

Inteligência Artificial e a Gestão de Riscos Psicossociais: Um Guia Estratégico para Conformidade com a NR-1 e Inovação no Ambiente de Trabalho Brasileiro

Sumário Executivo

A recente e imperativa evolução da legislação trabalhista brasileira, consolidada pela Norma Regulamentadora nº 1 (NR-1) e pela Lei 14.457/2022, representa um ponto de inflexão estratégico para a gestão corporativa. A exigência explícita de identificar, avaliar e, crucialmente, controlar os riscos psicossociais no ambiente de trabalho transcende a mera formalidade documental, demandando uma abordagem proativa e mensurável que os métodos tradicionais de gestão de Saúde e Segurança do Trabalho (SST) lutam para oferecer em escala. Neste cenário, os Modelos de Linguagem Avançados (LLMs), como o Google Gemini, emergem não como uma novidade futurista, mas como uma classe de ferramentas de controle viáveis e potencialmente superiores, enquadráveis como Controles de Engenharia e Administrativos.

Este relatório apresenta uma análise aprofundada de como estas tecnologias de Inteligência Artificial (IA) podem ser funcionalmente implementadas para atender a este novo paradigma regulatório. Demonstra-se como LLMs podem atuar diretamente na mitigação de fatores de risco como sobrecarga cognitiva, através da automação de tarefas; na prevenção de conflitos e assédio, ao fomentar uma comunicação mais saudável e fornecer canais de denúncia seguros; e no fortalecimento da segurança psicológica, ao oferecer suporte personalizado ao desenvolvimento de competências.

A análise detalha o processo de documentação dessas ferramentas no Programa de Gerenciamento de Riscos (PGR), propondo metodologias para avaliar sua eficácia e demonstrar conformidade. O potencial de Retorno sobre o Investimento (ROI) é explorado, conectando a implementação da IA à redução de custos tangíveis, como absenteísmo e rotatividade, e ao aumento da produtividade. Finalmente, o relatório aborda com seriedade os desafios críticos inerentes à tecnologia — privacidade de

dados, vieses algorítmicos e barreiras culturais à implementação —, defendendo que um framework de governança ética robusto não é um obstáculo, mas um acelerador para uma adoção bem-sucedida. O objetivo é fornecer aos líderes corporativos brasileiros um guia estratégico para navegar neste novo cenário, transformando uma obrigação legal em uma vantagem competitiva sustentável.

Seção 1: O Novo Paradigma Regulatório: Riscos Psicossociais na Legislação Trabalhista Brasileira

O cenário de Saúde e Segurança do Trabalho (SST) no Brasil atravessa uma transformação fundamental. A inclusão formal e explícita dos fatores de risco psicossociais no escopo das obrigações legais das empresas representa uma mudança de paradigma, movendo o foco da SST para além dos riscos físicos, químicos e biológicos, e reconhecendo o impacto da organização do trabalho na saúde mental dos colaboradores. Esta evolução não é um mero adendo à legislação, mas uma redefinição do que constitui um ambiente de trabalho seguro e saudável.

Análise da Evolução da NR-1

A Norma Regulamentadora nº 1 (NR-1) serve como a espinha dorsal do sistema de SST brasileiro, estabelecendo as disposições gerais para o Gerenciamento de Riscos Ocupacionais (GRO).¹ A sua atualização mais significativa é a determinação de que as organizações devem, em seu processo de GRO, "considerar as condições de trabalho, nos termos da NR-17, incluindo os fatores de risco psicossociais relacionados ao trabalho".² Este mandato consolida a obrigação de as empresas passarem por todas as etapas do GRO — identificar perigos, avaliar riscos, classificá-los, adotar medidas de prevenção e acompanhar o controle — também para os riscos de natureza psicossocial.³

A formalização definitiva desta obrigação ocorreu com a Portaria MTE nº 1.419, de 27 de agosto de 2024, que alterou o capítulo 1.5 da NR-1 para incluir expressamente os fatores de risco psicossociais no Programa de Gerenciamento de Riscos (PGR).⁵ Com vigência a partir de maio de 2025, inicialmente em caráter educativo e orientativo⁶, esta mudança impactará milhões de estabelecimentos empregadores no Brasil.⁷ Para guiar esta transição, o Ministério do Trabalho e Emprego (MTE) publicou o "Guia de Informações sobre os Fatores de Riscos Psicossociais Relacionados ao Trabalho", um

documento orientador que detalha como as empresas devem proceder.³

Esta evolução legislativa não deve ser vista como um fardo, mas como um alinhamento do Brasil com as melhores práticas e padrões internacionais, como a ISO 45003, que trata especificamente da gestão de riscos psicossociais. A legislação reconhece que a saúde mental é um componente indissociável da saúde do trabalhador e que a sua negligência acarreta custos significativos para as empresas e para a sociedade, através de absenteísmo, presenteísmo, queda de produtividade e aumento de doenças ocupacionais.

A Centralidade da NR-17 (Ergonomia)

Um ponto crucial da nova regulamentação é a forma como ela conecta a gestão dos riscos psicossociais à Norma Regulamentadora nº 17 (Ergonomia). A NR-1 estipula que o processo de GRO deve considerar as condições de trabalho "nos termos da NR-17".² O guia do MTE reforça esta conexão ao definir que os riscos psicossociais decorrem de "problemas na concepção, organização e gestão do trabalho".³

Esta vinculação é estrategicamente importante. Ela impede que as organizações tentem cumprir a norma através de medidas superficiais e de baixa eficácia, como programas de bem-estar focados exclusivamente no indivíduo (por exemplo, aulas de ioga ou aplicativos de meditação). Embora possam ter seu valor, essas são, na hierarquia de controle de riscos, medidas terciárias, que não atuam na fonte do problema. A lei exige uma intervenção primária, na origem do risco, que reside na forma como o trabalho é desenhado, distribuído e gerenciado. Fatores como volume de trabalho, clareza de papéis, autonomia, padrões de comunicação e estilo de liderança tornam-se, assim, objetos centrais da análise e do controle de riscos. É precisamente nestas áreas sistêmicas que as ferramentas de IA podem oferecer um impacto transformador.

Análise da Lei 14.457/2022 e o Novo Papel da CIPA

Paralelamente à evolução da NR-1, a Lei nº 14.457, de 21 de setembro de 2022, promoveu uma mudança fundamental no papel da Comissão Interna de Prevenção de Acidentes, que passou a se chamar "Comissão Interna de Prevenção de Acidentes e de Assédio" (CIPA).⁵ Esta alteração legislativa não foi meramente nominal; ela atribuiu à CIPA responsabilidades diretas e concretas na prevenção e combate ao assédio e

outras formas de violência no trabalho.

O Artigo 23 da lei determina que as empresas com CIPA devem adotar um conjunto de medidas obrigatórias, incluindo ⁸:

1. **Inclusão de regras de conduta** sobre assédio e violência nas normas internas da empresa, com ampla divulgação.
2. **Fixação de procedimentos para recebimento e acompanhamento de denúncias**, garantindo o anonimato do denunciante.
3. **Inclusão de temas sobre prevenção ao assédio** nas atividades e práticas rotineiras da CIPA.
4. **Realização de ações de capacitação e sensibilização**, no mínimo anualmente, para todos os níveis hierárquicos da empresa.

Esta lei transforma a prevenção ao assédio em um processo formal, sistemático e auditável, integrando as ações da CIPA diretamente às políticas internas e ao PGR da empresa.⁴ A exigência de um canal de denúncias eficaz e anônimo, em particular, representa um desafio para muitas organizações que dependem de métodos ultrapassados e, ao mesmo tempo, abre uma oportunidade clara para a implementação de soluções tecnológicas avançadas.

