

Saúde mental nas empresas: responsabilidade jurídica e estratégica

José dos Santos Santana Jr. (*)

A saúde mental no ambiente de trabalho deixou de ser uma preocupação periférica e assumiu status de obrigação legal e estratégica para as empresas

Em um cenário de crescente judicialização das relações trabalhistas, organizações que negligenciam o bem-estar emocional de seus funcionários estão cada vez mais expostas a sanções civis, trabalhistas e até penais.

A atualização da Norma Regulamentadora nº 1 (NR-1), por meio da Portaria nº 6.730/2020, tornou obrigatória a adoção do Programa de Gerenciamento de Riscos (PGR), que inclui, de forma expressa, os riscos psicossociais. Isso abrange pressões abusivas, metas inatingíveis, sobrecarga de trabalho, ausência de pausas, ambientes tóxicos e práticas de assédio moral — fatores que devem ser mapeados, controlados e prevenidos com o mesmo rigor aplicado a riscos físicos, químicos e ergonômicos.

A omissão diante dessas exigências legais pode gerar indenizações por danos morais e materiais, além da obrigação de pensões vitalícias. A Justiça do Trabalho tem sido cada vez mais assertiva ao responsabilizar empresas cujas práticas resultam em adoecimento emocional dos trabalhadores.

Neste contexto, o compliance trabalhista assume

papel central. Mais do que formalidades e documentos arquivados, ele deve ser parte da governança empresarial, exigindo ações concretas como políticas internas consistentes, treinamentos contínuos, canais de escuta ativa e lideranças preparadas para gerir pessoas com responsabilidade.

Nenhuma dessas iniciativas, no entanto, se sustenta sem o suporte de uma assessoria jurídica especializada e integrada à estratégia empresarial. Um departamento jurídico comprometido com a governança não apenas reage a conflitos, mas atua de forma preventiva, garantindo que o PGR seja efetivo, que os códigos de conduta sejam aplicados e que a cultura organizacional promova segurança psicológica.

Tratar o jurídico como mera despesa é um equívoco que pode custar caro. Investir em uma assessoria técnica sólida significa proteger o patrimônio, blindar a reputação e garantir a sustentabilidade institucional.

Cuidar da saúde mental no trabalho não é uma escolha — é uma exigência legal e, sobretudo, um imperativo de inteligência empresarial. Empresas que promovem ambientes psicologicamente seguros não apenas cumprem a legislação: protegem seu ativo mais estratégico — o futuro.

(*) Advogado especialista em Direito Empresarial e da Saúde e sócio do escritório Mariano Santana Sociedade de Advogados.

Três conselhos para uma trajetória profissional de sucesso

Ricardo Rocha, CEO da acaso, acredita que é essencial saber tirar o melhor da tecnologia e desenvolver as habilidades que nos tornam humanos

De acordo com a pesquisa “Workpulse 2024”, da Randstad Brasil, 70% dos profissionais em 34 mercados pelo mundo consideram a progressão de carreira um dos critérios mais importantes ao avaliar um ambiente de trabalho.

No atual cenário que vivemos, que está em constante evolução, estar sempre aprendendo e adaptar-se rapidamente às mudanças faz toda a diferença, garantindo destaque e maior valorização no mercado. “Não basta apenas usar as ferramentas para ser produtivo, é preciso investir em competências como comunicação, empatia, pensamento crítico e liderança, que ajudam a trabalhar melhor em equipe e a resolver problemas de forma criativa. É importante também saber tirar o melhor das tecnologias e, ao mesmo tempo, desenvolver habilidades que nos fazem humanos”, comenta Ricardo Rocha, CEO da acaso, empresa com foco no futuro do trabalho.

Pensando nisso, o especialista elencou três dicas para ter sucesso profissional em 2025. Confira:

1) Mapeie os seus processos e atividades e entenda quais Inteligências Artificiais (IA) podem te ajudar

Um dado divulgado pela Freshworks, líder no fornecimento de soluções SaaS, mostrou que 71% dos empregadores dariam preferência a um candidato com menos experiência, contanto que ele tivesse conhecimento em IA. O que evidencia que não é apenas sobre melhorar entregas e fazer mais em menos tempo, as companhias estão priorizando também essas competências. “Os profissionais



precisarão inserir IA na sua rotina. Essas tecnologias serão aliadas na potencialização das habilidades humanas, incluindo a criação de prompts, automações e a capacidade de treinar a ferramenta. Hoje, já existem sites como “There is an AI for that”, que mapeiam as atividades e mostram qual IA pode auxiliar em determinada tarefa”, comenta o executivo.

