DIREITO DIGITAL

BOLETIM DIGITAL

15ª EDIÇÃO

Notícias desta edição

ALMEIDA ADVOGADOS

ALMEIDA ADVOGADOS
DIREITO CORPORATIVO

BOLETIM DIGITAL

15ª EDIÇÃO

Este é o informativo preparado pela nossa área de Direito Digital com o objetivo de concentrar as principais notícias e mais relevantes discussões sobre os temas do mundo digital. Boa leitura!

INVESTIDOR PERDE R$ 500 MILHÕES EM BITCOIN APÓS GOLPE DE ENGENHARIA SOCIAL

Investidor teve 783 bitcoins roubados — cerca de R$ 500 milhões — após cair em golpe de engenharia social, em que criminosos se passaram por suporte de corretora e de carteira de hardware, levando-o a fornecer sua frase-semente em site malicioso. O roubo foi rápido e os ativos começaram a ser movimentados e lavados por meio de plataformas como Wasabi para dificultar o rastreamento. Esse episódio ocorreu no mesmo dia em que outro caso semelhante foi detectado no País de Gales, com investimento de R$ 15,5 milhões roubados — sugerindo possível coordenação ou padrão entre ataques.

OPERAÇÃO NO RJ COMBATE ATAQUE CIBERNÉTICO DE EXTORSÃO A EMPRESA DE LOGÍSTICA

A Polícia Civil do Rio de Janeiro deflagrou a "Operação Fantasma" contra-ataque cibernético que visava extorquir uma empresa de logística. O criminoso exigiu US$ 10 mil em criptomoedas para não divulgar dados de clientes e fornecedores. Mesmo após o pagamento, informações internas foram vazadas e o WhatsApp corporativo foi invadido, levando à apreensão de equipamentos e abertura de investigação criminal.

FALHA EM GERENCIADORES DE SENHA EXPÕE MILHÕES DE USUÁRIOS

Falha em gerenciadores de senhas expôs milhões de credenciais armazenadas, colocando em risco a segurança de inúmeros usuários. A vulnerabilidade permitiu que agentes maliciosos acessem dados sensíveis com facilidade, alertando para a necessidade urgente de atualização dos aplicativos. Usuários são orientados a ativar a autenticação de dois fatores, revisar e fortalecer senhas, além de verificar se o gerenciador foi atualizado com correções de segurança — medidas fundamentais para mitigar o risco de vazamentos futuros.

BRASIL: TENTATIVAS DE ATAQUE A 80% DAS EMPRESAS NO ÚLTIMO ANO

O CIO Report 2025, promovido pela Logicalis em parceria com a Vanson Bourne, revelou que 80% das grandes empresas brasileiras sofreram ao menos um incidente cibernético nos últimos 12 meses. Entre os ataques mais frequentes, estão malwares e ransomwares (40%), deepfakes maliciosos (37%), vazamentos de dados (34%), ataques com uso de inteligência artificial (31%) e phishing (28%). Em 84% dos casos houve violação efetiva de segurança, e quase 30% enfrentaram múltiplos episódios.

PHISHING AVANÇADO E BACKDOORS TÊM COMO ALVO LÍDERES CORPORATIVOS

A campanha de ciberespionagem atribuída ao grupo APT MuddyWater mira CFOs e executivos financeiros em vários continentes. Os ataques usam phishing sofisticado, disfarçado de comunicações de recrutamento da Rothschild & Co, hospedadas em domínios Firebase com CAPTCHAs falsos para enganar as vítimas.

As iscas levam a arquivos ZIP que instalam ferramentas legítimas, como NetBird e OpenSSH, configuradas para criar backdoors persistentes. O malware cria conta administrativa oculta, habilita RDP, ajusta firewall e agenda reinicializações automáticas, evitando detecção e facilitando a exfiltração de dados sensíveis.

CRIMINOSOS USAM TV BOX NÃO HOMOLOGADOS PARA ROUBAR DADOS DE USUÁRIOS, DIZ ANATEL

A Anatel alertou que aparelhos de TV Box não homologados estão sendo utilizados por criminosos para invadir redes domésticas e coletar dados pessoais. Esses dispositivos, que oferecem acesso ilegal a canais pagos e serviços de streaming, foram identificados como porta de entrada para malwares.