A confluência dessas mudanças legislativas cria um novo cenário onde a "conformidade passiva" — a mera atualização de documentos do PGR para incluir a palavra "estresse" — é insuficiente e arriscada. A fiscalização do MTE será cada vez mais orientada por dados, focando em setores com alta incidência de adoecimento mental, como teleatendimento e bancos, e analisando indicadores como taxas de afastamento por ansiedade e depressão.⁷ Empresas que não puderem demonstrar a implementação de medidas de controle tangíveis e sistêmicas, que atuem na organização do trabalho, estarão em não conformidade.

Ao mesmo tempo, a legislação, embora exigente em seus objetivos, é intencionalmente não prescritiva quanto aos métodos de controle a serem adotados. O próprio guia do MTE afirma que não cabe ao órgão definir ou sugerir uma metodologia específica, deixando esta decisão a cargo da organização e de seus profissionais de SST.³ Este vácuo metodológico cria uma oportunidade estratégica. Enquanto métodos tradicionais como workshops e consultorias são frequentemente caros, de difícil escalabilidade e de eficácia complexa de se quantificar, as ferramentas baseadas em IA oferecem, por sua natureza, escalabilidade para milhares de colaboradores e a geração de dados de uso que podem servir como base para a aferição de eficácia. Assim, a tecnologia surge como uma solução poderosa para preencher essa lacuna, oferecendo um caminho para uma conformidade

escalável, data-driven e, em última análise, mais eficaz.

Seção 2: A Inteligência Artificial como Medida de Controle de Engenharia e Administrativa

Para que a implementação de Modelos de Linguagem Avançados (LLMs) seja estratégica e defensável sob a ótica da legislação de SST, é fundamental enquadrá-los corretamente dentro da hierarquia de controle de riscos. Esta hierarquia, um princípio universal da segurança do trabalho, prioriza as ações de prevenção da mais eficaz para a menos eficaz: Eliminação, Substituição, Controles de Engenharia, Controles Administrativos e, por último, Equipamentos de Proteção Individual (EPI). No contexto dos riscos psicossociais, a categoria de EPI é conceitualmente inaplicável. O foco, portanto, recai sobre os controles de engenharia e administrativos, onde a IA pode ser posicionada de forma inovadora e robusta.

Enquadramento Teórico na Hierarquia de Controle de Riscos

A NR-1, em si, não oferece definições detalhadas para cada tipo de controle², mas adota os conceitos consagrados na prática de SST. O guia do MTE sobre riscos psicossociais orienta que as organizações devem implementar "medidas de prevenção" seguindo uma ordem de prioridade, o que remete diretamente a esta hierarquia.³

Classificar uma solução de IA como um controle de engenharia ou administrativo não é um mero exercício semântico. É uma decisão estratégica que eleva a tecnologia de uma simples "ferramenta de TI" ou "aplicativo de produtividade" para um componente integral da estratégia de conformidade e segurança da empresa. Essa classificação justifica o investimento, formaliza sua inclusão no PGR e alinha diferentes departamentos (RH, Jurídico, SST, TI) em torno de um objetivo comum de mitigação de riscos.

LLMs como Controle de Engenharia

Um controle de engenharia é uma medida que modifica o ambiente, as ferramentas ou os processos de trabalho para eliminar ou reduzir a exposição a um perigo na sua

fonte. A intervenção é feita no sistema, não no comportamento do trabalhador.

Quando um LLM é integrado diretamente ao ambiente de trabalho digital para alterar fundamentalmente as ferramentas e os fluxos de trabalho, ele atua como um controle de engenharia. A ferramenta de trabalho em si é redesenhada para ser intrinsecamente mais segura do ponto de vista psicossocial.

- **Exemplo Prático:** Considere o risco psicossocial de "sobrecarga de trabalho", especificamente o fator de "sobrecarga cognitiva".¹¹ Uma ferramenta de IA, como a Supernormal, que se integra a plataformas de reunião para transcrever conversas, gerar atas e destacar pontos de ação automaticamente, é um controle de engenharia.¹² O colaborador não precisa mais dividir sua atenção entre participar ativamente da discussão e tomar notas freneticamente. A ferramenta foi re-engenheirada para reduzir a carga mental. Da mesma forma, um LLM que sumariza automaticamente longas cadeias de e-mails ou relatórios densos modifica o processo de consumo de informação, atacando diretamente o perigo da saturação informacional.

LLMs como Controle Administrativo

Controles administrativos são mudanças nos procedimentos, nas políticas ou nas práticas de trabalho. Eles alteram a *forma como as pessoas trabalham* através de treinamento, sinalização, regras e diretrizes.

Quando um LLM é utilizado para treinar, guiar ou apoiar os colaboradores na adoção de procedimentos de trabalho mais seguros psicologicamente, ele funciona como um controle administrativo.

- **Exemplo Prático:** O risco de "más relações no local de trabalho" ou "assédio"³ é frequentemente exacerbado por uma comunicação agressiva ou ineficaz. Um assistente de IA que ajuda um gestor a redigir um feedback, analisando o texto e sugerindo alterações com base nos princípios da Comunicação Não Violenta (CNV), é um controle administrativo.¹³ A ferramenta não executa a tarefa pelo gestor, mas o treina em tempo real para seguir um procedimento de comunicação mais seguro. Outro exemplo claro é um chatbot de IA que atua como um tutor personalizado para o desenvolvimento de novas competências (*upskilling*), alterando o procedimento administrativo de treinamento e desenvolvimento da empresa para torná-lo mais acessível e contínuo.¹⁵

Validação Legal e Precedentes

A questão da validade de uma ferramenta de software como medida de controle no PGR encontra respaldo na própria regulamentação. A NR-1 permite que o PGR seja gerenciado "por meio de documentos físicos ou por sistema eletrônico" ¹⁶, estabelecendo que a gestão da segurança pode ser digital.

Mais diretamente, a norma prevê, em seu item 1.8.3, que microempresas e empresas de pequeno porte que optarem por não constituir um SESMT podem utilizar "ferramenta(s) de avaliação de risco a serem disponibilizada(s) pela SEPRT" (Secretaria Especial de Previdência e Trabalho) para estruturar seu PGR.¹⁷ Este ponto cria um precedente inequívoco: se o próprio governo federal prevê o uso de ferramentas de software para a *avaliação* de riscos, é perfeitamente coerente e legalmente defensável que uma organização utilize e documente uma ferramenta de software mais sofisticada (um LLM) como uma medida de *controle* de riscos dentro do mesmo sistema de gerenciamento.

A capacidade de uma única plataforma de IA operar simultaneamente como controle de engenharia e administrativo oferece uma flexibilidade estratégica notável. Uma ferramenta como o Microsoft Copilot ou o Google Gemini pode, ao mesmo tempo, automatizar a criação de apresentações a partir de um documento (controle de engenharia, reduzindo a carga de trabalho) e ajudar um colaborador a escrever um e-mail de solicitação de forma mais clara e empática (controle administrativo, melhorando a comunicação). Isso significa que um único investimento tecnológico pode ser documentado no PGR como uma solução multifacetada, abordando múltiplos riscos psicossociais através de diferentes mecanismos de controle. Esta dupla funcionalidade fortalece o caso de negócio e o ROI, apresentando uma solução integrada e eficiente para um problema complexo.

Seção 3: Aplicações Funcionais de LLMs na Mitigação de Riscos Psicossociais

A aplicação de Modelos de Linguagem Avançados (LLMs) na gestão de riscos psicossociais transcende a teoria e se materializa em funcionalidades práticas que podem ser integradas aos processos de trabalho existentes. Estas aplicações atuam

diretamente sobre os fatores de risco identificados pela legislação e pela literatura especializada, como sobrecarga, comunicação inadequada e falta de desenvolvimento.

