CONTROL 361 TECNOLOGIA E SERVIÇOS LTDA

POLÍTICA DE GESTÃO DE RISCO

Disque Idoso 165

2025 / 2026

Índice

01

PRINCÍPIOS E CONDUTAS

Esta seção estabelece os valores éticos fundamentais que devem nortear a atuação de todos os envolvidos no serviço.

Diretrizes de Atuação (O que fazer):

- Preservação da Dignidade: O atendimento deve ser pautado pelo respeito à integridade física, psicológica e moral da pessoa idosa, garantindo uma abordagem humanizada.
- Confidencialidade e Sigilo: É imperativo proteger a identidade do denunciante e da vítima, nos termos da lei, assegurando a segurança dos dados.
- Diligência na Identificação de Riscos: Todos os colaboradores têm a responsabilidade de identificar proativamente potenciais vulnerabilidades no sistema de atendimento e reportá-las.
- Comunicação Imediata: Situações que envolvam risco iminente de morte, maus-tratos ou violação grave de direitos devem ser comunicadas, de imediato, à hierarquia e à rede de proteção competente.
- Conformidade Normativa: O cumprimento estrito dos protocolos operacionais é a garantia de que o serviço cumpre a sua missão institucional.

Vedações (O que não fazer):

- Omissão de Denúncias: É terminantemente proibido ignorar, atrasar ou omitir qualquer denúncia ou pedido de auxílio.
- Desconsideração de Indícios: Não devem ser subestimados relatos
- que indiquem violência, negligência ou vulnerabilidade extrema.
- Desvio de Fluxo: Não é permitida a alteração, por iniciativa própria, dos fluxos de encaminhamento para os órgãos de proteção.
- Divulgação Indevida: É proibida a partilha de dados pessoais fora do âmbito do serviço ou sem base legal, sob pena de responsabilidade administrativa e civil.

02

OBJETIVOS

Esta Política visa estabelecer as diretrizes, a metodologia e os mecanismos de controlo necessários para identificar, avaliar, tratar e monitorizar os riscos associados ao funcionamento do Disque Idoso 165. O objetivo central é assegurar:

- A continuidade e a excelência operacional do serviço de atendimento.
- A proteção rigorosa dos dados pessoais, em estrita obediência ao RGPD/LGPD.

- A eficácia da articulação com a rede de proteção social (CRAS, CREAS, Saúde, Segurança Pública).
- A conformidade com o Estatuto da Pessoa Idosa e demais normativos.
- A salvaguarda da reputação da instituição perante a sociedade.

03 ABRANGÊNCIA E APLICABILIDADE

Esta Política de Gestão de Riscos possui aplicação transversal e é de observância obrigatória para todos os agentes que, de forma] direta ou indireta, contribuem para a execução do Disque Idoso 165. A abrangência compreende:

- Equipes Internas (Servidores e Gestores): Abrange todo ocorpo técnico, administrativo e de liderança, independentemente do vínculo (efetivos, comissionados ou designados). Estes agentes são responsáveis pela condução do fluxo operacional e pela tomada de decisão em casos críticos.
- Fornecedores e Terceiros: Aplica-se a todas as empresas contratadas ou prestadoras de serviço que atuam na sustentação do canal, incluindo equipes de atendimento (telemarketing), suporte de TI, segurança, manutenção de banco de dados e gestão de infraestrutura.

- Parceiros Estratégicos da Rede de Proteção: Embora não subordinados hierarquicamente, a política orienta a interação com órgãos da rede (CRAS, CREAS, Conselhos Municipais/Estaduais do Idoso, Delegacias Especializadas, Ministérios Públicos e Unidades de Saúde). O gerenciamento dos riscos de articulação com estes entes é parte integrante deste escopo.
- Estagiários e Bolsistas: Todos os indivíduos em programas de aprendizado ou estágio, que lidam com informações sensíveis e protocolos de atendimento.

04 ATRIBUIÇÕES E RESPONSABILI-DADES

A gestão de riscos é uma responsabilidade compartilhada. A distribuição de papéis visa garantir que nenhum risco relevante fique sem um "dono" ou sem monitoramento.

4.1 Alta Gestão (Órgão Supervisor / Secretária(o) de Pasta)

Compete à instância máxima de decisão garantir o suporte estratégico à política.
Estabelecer o Apetite ao Risco: Definir formalmente qual é o nível de exposição tolerável para o serviço, priorizando sempre a integridade do idoso.