A agência reforçou que apenas equipamentos certificados oferecem garantias mínimas de segurança, e anunciou medidas de fiscalização e apreensão para combater o comércio irregular desses produtos.

FALHA EM BARRAGEM DA NORUEGA FOI CAUSADA POR ATAQUE HACKER

Hackers invadiram a barragem Rizevatnet, na Noruega, e abriram uma comporta por cerca de quatro horas, causando vazamento de 500 litros de água por segundo. O incidente ocorreu em 7 de abril e foi facilitado por uso de senha fraca nos sistemas remotos. Apesar da gravidade, o rio suporta até 20.000 L/s, o que evitou inundações ou feridos; autoridades atribuíram o ataque a um grupo hacker pró-Rússia, embora a embaixada russa tenha negado envolvimento.

CRESCIMENTO DAS VERBAS DE CIBERSEGURANÇA CAI PELA METADE

Os investimentos em cibersegurança desaceleraram em 2025, com crescimento médio de apenas 4%, contra 8% no ano anterior. O relatório da IANS Research e Artico mostra que a fatia da segurança digital nos orçamentos de TI caiu de 11,9% para 10,9% — o primeiro recuo em cinco anos. Embora 51% dos CFOs classifiquem ameaças cibernéticas como risco crítico, os recursos destinados não acompanham a complexidade e frequência das ameaças.

A retração ocorre mesmo com projeções do Gartner indicando gastos globais em segurança de US$ 213 bilhões em 2025. Analistas acreditam que pressões regulatórias e maior conscientização sustentarão investimentos no médio prazo, sobretudo em pequenas e médias empresas. No curto prazo, porém, a contenção de gastos, congelamento de contratações e restrições a novos projetos aumentam a exposição a ataques e podem favorecer a exploração de vulnerabilidades por criminosos.

ORÇAMENTOS REDUZIDOS ACELERAM USO DE IA EM SEGURANÇA CIBERNÉTICA

Com cortes e crescimento mais lento dos investimentos em segurança (de 17% em 2022 para 4% em 2025), empresas recorrem cada vez mais à automação por inteligência artificial para compensar falta de pessoal, manter defesas ativas e lidar com ameaças em expansão. O Gartner estima gastos globais de US$ 213 bilhões em 2025, subindo a US$ 240 bilhões em 2026, ainda abaixo da demanda.

Estudos do IANS e Swimlane indicam que restrições orçamentárias, redução de apoio governamental e incertezas globais forçam equipes a “fazer mais com menos”. Ferramentas de IA auxiliam em tarefas de triagem e detecção, mas aumentam a dependência tecnológica e podem ampliar riscos a médio prazo.

ANPD E NIC.BR CELEBRAM ACORDO DE COOPERAÇÃO EM PROTEÇÃO DE DADOS

A Autoridade Nacional de Proteção de Dados (ANPD) e o Núcleo de Informação e Coordenação do Ponto BR (Nic.br) assinaram acordo de cooperação durante o 16º Seminário de Proteção à Privacidade e aos Dados Pessoais, em São Paulo. O objetivo é desenvolver ações conjuntas em proteção de dados e segurança da informação, incluindo iniciativas educativas, compartilhamento de informações, produção de relatórios e projetos de pesquisa.

A parceria atual aprofunda colaboração iniciada em 2021 e prevê criação de indicadores, notas técnicas e estudos sobre privacidade, segurança da informação e uso de inteligência artificial. Segundo o diretor-presidente da ANPD, Waldemar Gonçalves, a cooperação contribui para consolidar a cultura de proteção de dados no Brasil e facilita a harmonização regulatória, essencial para o fluxo internacional de dados e inovação econômica.

ANPD DEFENDE LEGISLAÇÃO TRANSPARENTE PARA BOA GOVERNANÇA DE IA

Waldemar Gonçalves, diretor-presidente da ANPD, defendeu, durante congresso em São Paulo, que a regulação da inteligência artificial no Brasil deve priorizar transparência, segurança, explicabilidade, proteção a direitos fundamentais e combate à discriminação algorítmica. Ele reforçou que a agência está pronta para coordenar o Sistema Nacional de Regulação e Governança de IA (SIA), apoiar o PL 2.338/2023 e conduzir iniciativas como sandbox regulatório e Radar Tecnológico. A cooperação internacional, inclusive com a Rede Ibero-americana de Proteção de Dados (RIPD), também foi enfatizada para harmonizar normas.