Subseção 3.1: Redução da Sobrecarga Cognitiva e Estresse

A sobrecarga de trabalho, tanto em volume quanto em complexidade, é um dos estressores mais prevalentes no ambiente corporativo moderno e um fator de risco psicossocial explicitamente citado no guia do MTE.³ A carga cognitiva, que é o esforço mental total necessário para executar uma tarefa, é um componente central deste risco.¹¹ Os LLMs oferecem soluções diretas e eficazes para mitigar essa carga.

Ferramentas de IA podem ser empregadas para automatizar tarefas repetitivas e cognitivamente exigentes. A capacidade de transcrever reuniões em tempo real, sumarizar os pontos discutidos e extrair itens de ação é uma das aplicações mais maduras.¹² Ao delegar a tarefa de anotação a um assistente de IA, os colaboradores podem se concentrar totalmente na discussão, melhorando a qualidade da colaboração e reduzindo o estresse de ter que processar e registrar informações simultaneamente.

Além das reuniões, os LLMs podem ser configurados para analisar e resumir longas cadeias de e-mails, relatórios extensos, documentos técnicos ou artigos complexos. Em vez de um colaborador passar horas lendo e decifrando informações, a IA pode fornecer um resumo conciso com os pontos-chave em segundos. Esta funcionalidade ataca diretamente a sobrecarga de informação, um dos principais contribuintes para o estresse e o burnout. Ao reduzir o tempo e o esforço mental dedicados a tarefas de baixo valor agregado, a IA libera capacidade cognitiva para atividades mais estratégicas e criativas, aumentando a produtividade e o bem-estar.

Subseção 3.2: Fomento à Comunicação Saudável e Prevenção de Conflitos

A qualidade da comunicação interpessoal é um pilar para um ambiente de trabalho psicologicamente seguro. Comunicação agressiva, ambígua ou ineficaz é uma fonte primária de conflitos, mal-entendidos e pode escalar para situações de assédio moral, configurando um grave risco psicossocial.³ Os LLMs podem ser utilizados como ferramentas de apoio para promover uma cultura de comunicação mais consciente e construtiva.

Uma aplicação de alto impacto é o treinamento e coaching em tempo real para líderes e colaboradores sobre Comunicação Não Violenta (CNV). A CNV é uma abordagem que visa promover relações mais empáticas e eficazes.¹⁸ Um assistente de IA pode ser integrado a plataformas de e-mail ou chat para analisar rascunhos de mensagens e oferecer sugestões para torná-las mais construtivas, focadas em observações (fatos), sentimentos, necessidades e pedidos claros, em vez de julgamentos ou críticas.¹³ Isso não apenas melhora a qualidade de uma interação específica, mas serve como um processo de aprendizagem contínuo para o usuário.

Adicionalmente, em linha com as novas obrigações da CIPA estabelecidas pela Lei 14.457/2022⁸, um chatbot baseado em LLM pode funcionar como um canal de denúncias inicial, seguro e anônimo. Muitos colaboradores hesitam em reportar microagressões ou desconfortos por medo de retaliação ou por não saberem a quem recorrer. Um chatbot oferece um espaço confidencial para que o colaborador possa relatar um incidente, receber informações sobre os próximos passos e ter seu relato documentado sem a necessidade de uma interação humana imediata.²¹ Isso permite que a organização identifique e intervenha em problemas em estágio inicial, antes que se transformem em crises de assédio ou conflitos graves.

Subseção 3.3: Suporte ao Desenvolvimento de Competências e Segurança Psicológica

A percepção de competência e a oportunidade de crescimento são fatores de proteção contra riscos psicossociais. Sentir-se estagnado, inadequado ou com habilidades obsoletas pode gerar ansiedade e insegurança. A segurança psicológica, definida como a crença de que um indivíduo não será punido ou humilhado por falar, fazer perguntas, expressar preocupações ou cometer erros, é fundamental para a inovação e o bem-estar.²²

Os LLMs podem desempenhar um papel transformador nesta área, funcionando como tutores personalizados e escaláveis. Uma plataforma de IA pode criar trilhas de aprendizagem individualizadas para o *upskilling* e *reskilling* dos colaboradores, adaptando-se ao ritmo e ao nível de conhecimento de cada um.¹⁵ Um colaborador que precisa desenvolver uma nova habilidade técnica ou uma *soft skill* pode interagir com um tutor de IA, fazendo perguntas, realizando exercícios e recebendo feedback imediato em um ambiente livre de julgamento.

Este ambiente de aprendizado seguro é um impulsionador direto da segurança psicológica. O colaborador pode "perguntar o óbvio" ou "errar sem medo" diante da

IA, algo que talvez hesitasse em fazer diante de um superior ou de colegas.¹⁵ Ao aumentar a percepção de competência e autoeficácia e ao fornecer um espaço seguro para a experimentação e o aprendizado, a empresa não apenas mitiga riscos psicossociais, mas também fomenta uma cultura de aprendizado contínuo e inovação, conectando diretamente a estratégia de SST à de gestão de talentos.

A implementação bem-sucedida dessas aplicações requer uma abordagem estratégica e faseada. É recomendável que as organizações comecem com as funcionalidades de menor sensibilidade e maior impacto percebido, como a automação de tarefas (Subseção 3.1). Isso gera "vitórias rápidas", demonstra o valor da tecnologia e constrói a confiança dos colaboradores. Uma vez que a IA é vista como uma aliada útil, a resistência cultural para adotar aplicações mais sensíveis, como o coaching de comunicação (Subseção 3.2) ou o desenvolvimento pessoal (Subseção 3.3), tende a diminuir significativamente. Iniciar o processo com uma ferramenta que analisa a comunicação interpessoal, por exemplo, poderia ser percebido como vigilância e comprometer toda a iniciativa. O design da interação humano-IA é, portanto, determinante: a mesma tecnologia pode capacitar ou criar novos estressores. O foco deve ser invariavelmente em aumentar a capacidade e oferecer suporte ao colaborador, e não em monitorar e julgar seu desempenho.²⁵

Seção 4: Integração e Documentação no Programa de Gerenciamento de Riscos (PGR)

A implementação de uma ferramenta de IA como medida de controle de riscos psicossociais só atinge a plena conformidade legal quando é devidamente integrada e documentada no Programa de Gerenciamento de Riscos (PGR) da organização. Este processo formaliza a tecnologia como parte da estratégia de SST, permitindo sua gestão, monitoramento e apresentação em caso de fiscalização.

Documentando a Medida de Controle

O PGR, conforme a NR-1, deve ser composto, no mínimo, por dois documentos centrais: o **Inventário de Riscos Ocupacionais** e o **Plano de Ação**.¹⁶ A documentação da medida de controle baseada em IA deve ser inserida de forma clara em ambos.

No **Inventário de Riscos**, que consolida a identificação de perigos e a avaliação de

riscos, a ferramenta de IA deve ser listada como uma "medida de prevenção implementada".²⁶ A descrição deve ser específica, conectando o risco à solução tecnológica.

- **Exemplo de Linguagem para o Inventário de Riscos:**
 - **Perigo:** Organização do trabalho com alto volume de comunicação digital e reuniões consecutivas.
 - **Risco Ocupacional:** Estresse crônico relacionado à sobrecarga cognitiva e informacional.
 - **Grupo de Trabalhadores Expostos:** Equipes de gestão e análise de projetos.
 - **Descrição da Medida de Prevenção Implementada (Controle de Engenharia):** "Implementação da plataforma de IA [Nome da Ferramenta] integrada aos sistemas de e-mail e calendário da empresa. A ferramenta automatiza a transcrição e sumarização de atas de reunião e a síntese de longas cadeias de e-mails, reduzindo a carga de processamento de informação exigida dos colaboradores."

