ISSN ONLINE 2675-3316

EDIÇÃO
05
MAIO 2025

INFORMATIVO LEGAL

BOLETIM INFORMATIVO JURÍDICO MENSAL

Nesta edição

Editorial

Na edição de maio do Informativo Legal, trazemos informações essenciais sobre temas relevantes, oferecendo dicas indispensáveis para você se manter bem informado. Saiba mais sobre descontos indevidos por associações e sindicatos nas contas de beneficiários do INSS; estratégias de criminosos para golpes de biometria facial; prevenção e responsabilização do assédio moral no ambiente corporativo; conceitos e aplicação jurídica de *compliance*; e os impactos dos conflitos geopolíticos em ataques cibernéticos. Como sempre, nosso objetivo é manter você, leitor, sempre atualizado e preparado para enfrentar esses desafios com dicas valiosas no campo jurídico.

Equipe do Informativo Legal

Descontos Indevidos por Associações e Sindicatos nas Contas de Beneficiários e Pensionistas do INSS sem Autorização Prévia

Nos últimos anos, tem crescido de forma preocupante o número de denúncias e reclamações por parte de aposentados e pensionistas do INSS sobre descontos indevidos em seus benefícios, realizados por associações, sindicatos ou entidades representativas sem a devida autorização. O tema tem ganhado repercussão nacional, especialmente diante da vulnerabilidade desse público e da dificuldade de muitos em identificar a origem de tais descontos ou buscar orientação adequada para solucioná-los.

Reportagens veiculadas na mídia, além de alertas emitidos por órgãos de defesa do consumidor e do próprio INSS, revelam que milhares de beneficiários foram surpreendidos com descontos mensais em seus pagamentos, sem nunca terem autorizado qualquer filiação ou contribuição. Muitas vezes, essas cobranças ocorrem por meio de registros fraudulentos ou sem a devida transparência quanto à finalidade do desconto.

A prática, além de ilegal, compromete a renda de pessoas que, em grande parte, dependem exclusivamente do benefício previdenciário para sua subsistência. Em resposta a essa realidade, o Poder Público e o Judiciário vêm adotando medidas para garantir maior proteção aos beneficiários e responsabilizar as entidades que praticam esses atos abusivos.

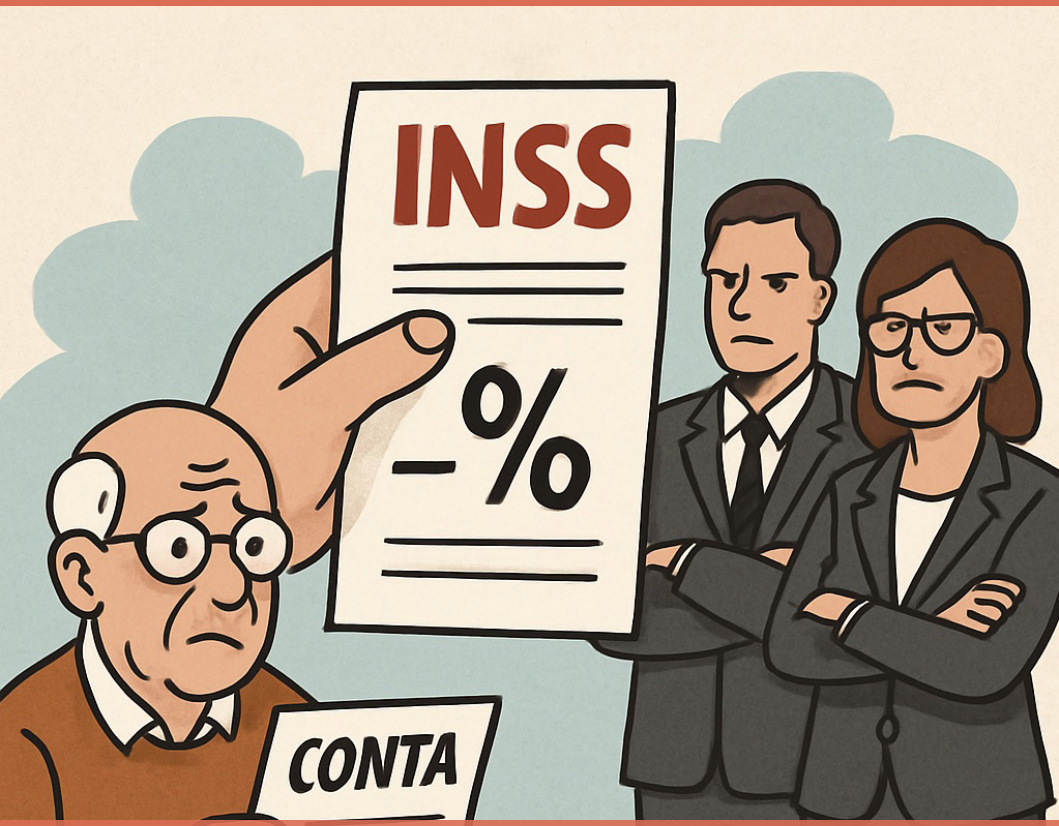
Diante desse cenário, é fundamental esclarecer os direitos dos segurados e os mecanismos legais disponíveis para contestar os descontos indevidos e buscar a reparação dos prejuízos sofridos.