PAÍSES LUSÓFONOS ESTRUTURAM COOPERAÇÃO E HARMONIA REGULATÓRIA EM PRIVACIDADE

Durante evento paralelo ao 16º Seminário de Privacidade em São Paulo, autoridades de proteção de dados de países lusófonos formalizaram a Rede Lusófona de Proteção de Dados (RLPD). Estabeleceram Grupos de Trabalho sobre os temas prioritários — como biometria, neurodados, IA, vigilância e transferência internacional de dados — e começaram um estudo comparativo de legislações nacionais, além de lançar logo e site institucional para estreitar cooperação.

ANPD PODERÁ DERRUBAR CONTEÚDO DIGITAL ILÍCITO E APLICAR SANÇÕES

O governo federal quer ampliar os poderes da ANPD, renomeada para Autoridade Nacional de Proteção de Dados e Serviços Digitais, para incluir a remoção de conteúdo ilícito (como discursos de ódio, terrorismo e material contra crianças) e aplicar sanções financeiras de até 10% do faturamento das plataformas. A proposta está em dois projetos de lei sobre serviços digitais e concorrência, já apresentados às grandes empresas de tecnologia em reunião no Palácio do Planalto.

RADAR LEGISLATIVO

PL 4160/2025

Cria um novo marco legal para o compartilhamento de postes de energia elétrica entre distribuidoras e prestadoras de telecomunicações. Estabelece que concessionárias devem ceder, de forma onerosa e regulada por Aneel e Anatel, o uso do espaço para instalação de cabos e equipamentos, com critérios técnicos e de segurança. Prevê ainda a atuação de uma cessionária independente e de uma entidade privada de assessoramento, responsável por apoiar a regulação, combater ocupações irregulares e propor soluções técnicas, visando reduzir riscos de acidentes, poluição visual e ampliar o acesso à internet de alta velocidade.

PL 4148/2025

Torna obrigatória a utilização de código numérico padronizado para identificação de chamadas de telemarketing ativo no território nacional e dá outras providências.

PL 4020/2025

Impõe carência de 48 horas para que prêmios mantidos em carteiras virtuais de apostas sejam reutilizados em novas apostas, buscando reduzir impulsividade e vício.

PL 3967/2025

Altera o Marco Civil da Internet para obrigar a identificação explícita de conteúdos gerados ou manipulados por inteligência artificial, visando transparência e combate à desinformação.

PL 3879/2025

Garante a preservação de perfis de candidatos, partidos e titulares de mandato em plataformas digitais durante o período eleitoral, vedando suspensão, bloqueio ou exclusão, salvo em casos expressamente previstos. Autoriza remoção apenas mediante decisão judicial fundamentada, restrita a crimes graves como hediondos, exploração sexual de crianças e adolescentes, tráfico de pessoas e terrorismo. Prevê sanções às plataformas em caso de descumprimento, incluindo multas de até 20% do faturamento, restabelecimento imediato de contas e indenizações.

PL 3923/2025

Regulamenta a atividade profissional de influenciador digital, reconhecendo-a como trabalho formal. Define atribuições, direitos e obrigações, impondo dever de informação fidedigna, respeito à dignidade humana, responsabilidade sobre conteúdos e cautelas específicas em produções voltadas a crianças e adolescentes. Proíbe a divulgação de conteúdos preconceituosos, violentos, ilícitos ou que incentivem práticas nocivas, prevendo sanções e até a impossibilidade de continuar exercendo a atividade em caso de descumprimento.

PL 3901/2025

Institui a Lei de Responsabilidade Social de Plataformas Digitais (LRSPD), aplicável a plataformas com mais de 1 milhão de usuários no Brasil. Estabelece princípios de responsabilidade social algorítmica, combate à desinformação, proteção de grupos vulneráveis e transparência sobre moderação e publicidade. Obriga relatórios trimestrais, rotulagem de anúncios, restrição de publicidade nociva a menores e criação de alertas para uso excessivo de telas. Prevê sanções de até 2% do faturamento (limitadas a R$ 50 milhões por infração) e cria o Conselho Nacional de Responsabilidade Digital para monitoramento e auditoria.

PL 4135/2025

Altera a Lei Geral de Proteção de Dados (LGPD) para exigir que plataformas digitais com mais de 3 milhões de usuários realizem auditorias anuais obrigatórias. Essas auditorias devem abranger a comercialização de dados pessoais, a responsabilidade civil das plataformas e a transparência algorítmica, mesmo na ausência de indícios de risco ou irregularidades.