Prover Recursos: Assegurar que existam recursos humanos, financeiros e tecnológicos suficientes para tratar os riscos mapeados.
Instituir a Cultura: Disseminar a cultura de gestão de riscos em todos os níveis hierárquicos, garantindo que o tema seja parte das reuniões de decisão.
Supervisão Estratégica: Acompanhar os indicadores de risco (KRIs) consolidados e tomar decisões sobre medidas estruturais de mitigação de alto impacto.

4.2 Coordenação do Disque Idoso (Gestão Tática)

Atua como o "Dono do Processo" (Process Owner), sendo a principal responsável pela execução da política no dia a dia.
Governança: Implementar e manter atualizada a Política de Gestão de Riscos, adaptando-a a novas exigências legais ou mudanças no fluxo de trabalho.
Gestão da Matriz: Coordenar o processo de identificação, análise e avaliação dos riscos, mantendo a Matriz de Riscos atualizada.
Monitoramento e Reporte: Consolidar indicadores de desempenho e de risco, reportando à Alta Gestão qualquer evento que supere o apetite ao risco definido.
Articulação Institucional: Gerenciar as interfaces com a rede de proteção (CRAS, CREAS, Saúde), garantindo que as falhas de articulação sejam mitigadas.

4.3 Supervisores e Gestores de Processos (Donos do Risco)

São responsáveis pelos processos específicos dentro da operação.

Gestão da Operação: Monitorar a execução dos protocolos de atendimento pela equipe, identificando desvios em tempo real.
Tratamento de Incidentes: Receber e gerir o tratamento de ocorrências críticas reportadas pela equipe de atendimento.
Formação: Identificar lacunas de competência na equipe (treinamento) que possam gerar riscos operacionais.
Feedback de Controle: Propor melhorias nos fluxos de trabalho com base nas dificuldades observadas na ponta da operação.

4.4 Equipe de Atendimento (Operacional / Primeira Linha de Defesa)

São os "sensores" do serviço; estão em contato direto com as vulnerabilidades.
Identificação Ativa: Reportar imediatamente à supervisão qualquer falha sistêmica, comportamento atípico ou dificuldade na aplicação dos protocolos.
Conformidade: Seguir rigorosamente os manuais de atendimento e protocolos de segurança de dados (LGPD).
Registro de Qualidade: Assegurar que todas as informações coletadas sejam precisas, evitando a subnotificação ou o erro de registro de denúncias.
Ética e Sigilo: Manter a integridade e o sigilo das informações do denunciante e da vítima em qualquer circunstância.

4.5 Área de Tecnologia da Informação e Segurança da Informação

Responsável pela resiliência tecnológica do canal.
Continuidade Operacional: Garantir a disponibilidade dos sistemas (telefonia e banco de dados) e executar planos de contingência em caso de falhas.
Proteção de Dados: Implementar barreiras de segurança cibernética (firewalls, criptografia, controle de acesso) para impedir o vazamento de dados sensíveis.
Monitoramento de Vulnerabilidades: Realizar testes e auditorias periódicas no sistema para identificar falhas técnicas antes que sejam exploradas.

4.6 Unidade de Controle Interno / Auditoria (Terceira Linha de Defesa)

Órgão independente que avalia se a gestão de riscos está funcionando.
Auditoria de Conformidade: Verificar, periodicamente, se as ações de mitigação propostas pela Coordenação estão sendo efetivamente executadas.
Avaliação de Eficácia: Avaliar se a metodologia de gestão de riscos é adequada para o serviço e se os controles implantados mitigam os riscos de forma satisfatória.
Recomendação: Emitir recomendações formais para correção de rumo, caso sejam identificadas falhas na estrutura de gestão.

05

PROCESSO DE GESTÃO DE RISCOS

A gestão de riscos no "Disque Idoso 165" é um processo contínuo, dinâmico e integrado à rotina administrativa, composto pelas seguintes etapas interconectadas:

5.1 Identificação de Riscos

Mapeamento: Realização de workshops, entrevistas com as equipes de ponta e análise histórica de denúncias e incidentes.
Inventário: Catalogação de todos os eventos potenciais que podem impedir o alcance dos objetivos do serviço, utilizando fontes internas (relatórios de sistema) e externas (demandas do Ministério Público, mudanças no Estatuto do Idoso).