No **Plano de Ação**, que detalha as medidas a serem introduzidas, aprimoradas ou mantidas, a implementação da IA deve ser tratada como um projeto, com cronograma, responsáveis e formas de acompanhamento.³

- **Exemplo de Linguagem para o Plano de Ação:**
 - **Ação:** Implementar módulo de coaching de Comunicação Não Violenta (CNV) na plataforma de IA [Nome da Ferramenta].
 - **Objetivo:** Reduzir incidentes de comunicação agressiva e melhorar o clima interpessoal entre as lideranças.
 - **Responsável:** Departamento de RH em conjunto com o Departamento de TI.
 - **Prazo:** Implementação piloto no Q3; Expansão para toda a liderança no Q4.
 - **Forma de Aferição de Resultados:** Monitoramento da taxa de adesão ao módulo e análise de resultados de pesquisas de clima organizacional pré e pós-implementação.

Metodologia de Avaliação de Eficácia

Um componente essencial do ciclo do GRO é "acompanhar o controle dos riscos ocupacionais"³ e "monitorar regularmente a eficácia das medidas de controle implementadas".²⁷ Para uma medida de controle baseada em IA, esta avaliação pode ser particularmente robusta, pois a tecnologia gera dados de uso que permitem uma análise quantitativa. A metodologia de avaliação deve ser multifacetada, combinando

indicadores de processo e de resultado.²⁸

1. **Indicadores de Processo (Leading Indicators):** Medem se a medida de controle está sendo efetivamente utilizada. Eles são preditivos e indicam a adesão à nova prática.
 - *Exemplos:* Percentual de gestores que utilizaram o assistente de feedback de CNV no último mês; número de resumos de reunião gerados automaticamente por semana; horas de trabalho economizadas com automação de tarefas; taxa de conclusão dos módulos de *upskilling* personalizados. Estes dados mostram que a ferramenta está ativa e integrada ao fluxo de trabalho.
2. **Indicadores de Resultado (Lagging Indicators):** Medem o impacto real da medida de controle sobre o risco que se propõe a mitigar. Eles olham para o passado para avaliar o efeito.
 - *Exemplos:* Comparação dos resultados de pesquisas de pulso sobre percepção de carga de trabalho antes e depois da implementação da ferramenta; redução no número de queixas formais ou informais sobre conflitos interpessoais; diminuição nas taxas de absenteísmo e rotatividade (turnover) em departamentos que adotaram a ferramenta ²⁹; melhora nos scores de engajamento e clima organizacional.³¹

A combinação desses dois tipos de indicadores fornece uma visão completa da eficácia. Os indicadores de processo demonstram que a medida está em vigor, enquanto os indicadores de resultado comprovam seu impacto na saúde e segurança dos trabalhadores. Esta abordagem data-driven é extremamente valiosa para justificar o investimento contínuo na tecnologia e para demonstrar conformidade de forma inequívoca.

Tabela Proposta: Mapeamento de Riscos Psicossociais, Controles baseados em LLM e Classificação no PGR

A tabela a seguir serve como um guia prático para que as equipes de SST e RH possam mapear os riscos, selecionar as soluções de IA apropriadas e planejar sua documentação e mensuração.

Risco Psicossocial Identificado	Fator de Risco Específico (Causa Raiz)	Aplicação do LLM (Solução Tecnológica)	Mecanismo de Ação do Controle	Classificação do Controle (NR-1)	Métricas de Eficácia (Leading / Lagging)
---------------------------------	--	--	-------------------------------	----------------------------------	--

(Guia MTE)					
Sobrecarga de Trabalho	Volume excessivo de e-mails, relatórios e reuniões consecutivas.	Assistente de IA para sumarização, transcrição e automação de relatórios.	Reduz a carga cognitiva e o tempo gasto em tarefas de baixo valor agregado.	Engenharia	Leading: Nº de tarefas automatizadas/s emana. Lagging: Redução de X% no auto-relato de estresse por sobrecarga.
Más Relações / Assédio Moral	Comunicação agressiva ou ineficaz por parte da liderança.	Módulo de treinamento e coaching em tempo real para Comunicação o Não Violenta (CNV).	Modifica o procedimento de comunicação, ensinando práticas mais construtivas.	Administrativo	Leading: % de gestores utilizando a ferramenta de feedback. Lagging: Redução no nº de queixas de conflito interpessoal.
Falta de Suporte / Baixa Clareza de Papel	Dificuldade em encontrar informações e procedimentos internos.	Base de conhecimento inteligente (chatbot) que responde a perguntas sobre políticas e processos.	Melhora o acesso à informação e a autonomia do colaborador.	Engenharia	Leading: Nº de consultas respondidas pelo chatbot. Lagging: Aumento na percepção de suporte organizacional em pesquisas.
Baixo Controle / Autonomia	Falta de oportunidades para desenvolvimento de novas habilidades.	Plataforma de <i>upskilling</i> com tutores de IA personalizados.	Aumenta a competência e a percepção de controle sobre a própria carreira.	Administrativo	Leading: Taxa de engajamento e conclusão de cursos. Lagging: Redução da taxa de turnover por falta de desenvolvimento.
Violência / Assédio (Lei 14.457/22)	Medo de retaliação impede o relato de incidentes.	Canal de denúncias anônimo e confidencial operado por	Fornecer um procedimento seguro e acessível para o recebimento de	Administrativo	Leading: Nº de relatos recebidos e processados. Lagging: Aumento da

		um chatbot de IA.	denúncias.		percepção de segurança para denunciar em pesquisas.
--	--	-------------------	------------	--	---

Seção 5: O Papel da CIPA na Era da Inteligência Artificial

A transformação da CIPA em "Comissão Interna de Prevenção de Acidentes e de Assédio" pela Lei 14.457/2022 não foi apenas uma mudança de nome, mas uma profunda ampliação de seu escopo e responsabilidades.⁵ Com um mandato explícito para atuar na prevenção de assédio e outras formas de violência psicológica, a CIPA se depara com a necessidade de ferramentas e metodologias que transcendem a tradicional inspeção de segurança física. Neste novo contexto, a Inteligência Artificial emerge como uma poderosa aliada, capaz de capacitar a comissão para cumprir suas novas obrigações de forma mais eficaz, estratégica e baseada em dados.

Capacitando a CIPA com Tecnologia

As novas atribuições da CIPA, detalhadas no Artigo 23 da Lei 14.457/22, incluem a implementação de "procedimentos para recebimento e acompanhamento de denúncias", com garantia de anonimato, e a realização de ações de capacitação e sensibilização.⁸ A tecnologia, especialmente as plataformas digitais, é vista como um facilitador essencial para a execução dessas tarefas.²¹

Uma das aplicações mais diretas e impactantes é o uso de um chatbot baseado em LLM para operar o canal de denúncias. Este sistema pode oferecer um nível de segurança, anonimato e disponibilidade que métodos tradicionais, como caixas de sugestão físicas ou endereços de e-mail genéricos, simplesmente não conseguem garantir.²¹ Um colaborador que se sinta vítima ou testemunha de assédio pode interagir com o chatbot a qualquer hora, de qualquer lugar, com a confiança de que sua identidade será preservada. O chatbot pode guiar o denunciante no relato, assegurando que informações cruciais sejam coletadas, documentar o caso de forma segura e criptografada, e encaminhá-lo automaticamente para o comitê responsável (que pode incluir membros da CIPA, RH e Compliance), cumprindo rigorosamente a exigência legal de um procedimento formal e anônimo.⁸

Além do canal de denúncias, a CIPA pode alavancar a IA em suas ações de prevenção. A comissão pode ativamente recomendar e promover o uso de ferramentas de

treinamento baseadas em LLM, que oferecem módulos sobre temas como Comunicação Não Violenta, vieses inconscientes, diversidade e inclusão. Esses treinamentos, por serem personalizados e interativos, tendem a ser mais eficazes do que palestras tradicionais. A CIPA pode, assim, cumprir sua obrigação de realizar "ações de capacitação, de orientação e de sensibilização" de forma mais moderna e engajadora.⁸

A adoção dessas tecnologias transforma fundamentalmente o papel da CIPA. Historicamente, em questões de comportamento, a comissão muitas vezes atuava de forma reativa, respondendo a incidentes já ocorridos. Com as ferramentas certas, a CIPA pode se tornar um agente de prevenção estratégico e proativo. A plataforma de denúncias, por exemplo, não serve apenas para registrar casos individuais. Ela pode agregar dados de forma anonimizada, gerando análises e dashboards que revelam padrões e tendências. A CIPA poderia, por exemplo, identificar um aumento no relato de microagressões em um determinado departamento ou um padrão de comunicação inadequada associado a uma equipe específica.