É vedada a realização de descontos em benefícios previdenciários pagos pelo INSS a título de mensalidade associativa, sindical ou contribuições similares sem que haja autorização prévia, expressa e individual do titular do benefício. A prática de proceder a tais descontos sem consentimento configura violação à legislação vigente e afronta direitos fundamentais do beneficiário.

A Constituição Federal, em seu artigo 5º, inciso XX, assegura o direito à liberdade de associação, dispondo que ninguém poderá ser compelido a associar-se ou a permanecer associado. Isso significa que qualquer filiação a sindicato, associação ou entidade representativa deve ocorrer de forma livre e voluntária, sendo imprescindível o consentimento claro do beneficiário para que possa haver qualquer cobrança ou desconto decorrente.

Além disso, a legislação previdenciária e as normas internas do INSS determinam que apenas serão admitidos descontos em folha de pagamento quando autorizados formalmente pelo beneficiário, por meio de documento que comprove sua concordância.

Portanto, o desconto realizado sem autorização é considerado indevido e pode ser contestado diretamente perante o INSS, com pedido de cancelamento imediato e restituição dos valores descontados. Caso o problema não seja solucionado na esfera administrativa, o beneficiário pode buscar a via judicial para obter a devolução dos valores pagos indevidamente e, conforme o caso, pleitear indenização por eventuais danos sofridos.



RECOMENDAÇÕES:

1. O beneficiário deve acompanhar mensalmente seu extrato de pagamento do INSS, disponível pelo aplicativo ou site "Meu INSS";
2. Em caso de identificação de desconto não autorizado, deve registrar reclamação junto ao INSS e solicitar o bloqueio imediato do desconto;
3. Recomenda-se também entrar em contato com a entidade responsável pelo desconto para obter esclarecimentos e, se necessário, solicitar cópia do suposto termo de adesão;
4. Se não houver solução administrativa, é possível buscar orientação jurídica para o ajuizamento de ação visando à restituição dos valores e responsabilização da entidade.

Todo desconto em benefício previdenciário deve ser realizado de forma lícita e transparente, com autorização expressa do titular. A ausência dessa autorização torna o desconto ilegal e passível de anulação, com direito à restituição dos valores e demais reparações cabíveis.

Rafael Rodrigues Raez

CONHEÇA AS ESTRATÉGIAS DOS CRIMINOSOS E NÃO CAIA NO GOLPE DA BIOMETRIA FACIAL

Com o avanço da tecnologia e a digitalização dos serviços bancários e públicos, a biometria facial passou a ser amplamente utilizada como ferramenta de segurança. Instituições financeiras, aplicativos de pagamento, órgãos governamentais e até plataformas de crédito utilizam esse recurso como forma de confirmar a identidade de seus usuários. No entanto, o que deveria representar proteção tem sido transformado por criminosos em mais uma arma para aplicar golpes sofisticados e devastadores.

Como funciona o golpe da biometria facial?

O golpe da biometria facial consiste na utilização indevida da imagem do rosto da vítima, em conjunto com outros dados pessoais, para acessar ou criar contas em bancos, *fintechs*, plataformas de crédito ou instituições públicas. A partir disso, os golpistas podem contrair empréstimos, realizar transferências, abrir empresas fraudulentas e comprometer o CPF da vítima de forma grave.