5.2 Análise de Riscos

Natureza: Compreensão das causas raiz e das consequências.
Qualificação: Avaliação da Probabilidade (a frequência com que o evento pode ocorrer) e do Impacto (a severidade do dano à pessoa idosa ou à imagem institucional), utilizando a Matriz de Criticidade (Probabilidade x Impacto).

5.3 Avaliação de Riscos

Priorização: Comparação do nível de risco obtido na análise com os critérios de "Apetite ao Risco" definidos pela gestão.
Tomada de Decisão: Determinação de quais riscos exigem ação imediata (Críticos/Altos) e quais podem ser apenas monitorados (Baixos).

5.4 Tratamento de Riscos

Planos de Ação: Seleção da estratégia de resposta para cada risco priorizado:
Mitigar: Reduzir a probabilidade ou o impacto do risco (ex: treinamento extra para atendentes).
Transferir/Compartilhar: Repassar a responsabilidade ou o ônus (ex: contratar seguro ou terceirizar suporte técnico).
Evitar: Alterar o processo para eliminar o risco (ex: mudar o software de registro).
Aceitar: Manter o risco dentro dos limites de tolerância (risco residual).

5.5 Monitoramento

Acompanhamento: Verificação contínua se os controles implementados estão sendo eficazes.
Indicadores (KRIs): Utilização de Key Risk Indicators (ex: taxa de queda de chamadas, tempo de resposta na triagem) para detectar desvios de forma precoce.

5.6 Comunicação e registro

Transparência: Garantir que todos os envolvidos compreendam os riscos e seus papéis na mitigação.
Documentação: Manutenção de um "Histórico de Riscos" (Matriz Viva) que deve ser auditável pelos órgãos de controle.

06 CLASSIFICAÇÃO DOS RISCOS

A classificação é o pilar que permite organizar a gestão. Os riscos serão categorizados seguindo três eixos fundamentais:

6.1 Quanto à Origem

Riscos Internos: Originados de falhas nos processos de trabalho, deficiências na gestão de pessoas, infraestrutura tecnológica obsoleta, erros humanos na triagem ou falta de integração entre setores da Secretaria.
Riscos Externos: Originados por fatores alheios ao controle direto do órgão, como mudanças na legislação, crises sanitárias, demandas judiciais intempestivas, cortes orçamentários, mudanças no perfil sociodemográfico da população idosa ou ataques cibernéticos externos.

6.2 Quanto à Dimensão

Dimensão Estratégica: Riscos que impactam o cumprimento da missão do Disque Idoso 165 a longo prazo (ex: perda de relevância do canal, falha na integração com políticas públicas de proteção).
Dimensão Operacional: Riscos que afetam o dia a dia da execução do serviço (ex: interrupção do atendimento telefônico, fila de espera elevada, erro na digitação de protocolos).

6.3 Macro Categorias (Tipologia)

Para fins de monitoramento, os riscos serão agrupados da seguinte forma:

Riscos Operacionais e de Continuidade: Falhas de processos, erros humanos, interrupção de infraestrutura, indisponibilidade do PABX ou do sistema de gestão de denúncias.

Riscos Tecnológicos e de Segurança da Informação: Vulnerabilidades em redes, acessos não autorizados, perda ou corrupção de dados e falhas em planos de backup.

Riscos de Compliance e Legal: Descumprimento do Estatuto da Pessoa Idosa, violações da LGPD, inobservância de prazos judiciais ou normas de controle interno (TCU/CGU).

Riscos Reputacionais e de Imagem: Perda de confiança da sociedade, repercussão negativa em redes sociais/imprensa decorrente de omissão ou atendimento inadequado.

Riscos de Proteção e Impacto Social: Riscos que afetam diretamente o usuário final, como falha na identificação de situação de emergência, omissão de socorro, falha na articulação com a rede de proteção ou subnotificação de violência grave.

Riscos de Integridade (Éticos): Conflitos de interesse, vazamento de denúncias para o agressor, corrupção ou uso de informações do canal para fins pessoais ou políticos.

CRITICIDADE

07

A criticidade é o indicador quantitativo que define a prioridade de resposta para cada risco identificado. Ela é calculada pela combinação da Probabilidade de ocorrência com a severidade do Impacto, utilizando uma matriz de risco 5x5.