PL 4126/2025

Dispõe sobre a proibição de instituições educacionais divulgarem imagens que identifiquem o rosto de crianças em redes sociais e dá outras providências.

PL 4030/2025

Altera o Código Penal e o Estatuto da Criança e do Adolescente para tipificar como crime a adultização e erotização digital de crianças e adolescentes, mesmo sem nudez explícita. Prevê penas de reclusão de 4 a 8 anos e multa, com agravamento se o conteúdo for divulgado em plataformas digitais. Também responsabiliza pais, tutores, influenciadores e adultos que induzam, permitam ou se omitam diante da exposição inadequada, além de estabelecer medidas preventivas, campanhas educativas e dever de responsabilidade das plataformas.

PL 3986/2025

Proíbe a monetização de conteúdos ilícitos ou exploratórios envolvendo crianças e adolescentes, impõe remoção em até 24h, prevenção tecnológica contra reuploads, criação de canal "Alerta Criança" e sanções de até R$ 50 milhões para plataformas que descumprirem.

PL 3991/2025

Altera o Código Penal e o ECA para instituir pena acessória de proibição do uso de redes sociais, celulares e internet a condenados por crimes digitais contra crianças e adolescentes, pelo mesmo período da pena de prisão.

PL 4014/2025

Tipifica como crime (3 a 6 anos de reclusão) a produção ou transmissão de conteúdo que retrate crianças e adolescentes em contexto de adultização sexualizada. Também veda monetização/impulsionamento desses conteúdos e responsabiliza plataformas que não removerem após notificação.

PL 4015/2025

Exige verificação de idade para acesso a conteúdo sexual explícito online, com sistema de "duplo anonimato" para proteger a privacidade. Estabelece requisitos técnicos, prazo de adequação de 180 dias e multas de até R$ 50 milhões por infração.

PL 4022/2025

Proíbe o uso de algoritmos e sistemas de recomendação para conteúdos sexuais envolvendo crianças e adolescentes. Cria o Selo de Conformidade Digital, exige auditorias e canais de denúncia, e tipifica no Código Penal o crime de "adultização com fins de erotização" (pena de 2 a 4 anos).

PL 3946/2025

O projeto altera o Marco Civil da Internet para determinar que menores de 16 anos só podem manter conta em redes sociais se vinculada a uma conta pré-existente de um responsável legal. A medida busca ampliar a supervisão parental e reduzir riscos como exposição a conteúdos impróprios, aliciamento, cyberbullying e impactos negativos à saúde mental de crianças e adolescentes.

PL 3924/2025

Cria a chamada Lei Felca, estabelecendo regras de proteção de crianças e adolescentes na internet. Exige verificação etária, consentimento parental e controle obrigatório de acesso, além de proibir publicidade direcionada com base em dados de menores. Determina que plataformas removam conteúdos ilícitos (exploração sexual, incentivo ao suicídio ou automutilação, ataques a escolas) e realizem campanhas anuais de conscientização. Também altera o ECA para aumentar penas de crimes digitais contra menores, chegando até 40 anos de reclusão em casos de exploração sexual.

PL 3902/2025

Institui o Direito à Desconexão Digital Infantil, com diretrizes para limitar a hiperexposição de crianças e adolescentes às telas. Prevê ações de escolas (restrição de tempo em atividades remotas, inclusão de cidadania digital nos currículos e promoção de atividades offline), obrigações das plataformas (alertas de pausa, controle parental, respeito a horários definidos pelos responsáveis, restrição de notificações noturnas) e campanha nacional de conscientização. O objetivo é combater dependência tecnológica, proteger a saúde mental e garantir desenvolvimento equilibrado.

AA nas redes sociais

Siga nosso perfil para **receber atualizações exclusivas** e conteúdo jurídico especializado em Direito Digital!

Márcio Chaves
Sócio

mmchaves@almeidalaw.com.br
+55 (11) 2714 6900 | 9828

Lucca Fontana
Advogado

lgfontana@almeidalaw.com.br
+55 (11) 2714 6900

Mario Baldir
Advogado

mrfilho@almeidalaw.com.br
+55 (11) 2714 6900

ALMEIDA
ADVOGADOS