O golpe pode ocorrer em várias etapas, geralmente combinando técnicas de engenharia social, *phishing* e vazamento de dados. Veja o passo a passo de como ele costuma ser aplicado:

1. Coleta de dados pessoais

Os criminosos obtêm informações como CPF, nome completo, data de nascimento, nome da mãe e endereço por meio de vazamentos, compras de dados na *dark web* ou até observando redes sociais públicas.

Muitas vítimas não percebem que expõem seus dados ao preencher cadastros em sites falsos ou responder formulários on-line duvidosos.

2. Contato fraudulento com a vítima

A vítima recebe uma ligação, e-mail, SMS ou mensagem de WhatsApp de um suposto atendente do banco, operadora ou órgão público.

O criminoso informa que é necessário "atualizar o cadastro", "revalidar os dados", "confirmar um pedido" ou "evitar o bloqueio da conta".

Em alguns casos, eles enviam *links* falsos, direcionando a vítima para páginas clonadas que imitam o site de uma instituição oficial.

3. Solicitação de foto (*selfie*) ou reconhecimento facial

Após conquistar a confiança da vítima, o criminoso pede que ela envie uma foto atual segurando um documento (RG ou CNH), ou mesmo apenas uma *selfie*.

Essa imagem é utilizada para validar o reconhecimento facial em aplicativos e bancos que aceitam biometria como forma de autenticação.

4. Validação de fraudes com a biometria facial

De posse da imagem e dos dados, o criminoso consegue abrir contas, pedir crédito, solicitar cartões ou fazer movimentações financeiras em nome da vítima.

Como muitos sistemas não pedem confirmação adicional além da biometria, a fraude é concluída com sucesso.

5. Descoberta tardia pela vítima

Em geral, a pessoa só percebe que foi vítima quando recebe cobranças indevidas, vê seu nome negativado ou tenta abrir crédito e descobre que seu CPF já está comprometido.

As técnicas utilizadas pelos golpistas, em regra, são de cunho emocional, com o uso de mensagens que geram medo ou urgência ("sua conta será bloqueada!", "tem um débito em aberto") ou o uso de perfis falsos nas redes sociais imitando logos de bancos e empresas para enganar usuários desatentos. Eles se passam por falsos atendentes, onde as ligações são feitas por atendentes treinados para parecerem profissionais, inclusive com uso de dados verdadeiros para convencer. Páginas clonadas, com sites idênticos aos originais, que capturam fotos, senhas e dados e, aplicativos maliciosos e falsos que capturam dados biométricos ao simular serviços oficiais, também são utilizados pelos golpistas.

Para se proteger, a prevenção é a melhor arma contra esse tipo de golpe. Veja boas práticas para evitar ser vítima:

- Desconfie de qualquer contato inesperado solicitando confirmação de dados ou fotos.
- Nunca envie *selfies* ou imagens de documentos fora dos canais oficiais da

instituição.

• Verifique o endereço de e-mail, número de telefone e *links* enviados. Sites oficiais costumam ter domínios seguros (com "https://") e e-mails institucionais.

• Não clique em *links* enviados por mensagens suspeitas, mesmo que pareçam vir de bancos.

• Evite expor dados pessoais em redes sociais, como número de documentos, fotos de RG/CNH ou nome de familiares.

• Use autenticação em dois fatores sempre que possível.

• Consulte com frequência seu CPF em plataformas como Registrato (Banco Central), Serasa ou Boa Vista.

• Mantenha seu celular e aplicativos sempre atualizados e use antivírus confiáveis.

O que fazer se você for vítima?

Se você foi enganado e acredita que seus dados ou sua imagem foram usados de forma indevida, siga estes passos imediatamente:

1. Registre um Boletim de Ocorrência relatando os fatos com o máximo de detalhes possível.

2. Entre em contato com seu banco ou instituição financeira e peça o bloqueio de contas suspeitas.

3. Notifique os órgãos de proteção ao crédito (Serasa, Boa Vista, SPC) para registrar o golpe.

4. Acompanhe os serviços do Registrato (plataforma gratuita do Banco Central) para ver quais contas estão atreladas ao seu CPF.