7.1 Matriz de Criticidade

A combinação dos fatores resulta na seguinte classificação:
Nível Muito Baixo / Baixo: Riscos toleráveis, gerenciados através de monitoramento rotineiro.
Nível Médio: Requer planos de ação de mitigação em médio prazo.
Nível Alto: Requer plano de ação prioritário e acompanhamento direto da gestão.
Nível Crítico: Risco inaceitável. Exige intervenção imediata, suspensão da atividade ou ativação do plano de contingência.

7.2 Detalhamento dos Critérios de Impacto

O Impacto mede a gravidade das consequências caso o evento de risco se materialize. A avaliação deve considerar a dimensão mais grave encontrada:
Sobre a Pessoa Idosa (Critério de Maior Peso): Avalia danos à vida, integridade física, saúde mental, ou violação grave de direitos fundamentais.

Qualquer impacto que coloque em risco a integridade do idoso é automaticamente classificado como "Alto" ou "Crítico".
Sobre a Continuidade do Serviço: Avalia a interrupção operacional.
Baixo: Pequena lentidão no sistema.
Crítico: Indisponibilidade total do canal de denúncias durante horário de pico ou falha prolongada que impeça a recepção de pedidos de socorro.
Financeiros: Avalia possíveis multas, glosas orçamentárias, custos extraordinários de emergência ou desvios de recursos públicos.
Jurídicos e de Compliance: Avalia riscos de ações civis públicas, descumprimento de Termos de Ajustamento de Conduta (TAC), sanções do Ministério Público ou multas administrativas.
Reputacionais: Avalia a perda de confiança da sociedade civil no "Disque Idoso 165". Considera o grau de exposição na mídia e o impacto negativo na percepção pública sobre a eficiência do Estado.
Proteção de Dados (LGPD): Avalia a extensão de incidentes de segurança. Considera o volume de registros expostos e o nível de sensibilidade das informações (ex: endereços residenciais, histórico de violência).

7.3 Detalhamento dos Critérios de Probabilidade

A Probabilidade avalia a chance de o evento de risco ocorrer em um horizonte temporal Deve ser baseada em fatos, não em intuições:
• Histórico de Ocorrências (Frequência):
• Avalia a reincidência do evento no passado.
• Muito Baixa: Nunca aconteceu.

• Muito Alta: Evento frequente ou recorrente (ex: quedas mensais do sistema de telefonia).
• Fragilidade dos Controles Existentes:
• Avalia a força das barreiras preventivas atuais.
• Alta Probabilidade: O risco é alto se o controle depender exclusivamente de memória humana, se for um processo manual sem validação, ou se não houver protocolos escritos.
• Baixa Probabilidade: O risco é menor se o processo for automatizado, auditado e possuir travas de segurança (ex: sistemas que bloqueiam acesso a dados sem autorização).
• Grau de Exposição do Processo (Contexto):
• Avalia o nível de vulnerabilidade frente ao ambiente.
Ambiente Estável: Baixa exposição a mudanças repentinas.
Ambiente Volátil: Processos sujeitos a picos de demanda (ex: Campanhas como o "junho Violeta"), ataques cibernéticos em infraestruturas públicas ou mudanças legislativas frequentes que tornam os controles atuais obsoletos.

DECLARAÇÃO DE APETITE AO RISCO

A declaração de apetite ao risco define o nível de exposição que a gestão do Disque Idoso 165 aceita, ou não, ao conduzir suas atividades diárias.

08

. O objetivo é equilibrar a agilidade no atendimento social com a responsabilidade pública e jurídica.
O Disque Idoso 165 estabelece os seguintes parâmetros de apetite:

8.1 Nível 1: Tolerância Zero (Apetite Nulo)

Abrangência: Riscos que envolvam violação da integridade física, psíquica, moral ou risco de morte da pessoa idosa.
Diretriz: A instituição rejeita qualquer risco que possa resultar em falha na proteção da vida do idoso. Não há margem para negligência, omissão no atendimento ou desvio de protocolo em denúncias de alto risco.
Aplicação: Qualquer decisão que coloque em dúvida a segurança do idoso deve ser imediatamente escalada para a instância superior ou rede de proteção competente (Ministério Público, Delegacias, etc.).

