturas clique no link: http://assinaturas.certisign.com.br/Verificar/B8E8-5424-4A7D-D6FB ou vá até o site http://assinaturas.certisign.com.br e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: B8E8-5424-4A7D-D6FB

Hash do Documento

A6856C5F6EEA8F09C218BBD014E90CA08972D2E82A39FC4002E8804E426C4C12

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 27/07/2026 é(são) :

☑ Lilian Regina Mancuso - 05.687.343/0001-90 em 27/07/2026 19:29 UTC-03:00
Tipo: Certificado Digital - JORNAL EMPRESAS E NEGOCIOS LTDA - 05.687.343/0001-90

Evidências

Geolocation: Location not shared by user.
IP: 172.16.4.12
AC: AC Certisign RFB G5