Munida dessas informações, a CIPA pode atuar de forma cirúrgica e preventiva. Em vez de uma campanha de conscientização genérica para toda a empresa, a comissão pode recomendar uma intervenção direcionada, como um workshop de liderança para os gestores daquele departamento específico ou uma revisão dos processos de trabalho daquela equipe. Essa abordagem baseada em dados torna as ações da CIPA mais eficientes, relevantes e capazes de gerar um impacto real na cultura organizacional, movendo a comissão de uma função de conformidade para um papel de parceira estratégica na construção de um ambiente de trabalho verdadeiramente saudável e seguro.

Seção 6: Análise de Impacto Organizacional: ROI e Vantagem Competitiva

A decisão de investir em tecnologias de IA para a gestão de riscos psicossociais deve ser sustentada por uma análise robusta de seu impacto organizacional, especialmente em termos de Retorno sobre o Investimento (ROI). Embora a conformidade legal seja o gatilho inicial, o verdadeiro valor da iniciativa reside em sua capacidade de gerar benefícios tangíveis e intangíveis que fortalecem a saúde financeira e a competitividade da empresa. O custo da inação, antes considerado "soft" e difícil de medir, agora se materializa em riscos legais e financeiros concretos,

tornando o cálculo do ROI ainda mais pertinente.

Calculando o Retorno Sobre o Investimento (ROI)

O cálculo do ROI para uma iniciativa de IA em SST psicossocial deve considerar tanto o "Investimento" quanto o "Retorno". O investimento inclui os custos de licenciamento da plataforma de IA, as horas de trabalho dedicadas à implementação, customização, treinamento e gestão da mudança. O retorno, por sua vez, é composto por uma série de ganhos que podem ser categorizados como "hard" (diretamente quantificáveis em termos financeiros) e "soft" (impactos estratégicos de longo prazo).

1. Custos Evitados (Hard ROI): Esta é a categoria mais direta de retorno financeiro.

- **Redução de Absenteísmo e Turnover:** Estudos indicam que programas eficazes de bem-estar podem levar a reduções significativas nas taxas de absenteísmo (até 30%) e turnover (até 40%).²⁹ O absenteísmo gera custos com a perda de produtividade e a necessidade de pagamento de horas extras ou substitutos. O turnover acarreta altos custos de recrutamento, seleção, integração e treinamento de novos colaboradores, além da perda de conhecimento institucional.³⁰ A redução desses índices, mesmo que modesta, se traduz em economias substanciais.
- **Mitigação de Riscos Legais:** A não conformidade com a NR-1 e a Lei 14.457/22 pode resultar em multas pesadas em caso de fiscalização. Além disso, um ambiente de trabalho com altos níveis de estresse e assédio aumenta exponencialmente o risco de ações trabalhistas por danos morais e doenças ocupacionais, que podem levar a indenizações vultosas e custos com advogados. A implementação de um sistema de controle robusto e documentado, como uma plataforma de IA, serve como uma forte evidência da devida diligência da empresa, reduzindo a probabilidade e o custo desses litígios.

2. Ganhos de Produtividade (Hard ROI):

- **Automação e Eficiência:** A automação de tarefas rotineiras e cognitivamente desgastantes (sumarização de e-mails, transcrição de reuniões, etc.) libera horas de trabalho dos colaboradores. Esse tempo pode ser realocado para atividades de maior valor agregado, como planejamento estratégico, inovação e relacionamento com clientes, gerando um ganho direto de produtividade.

3. Ganhos Intangíveis (Soft ROI): Embora mais difíceis de quantificar, estes ganhos são cruciais para a sustentabilidade e o sucesso a longo prazo.

- **Melhora do Employer Branding:** Empresas que investem ativamente na saúde mental de seus colaboradores e utilizam tecnologia de ponta para isso se tornam mais atraentes no mercado de talentos. Isso facilita a atração e retenção dos melhores profissionais, uma vantagem competitiva inestimável.
- **Aumento do Engajamento e Inovação:** Um ambiente psicologicamente seguro, onde os colaboradores se sentem apoiados e com menos estresse, é um terreno fértil para o engajamento, a criatividade e a inovação. Colaboradores engajados são mais produtivos e mais propensos a contribuir com ideias que impulsionam o negócio.
- **Fortalecimento da Cultura Organizacional:** A implementação de ferramentas que promovem comunicação saudável e desenvolvimento contínuo envia uma mensagem poderosa sobre os valores da empresa, fortalecendo uma cultura de respeito, confiança e aprendizado.

A análise do ROI deve, portanto, ir além de uma simples conta de custos versus benefícios diretos. Ela deve incorporar a perspectiva do gerenciamento de riscos, onde o "custo da não-ação" — representado por multas, processos judiciais, perda de talentos e queda de produtividade — é um fator decisivo. Sob essa ótica, o investimento em uma plataforma de IA para a gestão de riscos psicossociais deixa de ser uma despesa opcional de "bem-estar" e se torna um investimento estratégico essencial para a resiliência, a conformidade e a competitividade da organização no século XXI.

Seção 7: Navegando pelos Desafios: Riscos, Ética e Barreiras à Implementação

A adoção de Inteligência Artificial para gerenciar aspectos tão sensíveis quanto a saúde mental e as interações humanas no trabalho é uma jornada repleta de potencial, mas também de riscos significativos. Uma implementação bem-sucedida exige uma análise crítica e proativa dos desafios éticos, tecnológicos e culturais, especialmente no contexto brasileiro. Ignorar esses obstáculos não apenas compromete a eficácia da iniciativa, mas pode criar novos e mais complexos problemas.

Análise Crítica dos Riscos Tecnológicos e Éticos

A implementação de LLMs no ambiente de trabalho introduz uma série de dilemas éticos que devem ser gerenciados com o máximo rigor. A governança ética não deve ser vista como um freio ao progresso, mas como um acelerador da adoção, pois é a base para a construção da confiança necessária para que colaboradores e líderes utilizem as ferramentas de forma genuína.