8.2 Nível 2: Tolerância Baixa (Apetite Restrito)

Abrangência: Riscos relacionados à conformidade legal (Estatuto do Idoso, LGPD), sigilo de dados sensíveis e ética profissional.
Diretriz: A instituição busca o nível máximo de conformidade. Falhas que coloquem em risco a privacidade de dados (vazamentos) ou que exponham a instituição a sanções administrativas graves são consideradas inaceitáveis.
Aplicação: Exige-se a implementação rigorosa de controles preventivos (ex: auditoria de logs de acesso, treinamentos constantes em LGPD). Qualquer desvio deve ser corrigido imediatamente e comunicado ao controle interno.

8.3 Nível 3: Tolerância Moderada (Apetite Gerenciável)

Abrangência: Riscos operacionais de impacto limitado e baixo potencial de dano, como flutuações temporárias no tempo médio de espera ou pequenas instabilidades técnicas que não comprometam a denúncia urgente.
Diretriz: A instituição aceita que, em um ambiente de serviço público sob demanda, pequenas variações operacionais são inerentes à atividade, desde que existam planos de contingência (planos B) e que a qualidade final do serviço não seja comprometida.
Aplicação: A gestão deve monitorar esses riscos constantemente. Caso a "pequena falha" torne-se recorrente, ela deixa de ser "tolerância moderada" e passa a exigir uma intervenção corretiva.

8.4 Governança e Validação

Para que os níveis de apetite ao risco possuam eficácia normativa e vinculante, deverão ser observadas as seguintes diretrizes de governança:

I – Definição Formal

O apetite ao risco deverá ser formalmente estabelecido e aprovado pela Autoridade Gestora competente, mediante ato administrativo próprio, podendo ser o Secretário da Pasta, Diretor-Geral ou Comitê de Governança.
A definição deverá estar alinhada:
• aos objetivos estratégicos do serviço;

II – Monitoramento e Evidenciação

A Coordenação do Disque Idoso deverá apresentar relatórios periódicos de gestão de riscos, contendo:

• avaliação da exposição atual aos riscos mapeados;

• indicação objetiva se a operação está:

◦ dentro do limite de tolerância;

◦ em zona de alerta;

◦ ou em situação de extrapolação do apetite definido;

• medidas corretivas eventualmente adotadas.

Os relatórios deverão integrar o sistema de controle interno e permanecer disponíveis para auditoria.

III – Reavaliação Periódica

O apetite ao risco não possui caráter estático. Sua revisão será obrigatória sempre que ocorrer:

• alteração legislativa relevante;

• mudança estrutural no modelo de atendimento;

• adoção de novas tecnologias (ex.: ferramentas de Inteligência Artificial);

• eventos críticos que revelem inadequação dos parâmetros vigentes.

A revalidação deverá ocorrer, no mínimo, anualmente.

IV – Desvio de Apetite e Incidente Crítico

A ocorrência de evento que ultrapasse o limite máximo de risco aceitável será classificada como Incidente Crítico de Governança, implicando:

• comunicação imediata à autoridade superior;

• acionamento do protocolo interno de contingência;

• registro formal do ocorrido;

• reporte aos órgãos de controle interno e, quando cabível, às autoridades competentes.

Nos casos que envolvam dados pessoais sensíveis, observar-se-á o dever de comunicação previsto na Autoridade Nacional de Proteção de Dados.

8.5 Tabela de Referência – Matriz Sintética de Apetite ao Risco

TIPO DE RISCO	NIVEL DE APETITE	AÇÃO ESPERADA DA EQUIPE
Vida e Integridade do Idoso	Zero	Intervenção imediata, prioridade absoluta e acionamento da rede de proteção.
Proteção de Dados Pessoais e Sigilosos	Baixo	Observância estrita da LGPD, controle de acesso, rastreabilidade e auditoria contínua.
Eficiência Operacional	Moderado	Monitoramento por indicadores, análise de falhas e implementação de melhoria contínua.

09

TRATAMENTO DOS RISCOS

O tratamento de riscos consiste na seleção e implementação de estratégias para modificar o risco, de modo a mantê-lo dentro dos limites do Apetite ao Risco estabelecido pela organização. Após a avaliação da criticidade, os gestores do "Disque Idoso 165" devem escolher a resposta mais eficaz para cada evento identificado.