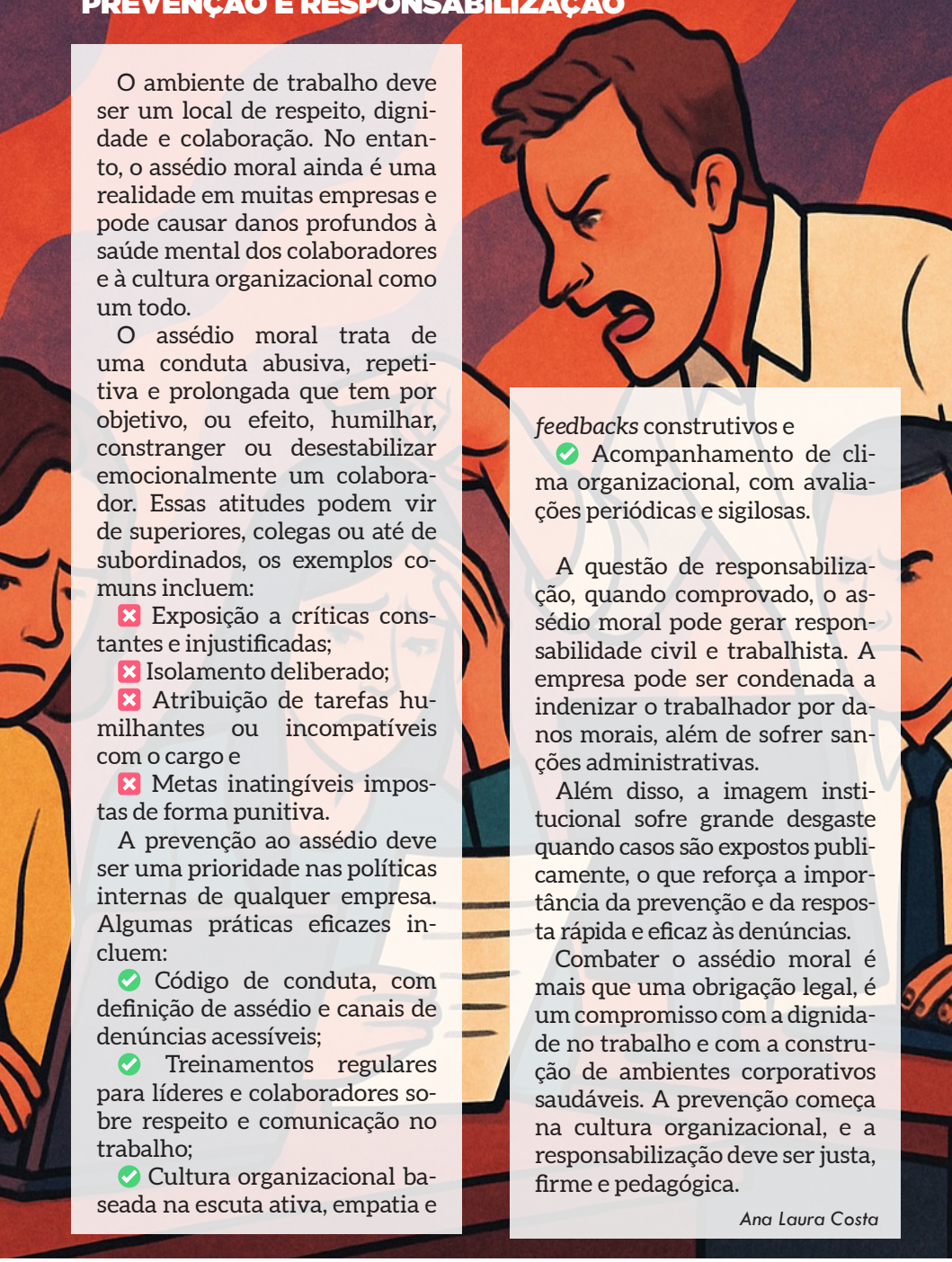
5. Considere uma notificação judicial ou ação para contestar dívidas ou danos causados por terceiros.

6. Procure um advogado de sua confiança para orientações sobre como responsabilizar os envolvidos e obter reparação por eventuais prejuízos.

A biometria facial é uma tecnologia poderosa, mas não é infalível quando combinada à engenharia social e à exposição de dados pessoais. A conscientização e o cuidado com a própria imagem são essenciais. Não caia em armadilhas que pedem *selfies*, atualizações cadastrais por mensagens ou "confirmações de identidade" fora de canais seguros. Sua imagem é sua identidade. Proteja-a como protege sua senha.

Stephany Villalpando

ASSÉDIO MORAL NO AMBIENTE CORPORATIVO: PREVENÇÃO E RESPONSABILIZAÇÃO



O ambiente de trabalho deve ser um local de respeito, dignidade e colaboração. No entanto, o assédio moral ainda é uma realidade em muitas empresas e pode causar danos profundos à saúde mental dos colaboradores e à cultura organizacional como um todo.