- **Vieses Algorítmicos e Discriminação:** Os algoritmos de IA aprendem a partir dos dados com os quais são alimentados. Se esses dados refletem preconceitos históricos da sociedade ou da própria empresa (de gênero, raça, idade, etc.), a IA pode não apenas replicar, mas amplificar esses vieses em suas decisões e recomendações.³⁴ Um sistema de recrutamento que aprende com dados passados pode continuar a favorecer perfis historicamente privilegiados, e uma ferramenta de análise de comunicação pode penalizar estilos de linguagem associados a determinados grupos demográficos.
- **Privacidade e Segurança dos Dados:** As ferramentas de IA, para serem eficazes, precisam processar grandes volumes de dados, muitos dos quais são extremamente sensíveis, como comunicações privadas, avaliações de desempenho e relatos de saúde mental.³⁴ Isso cria um risco elevado de violações de privacidade e segurança. É imperativo garantir que os dados sejam anonimizados sempre que possível, que o acesso seja rigorosamente controlado e que a plataforma tecnológica possua as mais altas certificações de segurança para prevenir vazamentos e ataques cibernéticos.
- **Falta de Transparência (Problema da "Caixa-Preta"):** Muitos modelos de IA, especialmente os mais complexos, operam de uma maneira que é difícil de explicar, até mesmo para seus desenvolvedores.³⁵ Se uma IA recomenda uma ação ou chega a uma conclusão sobre um colaborador, a incapacidade de entender o "porquê" por trás dessa decisão mina a confiança e a capacidade de auditoria. As organizações devem priorizar soluções que ofereçam algum grau de explicabilidade e transparência.
- **Desumanização e Dependência Excessiva:** Existe o risco de que a automação do suporte e da comunicação leve à desumanização das relações de trabalho.²⁵ Um chatbot nunca substituirá a empatia de uma conversa humana genuína. Além disso, a dependência excessiva da tecnologia pode atrofiar a capacidade de julgamento e a inteligência emocional dos próprios gestores, que podem passar a confiar cegamente nas recomendações da máquina.³⁵ Um princípio fundamental deve ser o "humano no circuito" (*human-in-the-loop*), onde a IA atua como um copiloto que aumenta a capacidade humana, mas a decisão e a responsabilidade final permanecem com

as pessoas.

Barreiras Culturais e Técnicas no Brasil

Além dos riscos éticos universais, a implementação de IA no Brasil enfrenta barreiras específicas que precisam ser consideradas na estratégia de adoção.

- **Barreiras Culturais:** Pesquisas indicam que, apesar do crescimento da adoção de IA no país ³⁶, existe uma forte resistência cultural. Fatores como o medo da substituição de empregos, a falta de confiança na tecnologia e o receio geral de mudanças são prevalentes.³⁷ Muitos colaboradores e até mesmo líderes podem ver a introdução de uma IA que analisa comunicação ou desempenho como uma ferramenta de vigilância, e não de apoio. Superar essa barreira exige um plano de gestão da mudança e comunicação transparente e robusto, que enfatize o papel da IA como uma ferramenta de aumento de capacidade (*augmentation*) e que demonstre claramente os benefícios para o colaborador individual.
- **Barreiras Técnicas e de Custo:** A implementação de IA de ponta exige um investimento financeiro significativo e acesso a talentos especializados em áreas como ciência de dados e engenharia de IA, que ainda são escassos no mercado brasileiro.³⁷ Para muitas empresas, especialmente as de médio porte, o custo e a complexidade técnica podem ser proibitivos. A solução pode passar por parcerias com fornecedores de tecnologia que oferecem plataformas como serviço (SaaS), reduzindo o investimento inicial em infraestrutura e a necessidade de uma grande equipe interna de especialistas.

A superação desses desafios exige uma abordagem deliberada e multidisciplinar. A criação de um comitê de ética em IA, a redação de uma política clara sobre o uso de dados e a realização de projetos piloto em ambientes controlados são passos essenciais para construir a confiança e a competência necessárias para uma implementação bem-sucedida e responsável em larga escala.

Seção 8: Perspectivas Futuras: Tendências Globais e o Cenário Brasileiro

A integração da Inteligência Artificial na gestão do bem-estar corporativo e na mitigação de riscos psicossociais não é um fenômeno isolado, mas parte de uma tendência global que está redefinindo as relações de trabalho e a regulamentação

tecnológica. Compreender essas tendências é crucial para que as empresas brasileiras possam se posicionar estrategicamente, antecipando futuras exigências e aproveitando as oportunidades de inovação.

Tendências Globais em IA para o Bem-Estar Corporativo

No cenário internacional, observa-se uma convergência de esforços para criar um ambiente de uso da IA que seja, ao mesmo tempo, inovador e seguro. Governos e órgãos multilaterais estão se movendo para estabelecer marcos regulatórios que equilibrem o fomento à tecnologia com a proteção dos direitos fundamentais.

- **Regulamentação Baseada em Risco:** A tendência predominante, exemplificada pelo AI Act da União Europeia, é uma abordagem regulatória baseada em risco.⁴⁰ Em vez de regular a tecnologia de IA em si, a legislação foca em suas aplicações, impondo obrigações mais rigorosas para os casos de uso considerados de "alto risco" — categoria na qual a gestão de pessoas e o ambiente de trabalho frequentemente se enquadram.
- **Colaboração Internacional e Padrões de Segurança:** Há um reconhecimento crescente de que os riscos da IA, especialmente dos modelos generativos mais poderosos, transcendem fronteiras. Isso impulsiona a busca por colaboração internacional para desenvolver padrões comuns de segurança, ética e interoperabilidade.⁴⁰ As empresas brasileiras que adotarem padrões elevados de governança desde já estarão mais bem preparadas para operar em um ecossistema global cada vez mais interconectado.
- **Foco Corporativo em Governança e ROI:** Globalmente, as empresas estão aumentando seus investimentos em IA Generativa, motivadas principalmente pela promessa de redução de custos e aumento de receita.³⁶ Contudo, a experiência também está elevando a conscientização sobre os riscos, como imprecisão, violação de propriedade intelectual e segurança de dados.³⁶ Isso está levando as organizações mais maduras a fortalecerem suas estruturas de governança de IA, entendendo que uma implementação segura e ética é um pré-requisito para o sucesso a longo prazo.⁴¹

Projeções para o Cenário Brasileiro

O Brasil se encontra em um ponto de inflexão particularmente dinâmico. A pressão regulatória interna, impulsionada pela NR-1, está convergindo com a onda de inovação tecnológica global em IA Generativa. Essa combinação cria uma

"tempestade perfeita" que deve acelerar drasticamente a adoção de tecnologia no campo da gestão de pessoas e SST.

- **Adoção Acelerada por Necessidade:** Enquanto a adoção de IA em muitas áreas pode ser vista como opcional ou uma busca por ganhos marginais de produtividade, a necessidade de gerenciar riscos psicossociais de forma eficaz e documentada se tornou uma exigência legal inadiável. Este imperativo de conformidade atuará como um poderoso catalisador, levando empresas que antes hesitavam em investir em IA a fazê-lo agora, com um caso de uso claro e urgente.
- **Divergência Competitiva:** Nos próximos anos, é provável que vejamos uma divergência no mercado brasileiro. De um lado, empresas proativas que adotarem a IA como uma ferramenta estratégica para a gestão de riscos psicossociais. Elas não apenas garantirão a conformidade, mas também colherão os benefícios de um melhor clima organizacional, maior atratividade para talentos e aumento da produtividade. Do outro lado, empresas retardatárias que se apegarem a métodos tradicionais ou a uma conformidade meramente superficial. Estas enfrentarão riscos crescentes de sanções legais, litígios trabalhistas, perda de talentos e dificuldades para competir em um mercado que valoriza cada vez mais o bem-estar e a saúde mental.
- **O Padrão de Cuidado Evoluirá:** À medida que as empresas líderes demonstrarem a eficácia das ferramentas de IA, o uso dessas tecnologias para monitorar e controlar riscos psicossociais pode se tornar, gradualmente, o "padrão de cuidado" esperado no mercado. O que hoje é inovador pode se tornar a prática padrão amanhã. A documentação do uso de uma plataforma de IA no PGR se tornará um diferencial competitivo e, eventualmente, uma prática comum entre as organizações mais bem gerenciadas do país.

O Brasil não está apenas seguindo uma tendência global; está vivenciando uma confluência única de fatores que posiciona a gestão de riscos psicossociais como a porta de entrada para uma transformação digital mais ampla e profunda na área de recursos humanos e segurança do trabalho.