9.1 Estratégias de Tratamento

As respostas possíveis ao risco são classificadas em quatro categorias principais:

Mitigar (Reduzir): Ações destinadas a diminuir a probabilidade de ocorrência ou reduzir o impacto (severidade) do risco. É a estratégia preferencial para o serviço público.

Exemplo: Implementar treinamento recorrente sobre LGPD para reduzir o risco de vazamento de dados; instalar geradores de energia para mitigar o impacto de quedas de rede elétrica.

Evitar (Eliminar): Alteração radical no processo para eliminar a causa do risco.

Exemplo: Interromper a coleta de um dado que não é essencial e que, se vazado, traria grande risco à integridade do idoso.

Transferir (Compartilhar): Transferir parte do risco a terceiros, sem eliminar a responsabilidade final do órgão.

Exemplo: Contratar empresas especializadas com SLAs (Acordos de Nível de Serviço) rígidos para a manutenção dos sistemas telefônicos, ou firmar parcerias institucionais que dividam a responsabilidade pelo atendimento na ponta.

Aceitar (Monitorar): Decisão fundamentada de manter o risco, caso ele esteja dentro do nível de tolerância ou se o custo de mitigação for superior ao benefício. O risco aceito deve ser permanentemente monitorado.

Exemplo: Aceitar o risco residual de falhas mínimas na rede telefônica que não impactam a urgência, mas manter monitoramento mensal.

9.2 Diretrizes e Regras Operacionais

A execução do tratamento deve seguir rigorosamente as regras abaixo, visando a rastreabilidade e a responsabilidade

Formalização para Riscos Altos e Críticos: Todo risco classificado como "Alto" ou "Crítico" exige obrigatoriamente a criação de um Plano de Ação Formal. Este plano deve conter:

Descrição da ação corretiva/preventiva;

Prazo para implementação (data de início e fim);

Recursos necessários (orçamentários ou humanos);

Indicador de sucesso (como saberemos que o risco foi reduzido?).

Designação de Responsabilidade: Para todo risco identificado, deve haver um "Gestor do Risco" (ou Dono do Risco) claramente designado. Nenhuma mitigação deve ser conduzida de forma coletiva e indefinida; a responsabilidade nominal é fundamental para a governança.

Tratamento de Riscos Materializados: Caso um risco se concretize (ex: um incidente de segurança), a resposta imediata é o acionamento do Plano de Contingência, seguido de:
Análise de Causa Raiz: Entender o que falhou (processo, pessoas ou tecnologia);
Ação Corretiva: Medida imediata para estancar o problema;
Ação Preventiva: Medida para garantir que a falha não se repita.
Documentação e Registro: O tratamento deve ser documentado na "Matriz de Riscos" da unidade, servindo como histórico para auditorias futuras e para o aprimoramento contínuo dos processos.

9.3 Ciclo de Vida do Tratamento (PDCA)

O tratamento não é um evento único, mas um ciclo de melhoria contínua (Planejar - Executar - Verificar - Agir):
Planejamento: Definição da estratégia (mitigar, evitar, etc.) e alocação de recursos.
Implementação: Execução das medidas de controle (controles preventivos e detectivos).
Monitoramento: Verificação se o nível de risco residual (o risco que sobra após a mitigação) está abaixo do limite de tolerância.
Ajuste: Caso o risco residual ainda esteja alto, o ciclo deve ser reiniciado com novas medidas ou nova estratégia.

10 COMUNICAÇÃO, MONITORAMENTO E REPORTE

O monitoramento e a comunicação constituem o ciclo de retroalimentação da Política de Gestão de Riscos. Estes processos garantem que a organização mantenha visibilidade sobre a eficácia dos controles e sobre a evolução do perfil de risco do Disque Idoso 165.

10.1 Monitoramento Contínuo e Indicadores (KRIs)

O monitoramento não será esporádico, mas contínuo. A Coordenação do Disque Idoso utilizará Indicadores-Chave de Risco (KRIs - Key Risk Indicators) para detectar precocemente qualquer desvio em relação ao apetite ao risco definido.
Monitoramento de Controles: Periodicamente, a efetividade dos controles (ex: rotinas de segurança de TI, protocolos de atendimento) será testada. Se um controle falhar, o risco associado será automaticamente reclassificado.
Painel de Bordo (Dashboard): A gestão manterá um painel visual atualizado com indicadores como:
Taxa de abandono de chamadas em horários críticos;
Número de incidentes de violação de dados (LGPD);
Tempo médio de resposta entre a denúncia e o encaminhamento à rede de proteção;
Índice de reclamações sobre a qualidade do atendimento.