O assédio moral trata de uma conduta abusiva, repetitiva e prolongada que tem por objetivo, ou efeito, humilhar, constranger ou desestabilizar emocionalmente um colaborador. Essas atitudes podem vir de superiores, colegas ou até de subordinados, os exemplos comuns incluem:

- ✖ Exposição a críticas constantes e injustificadas;
- ✖ Isolamento deliberado;
- ✖ Atribuição de tarefas humilhantes ou incompatíveis com o cargo e
- ✖ Metas inatingíveis impostas de forma punitiva.

A prevenção ao assédio deve ser uma prioridade nas políticas internas de qualquer empresa. Algumas práticas eficazes incluem:

- ✔ Código de conduta, com definição de assédio e canais de denúncias acessíveis;
- ✔ Treinamentos regulares para líderes e colaboradores sobre respeito e comunicação no trabalho;
- ✔ Cultura organizacional baseada na escuta ativa, empatia e *feedbacks* construtivos e
- ✔ Acompanhamento de clima organizacional, com avaliações periódicas e sigilosas.

A questão de responsabilização, quando comprovado, o assédio moral pode gerar responsabilidade civil e trabalhista. A empresa pode ser condenada a indenizar o trabalhador por danos morais, além de sofrer sanções administrativas.

Além disso, a imagem institucional sofre grande desgaste quando casos são expostos publicamente, o que reforça a importância da prevenção e da resposta rápida e eficaz às denúncias.

Combater o assédio moral é mais que uma obrigação legal, é um compromisso com a dignidade no trabalho e com a construção de ambientes corporativos saudáveis. A prevenção começa na cultura organizacional, e a responsabilização deve ser justa, firme e pedagógica.

Ana Laura Costa

COMPLIANCE: CONCEITOS E APLICAÇÃO JURÍDICA

O conceito moderno de *compliance* surgiu nos Estados Unidos, no setor financeiro, após escândalos corporativos nas décadas de 1970 e 1980. Desde então, práticas de integridade corporativa foram inseridas para prevenir subornos e fraudes em empresas. No âmbito internacional, diversos instrumentos reforçaram a importância do *compliance*, como a Convenção contra Suborno de Funcionários Públicos Estrangeiros (1997) e a Convenção das Nações Unidas contra a Corrupção (2003).

Assim, nas últimas décadas, a governança corporativa tem incorporado novos modelos, com destaque para as práticas de *compliance*, instrumento que consolida a sustentabilidade jurídica, econômica e a reputação das organizações.

O termo *compliance* deriva do verbo inglês "to comply", que significa "agir de acordo com" ou "estar em conformidade", assim, na esfera jurídica, *compliance* refere-se ao conjunto de mecanismos e procedimentos internos adotados pelas organizações para garantir o cumprimento das leis, normas regulatórias, diretrizes internas e padrões éticos. No Brasil, ganhou força com a Lei Anticorrupção, que estabeleceu responsabilidade às pessoas jurídicas por atos contra

a administração pública, com a possibilidade de aplicação de sanções administrativas e civis, previsão de acordo de leniência com empresas colaboradoras e valoração do programa de integridade como critério para atenuação de penalidades.

Leis Federais também foram criadas ao longo desse período, como a Lei de Improbidade Administrativa (Lei n. 8.429/1992), Lei de Lavagem de Dinheiro (Lei n. 9.613/1998), Lei Geral de Proteção de Dados – LGPD (Lei 13.709/2018), além de normas das agências reguladoras (ANVISA, CVM, ANEEL e outras), que exigem programas de *compliance* setorial.

Um programa de *compliance* robusto pode ser essencial para viabilizar a governança corporativa efetiva, exigindo práticas corporativas transparentes, responsáveis e sustentáveis. Dentre os principais princípios aplicáveis, temos a ética, integridade, prestação de contas e gestão de riscos.

Assim, o programa de *compliance*, para ter eficácia, deve ser adaptado ao setor de atuação da empresa e, construído sobre pilares fundamentais, destacando-se: a adoção de um código de conduta, construção de políticas internas, comprometimento da alta direção, treinamento e capacitação contínua, estabelecimento de um comitê de ética e sustentabilidade, a implantação de canais de denúncia voltados para questões de assédio, discriminação ou degradação ambiental e a realização do *due diligence* (diligência devida – procedimentos de apuração interna e aplicação de medidas disciplinares quando necessário), além de monitoramento e melhoria contínua, com auditorias periódicas e revisão de processos para assegurar a efetividade do programa.