Seção 9: Recomendações Estratégicas para Implementação

Para transformar o potencial da Inteligência Artificial em resultados concretos e conformidade robusta, as organizações precisam de um roteiro claro e pragmático. A seguir, apresenta-se uma proposta de plano de ação estratégico, dividido em fases, para guiar os líderes executivos na implementação de LLMs como ferramentas de

controle de riscos psicossociais.

Fase 1: Estabelecimento da Governança e Estrutura (Meses 1-2)

1. **Formar uma Equipe de Projeto Multidisciplinar:** O sucesso da iniciativa depende da colaboração entre diferentes áreas. Crie um comitê gestor com representantes de alto nível dos departamentos de Recursos Humanos, Jurídico/Compliance, Saúde e Segurança do Trabalho (SST), Tecnologia da Informação (TI) e um representante da CIPA. Esta equipe será responsável por supervisionar todo o projeto.
2. **Redigir uma Carta de Princípios para o Uso Ético da IA:** Antes de avaliar qualquer tecnologia, defina as regras do jogo. Desenvolva um documento formal que estabeleça os princípios éticos da empresa para o uso de IA na gestão de pessoas. Este documento deve abordar, no mínimo: privacidade de dados, transparência, mitigação de vieses, o princípio do "humano no circuito" e o compromisso de usar a tecnologia para apoiar, e não para vigiar, os colaboradores.

Fase 2: Mapeamento de Riscos e Seleção do Projeto Piloto (Mês 3)

1. **Realizar o Mapeamento de Riscos Psicossociais:** Utilize o Inventário de Riscos do PGR e a "Tabela de Mapeamento" proposta na Seção 4 deste relatório para identificar os riscos psicossociais mais prevalentes e impactantes na sua organização.
2. **Selecionar a Aplicação Piloto:** Escolha uma aplicação de LLM que ofereça o melhor balanço entre alto impacto potencial e baixa sensibilidade percebida. Geralmente, começar com a automação de tarefas para reduzir a sobrecarga de trabalho (Controle de Engenharia) é uma estratégia de "vitória rápida" que gera aceitação.
3. **Definir o Grupo Piloto:** Selecione um departamento ou equipe que seja representativo e tenha uma liderança engajada e aberta à inovação para participar do projeto piloto.

Fase 3: Seleção de Tecnologia e Gestão da Mudança (Meses 4-5)

1. **Avaliar e Selecionar a Plataforma de IA:** Pesquise fornecedores de tecnologia. Crie uma matriz de avaliação com critérios claros, incluindo: segurança da informação (certificações como ISO 27001), conformidade com a LGPD, capacidade de customização, transparência do modelo, qualidade do suporte técnico e alinhamento com a sua Carta de Princípios Éticos.
2. **Desenvolver um Plano de Comunicação e Treinamento:** A gestão da mudança é crucial. Crie um plano de comunicação transparente que explique o "porquê"

do projeto, seus objetivos, como a ferramenta funciona e, principalmente, quais são os benefícios diretos para os colaboradores. Desenvolva materiais de treinamento claros e práticos.

Fase 4: Implementação e Monitoramento do Piloto (Meses 6-9)

1. **Lançar a Ferramenta no Grupo Piloto:** Realize o treinamento e implemente a ferramenta no departamento selecionado. Ofereça canais de suporte próximos para tirar dúvidas e resolver problemas rapidamente.
2. **Coletar e Analisar Dados:** Monitore os indicadores de processo (*leading indicators*), como taxas de adoção e frequência de uso. Realize pesquisas de pulso e colete feedback qualitativo dos participantes do piloto para entender sua percepção e identificar pontos de melhoria.

Fase 5: Avaliação, Documentação e Planejamento de Expansão (Meses 10-12)

1. **Avaliar os Resultados do Piloto:** Analise os dados coletados, tanto os indicadores de processo quanto os de resultado (*lagging indicators*), como variações em pesquisas de clima ou produtividade. Avalie o ROI do piloto.
2. **Documentar Formalmente no PGR:** Com base nos resultados positivos do piloto, refine a descrição da medida de controle e incorpore-a oficialmente no Inventário de Riscos e no Plano de Ação do PGR da empresa.
3. **Construir o Caso de Negócio para Expansão:** Utilize os dados e o ROI do piloto para construir um caso de negócio robusto e apresentar à alta gestão um plano para a expansão da iniciativa para toda a organização. Este plano deve incluir um cronograma, orçamento e as lições aprendidas durante a fase piloto.

Seguir este roteiro estruturado permitirá que a organização navegue pela complexidade da implementação da IA de forma segura, ética e estratégica, transformando uma obrigação regulatória em uma poderosa alavanca para a criação de um ambiente de trabalho mais saudável, produtivo e inovador.

Referências citadas

1. Riscos psicossociais: o que são e como se adequar para a NR1 - Senior Sistemas, acessado em junho 20, 2025, <https://www.senior.com.br/blog/riscos-psicossociais>
2. NORMA REGULAMENTADORA N.º 01 - NR 1 - DISPOSIÇÕES GERAIS e GERENCIAMENTO DE RISCOS OCUPACIONAIS - Guia Trabalhista, acessado em junho 20, 2025, <https://www.guiatrabalhista.com.br/legislacao/nr/nr1.htm>
3. Guia de informações sobre os Fatores de Riscos Psicossociais Relacionados ao Trabalho, acessado em junho 20, 2025, <https://cdn.protecao.com.br/wp-content/uploads/2025/04/Guia-Fatores-de-Riscos-Psicossociais-MTE.pdf>

4. Atualizações na lei fortalece a gestão de riscos ocupacionais | UNINTER NOTÍCIAS, acessado em junho 20, 2025, <https://www.uninter.com/noticias/atualizacoes-na-lei-fortalecem-a-gestao-de-riscos-ocupacionais>
5. A implementação dos Riscos Psicossociais da NR-01 - ABMES, acessado em junho 20, 2025, <http://abmes.org.br/blog/detalhe/18904/a-implementacao-dos-riscos-psicossociais-da-nr-01>
6. Inclusão de fatores de risco psicossociais no GRO começa em caráter educativo a partir de maio, acessado em junho 20, 2025, <https://www.gov.br/trabalho-e-emprego/pt-br/noticias-e-conteudo/2025/abril/inclusao-de-fatores-de-risco-psicossociais-no-gro-comeca-em-carater-educativo-a-partir-de-maio>
7. Empresas brasileiras terão que avaliar riscos psicossociais a partir de 2025 - Portal Gov.br, acessado em junho 20, 2025, <https://www.gov.br/trabalho-e-emprego/pt-br/noticias-e-conteudo/2024/Novembro/empresas-brasileiras-terao-que-avaliar-riscos-psicossociais-a-partir-de-2025>
8. L14457 - Planalto, acessado em junho 20, 2025, https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/114457.htm
9. Lei 14.457 de 2022 cipa - Contato Seguro, acessado em junho 20, 2025, <https://canaldaetica.com.br/glossario/glossario-l/lei-14-457-de-2022-cipa/>
10. NR-01 (Disposições Gerais e Gerenciamento de ... - Portal Gov.br, acessado em junho 20, 2025, <https://www.gov.br/trabalho-e-emprego/pt-br/aceso-a-informacao/participacao-social/conselhos-e-orgaos-colegiados/comissao-tripartite-partitaria-permanente/normas-regulamentadora/normas-regulamentadoras-vigentes/nr-01-atualizada-2025-i-1.pdf>
11. Tecnologias de informação e comunicação: revisão de escopo dos instrumentos de avaliação dos fatores de risco psicossociais no trabalho contemporâneo - SciELO, acessado em junho 20, 2025, <https://www.scielo.br/j/rbso/a/NJfgzNJmG9PLFX6Sy84KSDN/?lang=pt>
12. Estratégias para gerenciar a sobrecarga cognitiva - Supernormal, acessado em junho 20, 2025, <https://www.supernormal.com/pt-br/blog/reduce-cognitive-load>
13. FEEDBACK ESTRUTURADO com IA: Passo a Passo - YouTube, acessado em junho 20, 2025, <https://www.youtube.com/watch?v=TgR5mZwxVko>
14. 6 técnicas para praticar a comunicação não-violenta no ambiente de trabalho - Mindsight, acessado em junho 20, 2025, <https://mindsight.com.br/comunicacao-nao-violenta-no-ambiente-de-trabalho/>
15. Principais tendências de educação e habilidades da IA generativa para 2025 - AWS, acessado em junho 20, 2025, <https://aws.amazon.com/pt/executive-insights/content/top-generative-ai-skills-and-education-trends-for-2025/>
16. Programa de Gerenciamento de Riscos - PGR — Ministério do Trabalho e Emprego, acessado em junho 20, 2025,