10.2 Comunicação de Eventos Críticos (Fluxo de Escalação)

Esta é a regra de ouro para a segurança da pessoa idosa. Qualquer risco que coloque em perigo a integridade física ou a vida do idoso, ou ualquer falha grave de segurança/sigilo, deve seguir um Fluxo de Escalação Imediato:
Identificação pelo Atendente: O colaborador que identificar um evento crítico deve reportar ao Supervisor de Plantão no momento da ocorrência.
Escalação Hierárquica: O Supervisor deve avaliar a severidade e, se necessário, comunicar a Coordenação Geral no prazo máximo de [X] horas.
Comunicação Externa: Se o evento envolver risco iminente à vida, a comunicação deve ser feita simultaneamente aos órgãos de segurança pública ou rede de proteção (CREAS/Ministério Público), sem prejuízo ao registro interno.
Proibição de Ocultação: A tentativa de esconder ou atrasar a comunicação de um evento crítico é considerada falta grave e passível de sanções administrativas.

10.3 Relatórios Periódicos de Gestão

A gestão produzirá relatórios formais para garantir que os tomadores de decisão (Secretaria/Alta Gestão) estejam informados sobre o panorama de riscos:
Relatório Trimestral de Riscos: Documento consolidado apresentando:
Principais riscos monitorados;
Resumo dos incidentes ocorridos no período;
Status das ações de mitigação (concluídas vs. atrasadas);

Novos riscos identificados durante o trimestre.
Reuniões de Revisão de Riscos: Reuniões semestrais da Alta Gestão para avaliar se a Matriz de Riscos ainda reflete a realidade do serviço ou se precisa de ajustes estratégicos.

10.4 Registro Formal e Auditoria (Rastreabilidade)

Toda comunicação ou evento relevante deve ser registrado em sistema informatizado, garantindo a rastreabilidade total (trilha de auditoria).
Diário de Ocorrências de Riscos: Registro cronológico de todos os incidentes. Nenhuma informação deve ser mantida apenas verbalmente.
Padronização: Todos os eventos devem ser registrados com: data/hora, descrição do fato, classificação do risco associado, impacto observado e medida corretiva adotada.
Integridade dos Registros: Os registros devem ser protegidos contra alteração indevida, garantindo que a base de dados sirva como prova documental para eventuais auditorias externas (Tribunais de Contas ou Ministério Público).

BASE LEGAL E REFERENCIAIS NORMATIVOS

11

A presente Política de Gestão de Riscos do Disque Idoso 165 está fundamentada em um conjunto de diplomas legais, normativos e diretrizes que conferem legitimidade e orientam a conduta da instituição. O seu cumprimento é obrigatório e visa assegurar a conformidade, a ética e a eficiência administrativa.

11.1 Legislação Federal (Direito Material)

A atuação do Disque Idoso 165 é regida, primordialmente, pelos seguintes dispositivos legais:
Lei nº 10.741/2003 (Estatuto da Pessoa Idosa): Diploma central que estabelece a obrigação do Estado em criar mecanismos para prevenir toda forma de negligência, discriminação, violência, crueldade ou opressão contra a pessoa idosa (Art. 4º). Esta política visa garantir a efetividade desse mandamento legal através da gestão dos riscos que impedem a proteção social.
Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD): Fundamento obrigatório para o tratamento de dados no canal 165. A política de riscos assegura que o princípio da segurança e da confidencialidade seja respeitado no processamento das denúncias.
Lei nº 12.846/2013 (Lei Anticorrupção): Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública. A gestão de riscos atua como mecanismo de compliance para evitar desvios de finalidade e garantir a integridade do canal.
Lei nº 14.129/2021 (Lei do Governo Digital): Estabelece princípios e diretrizes para a modernização da administração pública, reforçando a importância da segurança da informação e da continuidade dos serviços públicos digitais.