2) Desenvolva conexões e habilidades humanas

Com a tecnologia evoluindo cada vez mais rápido, as empresas precisarão olhar principalmente para as flex skills, que são as habilidades mais transversais, intrínsecas às pessoas e que precisam ser desenvolvidas. “O diferencial estará justamente nas skills essencialmente humanas, que máquinas ainda não conseguem replicar. É sobre conexão consigo mesmo, entre colegas e com o propósito do que você faz. Saber trabalhar com IA é diferente de se tornar uma e o mercado pede pessoas cada vez mais autênticas, criativas e capazes de criar conexões genuínas”, explica Rocha.

3) Conheça-se profundamente e aprenda a se autoliderar

As pessoas estão cada vez mais desconectadas de si mesmas e isso gera várias consequências, entre elas a sensação de frustração com o trabalho. Existem diversos fatores para isso, mas certamente quem não se conhece está mais distante de encontrar os melhores caminhos para a própria carreira. “O processo de autoconhecimento é contínuo e requer uma segunda camada: a autogestão e a autoliderança. As organizações estão fazendo movimentos para se tornarem mais horizontais e isso vai demandar que os talentos consigam liderar a si mesmos”, finaliza o executivo.

Nova ameaça sequestra domínios respeitáveis

O sequestro de subdomínios por meio de recursos abandonados da nuvem é um problema que provavelmente todas as grandes organizações já enfrentaram, e esses ataques estão em ascensão. A Infoblox Threat Intel rastreou parte dessa atividade até um hacker, chamado Hazy Hawk, que usa domínios sequestrados para realizar golpes em larga escala e distribuir malware. Esta descoberta destaca a necessidade crítica das organizações gerenciarem seus registros de DNS e recursos da nuvem com vigilância.

Quem é Hazy Hawk?

Hazy Hawk é um agente sofisticado que sequestra registros DNS esquecidos de serviços de nuvem descontinuados, como buckets do Amazon S3 e endpoints do Azure. Ao assumir o controle desses recursos abandonados, o Hazy Hawk consegue hospedar URLs maliciosos que

levam usuários desavisados a golpes e malware.

Identificar registros de DNS vulneráveis na nuvem é significativamente mais desafiador do que identificar domínios comuns não registrados. À medida que o uso da nuvem cresceu, o número de recursos abandonados do tipo “lançar e esquecer” disparou. Especialmente para as empresas que não utilizam uma solução abrangente de visibilidade e gestão para controlar todos os seus patrimônios digitais.

O Hazy Hawk sequestrou com sucesso subdomínios de organizações respeitáveis, incluindo o Centro de Controle de Doenças dos EUA (CDC), várias agências



governamentais, universidades e empresas internacionais desde dezembro de 2024.

Detalhes do Hazy Hawk:

• **Técnicas sofisticadas:** ao contrário dos sequestradores de domínio tradicionais, o Hazy Hawk tem como alvo as configurações incorretas de DNS na nuvem

e deve ter acesso a serviços comerciais de DNS passivo para fazer isso;

• **Impacto de amplo alcance:** os domínios sequestrados são usados para distribuir uma variedade de golpes, incluindo anúncios falsos e notificações push maliciosas, afetando milhões de usuários em todo o mundo;

• **Consequências econômicas:** os golpes facilitados pelo Hazy Hawk contribuem para o mercado de fraudes multibilionário, com perdas financeiras significativas reportadas, especialmente entre a população idosa nos Estados Unidos;

• **Ofuscação:** Hazy Hawk usa defesas em camadas para proteger

suas operações, incluindo sequestro de domínios confiáveis, ofuscação de URLs e redirecionamento de tráfego por meio de vários domínios.

Medidas de Proteção

Para prevenir agentes de ameaças como o Hazy Hawk, as organizações devem implementar práticas robustas de gerenciamento de DNS, incluindo auditorias regulares de registros de DNS e a remoção imediata de registros associados a serviços de nuvem descontinuados. Além disso, os usuários devem ser orientados a negar solicitações de notificações push de sites desconhecidos para evitar serem vítimas de golpes. Para mais informações sobre o Hazy Hawk, leia o blog da pesquisa completa em (<https://blogs.infoblox.com/threat-intelligence/cloudy-with-a-chance-of-hijacking-forgotten-dns-records-enable-scam-actor/>).