- https://www.gov.br/trabalho-e-emprego/pt-br/assuntos/inspecao-do-trabalho/pg_r
17. NR 01 - DISPOSIÇÕES GERAIS e GERENCIAMENTO DE RISCOS OCUPACIONAIS
Publicação DOU - Portal Gov.br, acessado em junho 20, 2025,
<https://www.gov.br/trabalho-e-emprego/pt-br/aceso-a-informacao/participacao-social/conselhos-e-orgaos-colegiados/comissao-tripartite-partitaria-permanente/normas-regulamentadora/normas-regulamentadoras-vigentes/nr-01-atualizada-2024.pdf>
 18. Comunicação Não Violenta e um ambiente de trabalho colaborativo - Think Work Lab, acessado em junho 20, 2025,
<https://thinkworklab.com/guias/comunicacao-nao-violenta-tudo-sobre/>
 19. Comunicação não-violenta no trabalho: Siga estes 4 passos - Factorial, acessado em junho 20, 2025, <https://factorialhr.pt/blog/comunicacao-nao-violenta/>
 20. Curso gratuito - Técnicas de Feedback e Comunicação Não Violenta para Gestores - Even3, acessado em junho 20, 2025,
<https://www.even3.com.br/curso-gratuito-tecnicas-de-feedback-e-comunicacao-nao-violenta-para-gestores-478031/>
 21. Como a Lei 14.457/22 se uniu à tecnologia na prevenção do ..., acessado em junho 20, 2025,
<https://canaldaetica.com.br/blog/como-a-lei-14-457-22-se-uniu-a-tecnologia-na-prevencao-do-assedio-no-trabalho/>
 22. Curso Online Segurança Psicológica: promova um ambiente de trabalho seguro e colaborativo | Alura, acessado em junho 20, 2025,
<https://www.alura.com.br/curso-online-seguranca-psicologica-promova-ambiente-trabalho-seguro-colaborativo>
 23. Pós-graduação em Psicologia Organizacional e Gestão de Pessoas | Lançamentos, acessado em junho 20, 2025,
<https://online.pucrs.br/pos-graduacao/psicologia-organizacional-e-gestao-de-pessoas-edicao-lancamentos>
 24. (PDF) O USO DE IA EM AMBIENTES DE APRENDIZAGEM PERSONALIZADOS, acessado em junho 20, 2025,
https://www.researchgate.net/publication/380966263_O_USO_DE_IA_EM_AMBIENTES_DE_APRENDIZAGEM_PERSONALIZADOS
 25. Impactos da inteligência artificial na Psicologia - Dot.Lib, acessado em junho 20, 2025, <https://dotlib.com/blog/impactos-da-inteligencia-artificial-na-psicologia>
 26. Programa de Gerenciamento de Riscos Ocupacionais - Portal Gov.br, acessado em junho 20, 2025,
<https://www.gov.br/fundacentro/pt-br/comunicacao/noticias/noticias/2020/8/fundacentro-realiza-serie-de-webinars-sobre-pgr/trivelato-2020-webinar-4-como-construir-um-inventario-de-riscos-ocupacionais.pdf>
 27. Como avaliar a eficácia do seu Programa de Gerenciamento de ..., acessado em junho 20, 2025,
<https://www.connapa.com.br/como-avaliar-a-eficacia-do-seu-programa-de-gerenciamento-de-risco>
 28. O que é avaliação de eficácia? Por que ela importa para o GRO? - SOC, acessado

- em junho 20, 2025,
<https://www.soc.com.br/blog-de-sst/o-que-e-avaliacao-de-eficacia-por-que-ela-e-importante-para-o-gro/>
29. ROI do Bem-Estar Corporativo - charya, acessado em junho 20, 2025,
<https://charya.com.br/blog/roi-do-bem-estar-corporativo/>
 30. O impacto da rotatividade e do absenteísmo de pessoal sobre o custo do produto: um estudo em uma indústria gaúcha. - Anais do Congresso Brasileiro de Custos, acessado em junho 20, 2025,
<https://anaiscbc.emnuvens.com.br/anais/article/download/253/253/0>
 31. Como Avaliar os Riscos Psicossociais no PGR: Obrigação Legal, Importância e Soluções., acessado em junho 20, 2025,
<https://www.bioprotecao.com.br/post/como-avaliar-os-riscos-psicossociais-no-pgr-obriga%C3%A7%C3%A3o-legal-import%C3%A2ncia-e-solu%C3%A7%C3%B5es>
 32. O novo papel da CIPA na prevenção de assédio sexual e moral, acessado em junho 20, 2025,
<https://bertonbortolotto.com.br/novo-papel-da-cipa-na-prevencao-de-assedio/>
 33. CIPA: tudo o que você precisa saber sobre a Lei 14.457/22 - Blog 1Doc, acessado em junho 20, 2025, <https://blog.1doc.com.br/cipa/>
 34. Desafios éticos do uso da Inteligência Artificial - Fênix Educação, acessado em junho 20, 2025,
<https://www.fenixeducacao.org.br/blog/desafios-eticos-do-uso-da-ia>
 35. Riscos que Podem Sabotar sua Empresa - IA no Compliance, acessado em junho 20, 2025,
<https://becompliance.com/ia-no-compliance-os-riscos-invisiveis-que-podem-sabotar-sua-empresa/>
 36. Uso de Inteligência Artificial aumenta e alcança 72% das empresas, diz pesquisa, acessado em junho 20, 2025,
<https://www.cnnbrasil.com.br/economia/negocios/uso-de-inteligencia-artificial-aumenta-e-alcanca-72-das-empresas-diz-pesquisa/>
 37. Inteligência artificial no Brasil: 7 barreiras para a plena adoção!, acessado em junho 20, 2025, <https://www.zendesk.com.br/blog/inteligencia-artificial-no-brasil/>
 38. Resistência Humana Dificulta Adoção de IA por Empresas Brasileiras - Forbes Brasil, acessado em junho 20, 2025,
<https://forbes.com.br/forbes-tech/2024/10/resistencia-humana-dificulta-adocao-de-ia-por-empresas-brasileiras/>
 39. 11 barreiras para a adoção eficaz da IA e como superá-las | Artigos e Editoriais | Notícias, acessado em junho 20, 2025,
<https://assespro.rio/noticias/artigos-e-editoriais/11-barreiras-para-a-adocao-eficaz-da-ia-e-como-supera-las-242.html>
 40. Regulamentação da Inteligência Artificial, tendências globais | EY ..., acessado em junho 20, 2025,
https://www.ey.com/pt_br/insights/ai/how-to-navigate-global-trends-in-artificial-intelligence-regulation
 41. Sistemas de IA generativa precisam ser continuamente confrontados ou testados

- EY, acessado em junho 20, 2025,

https://www.ey.com/pt_br/newsroom/2025/06/sistemas-ia-generativa-continuam-ente-confrontados-testados