11.2 Referenciais de Governança Pública (Direito Normativo)

Para além da legislação estrita, a política adota as melhores práticas recomendadas pelos órgãos de controle, que funcionam como soft law e orientam as auditorias:
TCU – Referencial de Governança Pública: O Tribunal de Contas da União, por meio de seus referenciais, exige que os órgãos públicos implementem processos de gestão de riscos para assegurar que os resultados pretendidos sejam alcançados. Esta política espelha as recomendações de liderança, estratégia e controle.
CGU – Diretrizes de Gestão de Riscos: A Controladoria-Geral da União estabelece a metodologia de identificação, análise e resposta aos riscos no setor público federal. Este documento foi adaptado para a realidade do Disque Idoso, incorporando a visão de monitoramento contínuo sugerida pela CGU.
Normas da ABNT ISO 31000 (Gestão de Riscos): Embora seja uma norma voluntária, ela é o padrão internacional adotado pela Administração Pública brasileira para definir os processos de gestão de riscos. A estrutura desta política segue as etapas de identificação, análise e tratamento preconizadas pela ISO.
Esta Política de Gestão de Riscos tem força normativa interna e prevalece sobre fluxos operacionais informais.
Prevalência: Em caso de conflito entre esta Política e práticas operacionais antigas, prevalecem as disposições aqui contidas.
Harmonização: Esta política deve ser lida em conjunto com o Regimento Interno do órgão e com as demais normas de conduta vigentes na instituição.
Atualização Permanente: A base legal aqui descrita sofrerá revisões periódicas. Sempre que houver edição de novas leis, decretos ou instruções normativas pelos órgãos de controle (TCU/CGU) que afetem a gestão do Disque Idoso, a coordenação deverá, no prazo de até 90 dias, avaliar a necessidade de atualização desta política.

12

DISPOSIÇÕES FINAIS E VIGÊNCIA

Esta política constitui o pilar normativo da gestão de riscos do serviço "Disque Idoso 165". As disposições aqui contidas visam garantir a longevidade, a clareza e a adaptabilidade do serviço aos desafios institucionais.

12.1 Vigência e Publicidade

Esta Política de Gestão de Riscos entra em vigor na data de sua publicação no veículo oficial de comunicação da instituição ou na rede interna (Intranet), produzindo efeitos imediatos para todos os servidores, colaboradores e prestadores de serviço.

12.2 Revisão Ordinária e Extraordinária

A revisão desta política visa garantir que ela permaneça alinhada às melhores práticas e às mudanças no cenário social e tecnológico.
Revisão Ordinária: Ocorre obrigatoriamente a cada 2 (dois) anos, contados a partir da data de sua última atualização, para avaliar a eficácia dos controles e a adequação da Matriz de Riscos à realidade da operação.
Revisão Extraordinária: Poderá ocorrer a qualquer momento, independentemente do prazo bienal, por decisão da Alta Gestão ou por necessidade de:
Alteração legislativa (ex: mudanças na legislação de proteção ao idoso ou proteção de dados);

Mudanças estruturais significativas no fluxo de atendimento ou nas ferramentas tecnológicas (ex: adoção de inteligência artificial ou novos sistemas de PABX);
Ocorrência de incidentes críticos recorrentes que evidenciem falhas estruturais na política atual.

12.3 Capacitação e Disseminação

A eficácia desta política depende do conhecimento da mesma por todos os agentes envolvidos.
A Coordenação do Disque Idoso 165 compromete-se a promover ações de treinamento e conscientização sempre que esta política for revisada ou quando novos colaboradores ingressarem no serviço.
É dever de cada colaborador ler, compreender e aplicar as diretrizes aqui estabelecidas. O desconhecimento desta política não exime o colaborador de responsabilidade administrativa em caso de falha evitável.

12.4 Integração Normativa

Esta política não substitui as demais normas internas (como o Código de Ética ou Regimento Interno do órgão), mas as complementa. Em caso de conflito entre esta política e regulamentos anteriores, prevalecem as normas mais recentes e específicas sobre gestão de riscos, salvo se a norma anterior conferir maior proteção à pessoa idosa.

12.5 Omissões e Casos Concretos

Os casos omissos ou as dúvidas de interpretação decorrentes da aplicação desta Política serão submetidos à análise do Comitê de Governança ou da autoridade máxima da Pasta (Secretário/Diretor), que emitirá parecer técnico definitivo.

12.6 Termo de Aprovação

Esta Política de Gestão de Riscos foi revista e aprovada pela autoridade competente, nos termos das normas de governança em vigor.

CONTROL 361°

2025/2026