Atendidos os pilares fundamentais, o programa de *compliance* traz diversos benefícios como a mitigação de riscos legais e sanções administrativas, redução de danos reputacionais associados a escândalos e investigações, melhoria na governança corporativa, facilidade no acesso a capital e financiamentos internacionais, além de vantagens em processos licitatórios e contratos com o poder público. Apesar de tais benefícios, as organizações enfrentam desafios na implantação do programa, uma vez que há resistência cultural à mudança, falta de recursos e pessoal qualificado, subvalorização dos riscos e dificuldade na mensuração do impacto do *compliance* sobre os resultados financeiros.

Nota-se, portanto, que um programa de *compliance*, bem estruturado, ultrapassa a ideia de mero cumprimento legal e se configura como um instrumento estratégico de gestão e proteção jurídica, uma vez que sua adoção é fundamental para garantir a perenidade, a ética e a responsabilidade empresarial.

Juliana Vale dos Santos

Conflitos Geopolíticos: Ataques Cibernéticos e Entidades Comerciais

Os ataques cibernéticos estão se tornando uma ferramenta cada vez mais comum em conflitos geopolíticos, com entidades comerciais frequentemente sendo alvos táticos. Esses ataques visam desestabilizar economias, minar a confiança nas instituições e criar caos em momentos de fragilidade nacional.

Evidências de Ataques Cibernéticos

Um relatório recente da NETSCOUT revelou que os ataques de negação de serviço distribuído (DDoS) se estabeleceram como um método predominante de conduzir guerras cibernéticas associadas a eventos sociopolíticos. Durante o segundo semestre de 2024, foram registrados mais de um milhão de ataques DDoS na América Latina, com o Brasil liderando com meio milhão de incidentes. Esses ataques mostraram uma forte conexão com conflitos sociais e políticos, como o aumento de 2.844% em Israel relacionado ao resgate de reféns e conflitos políticos.

Exemplos Notáveis

Conflito Rússia-Ucrânia: Desde o início do conflito, houve um aumento significativo nos ataques cibernéticos direcionados a infraestruturas críticas na Ucrânia, incluindo redes de energia e sistemas de comunicação.

Conflito Taiwan-China: A tensão entre Taiwan e China também resultou em uma série de ataques cibernéticos, com *hackers* chineses visando empresas taiwanesas para roubar informações sensíveis e desestabilizar a economia local.

Dicas de Prevenção

1. ***Utilize senhas fortes e autenticação em dois fatores:*** Senhas complexas e autenticação em dois fatores podem dificultar o acesso não autorizado.
2. ***Mantenha sistemas e softwares atualizados:*** Atualizações regulares corrigem falhas e brechas de segurança.
3. ***Educação corporativa:*** Treine colaboradores para reconhecer e evitar ameaças cibernéticas, como *phishing* e *links* suspeitos.
4. ***Criptografia de dados:*** Codifique informações sensíveis para que, mesmo em caso de roubo, os dados permaneçam inacessíveis.
5. ***Uso de firewalls e softwares de proteção:*** Implemente *firewalls* e *softwares* de proteção como antivírus e anti-*malware* para monitorar e bloquear atividades suspeitas.

A crescente ligação entre ataques cibernéticos e conflitos geopolíticos destaca a importância de uma postura proativa em cibersegurança. Estar preparado e informado é crucial para proteger entidades comerciais e garantir a estabilidade em tempos de crise.

Referências

[1] TI Inside
[2] Valor Agregado
[3] TecMundo

Denis Rodrigo de Lima
Coordenador de TI

EXPEDIENTE

Juliana Vale dos Santos
Coordenadora jurídica

Rafael Rodrigues Raez
Advogado

Stephany Villalpando Gomez
Advogada

Ana Laura Costa
Assistente jurídica

Bruna San Gregório
Coordenadora editorial

Bruna Diseró
Assistente editorial

Cintia Machado dos Santos
Analista editorial

Acesse online:
https://saocamilo-sp.br/InformativoLegal
E-mail: secretariapublica@saocamilo-sp.br

CENTRO UNIVERSITÁRIO SÃO CAMILO