**TeleUp –**

**PLATAFORMA DE TELECOMUNICAÇÃO GAMIFICADA**

### **INTEGRANTES DO PROJETO:**

**Gerenciamento do Projeto**

* **Gerente de Projeto:** Hyttalo Ivann Costa Alves da Silva
* **Coordenadores/Líderes Técnicos:** Mateus Tavares e Guilherme Giacomello

**Time de Estratégia:**

* Gabriel Bento
* Daniel Cabrera
* Guilherme Cordeiro
* Nicollas Torres
* Felipe Correa

**Time de Tecnologia:**

* Vinícius Duarte
* Gustavo Roque
* Ivan Prestes
* João Nunes
* Rafael Satirio
* Guilherme Santos

### **SUMÁRIO:**

**1 INTRODUÇÃO E JUSTIFICATIVA**

**2 PROBLEMAS A SEREM RESOLVIDOS COM A TELEUP**

**3 OBJETIVO**

**4 SOLUÇÃO PROPOSTA**

**5 ESCOPO E MODULOS DE SOLUÇÃO**

**5.1 MODULO 1: DASHBOARD DO OPERADOR**

**5.2 MODULO 2: SISTEMAS DE DISCAGEM INTELIGENTE**

**5.3 MODULO 3: PAINEL DO GESTOR**

**5.4 MÓDULO 4: INTEGRAÇÃO EM NUVEM E ADMINISTRAÇÃO**

**6 TECNOLOGIAS (STACK)**

**7 STAKEHOLDERS DO PROJETO**

**8 PLANEJAMENTO DO PROJETO**

**8.1 DEFINIÇÃO DAS ATIVIDADES (ESTRUTURA ANALÍTICA DO PROJETO)**

**8.2 SEQUENCIAMENTO DAS ATIVIDADES**

**8.3 ESTIMATIVA DE DURAÇÃO**

**8.4 DESENVOLVIMENTO DO CRONOGRAMA**

**8 APLICAÇÃO DA NORMA ISO 27001**

**9 REQUISITOS DO PROJETO**

**9.1 REQUISITOS FUNCIONAIS**

**9.2 REQUISITOS NÃO FUNCIONAIS**

**10 PLANOS DE CONTINGÊNCIA**

**10.1 PLANO DE CONTINGÊNCIA 1: ANÁLISE DE ÁUDIO POR API DE IA**

**10.2 PLANO DE CONTINGÊNCIA 2: FILA INTELIGENTE DE ATENDIMENTO**

**10.3 PLANO DE CONTINGÊNCIA 3: ROTEAMENTO DE CHAMADAS "LIMPAS"**

**10.4 PLANO DE CONTINGÊNCIA 4: DISPONIBILIDADE E INTEGRIDADE DOS DADOS**

**10.5 PLANO DE CONTINGÊNCIA 5: CONTROLES ISO 27001**

**10.6 PLANO DE CONTINGÊNCIA 6: DASHBOARD DE MÉTRICAS EM TEMPO REAL**

**10.7 PLANO DE CONTINGÊNCIA 7: PAINEL DO GESTOR - CRIAÇÃO DE TAREFAS**

**10.8 PLANO DE CONTINGÊNCIA 8: LATÊNCIA NA ENTREGA DE CHAMADAS**

### **1. Introdução e Justificativa**

O setor de telecomunicações enfrenta desafios constantes que vão desde a modernização de sistemas legados até a otimização da mão de obra e a necessidade de evolução tecnológica contínua. Empresas, especialmente startups, necessitam de soluções que unifiquem processos, reduzam o tempo ocioso e integrem-se facilmente a tecnologias em nuvem, tornando a operação mais acessível e eficiente.

### **2. Problemas a Serem Resolvidos**

1. **Sistemas Legados e Fragmentados:** Muitas empresas operam com múltiplos sistemas legados que não se comunicam, gerando processos manuais, lentos e suscetíveis a erros.
2. **Ineficiência dos Discadores Manuais:** A utilização de discadores manuais e a dificuldade em diferenciar chamadas produtivas (seres humanos) de robôs e mensagens automáticas resultam em alto tempo ocioso e baixa produtividade dos operadores.
3. **Necessidade de Modernização e Integração:** Existe uma demanda por um sistema acessível que unifique a infraestrutura e o software, permitindo a integração com serviços em nuvem para otimizar operações.

### **3. Objetivo do Projeto:**

Desenvolver uma plataforma web e gamificada, que substitua sistemas legados e discadores manuais por uma solução inteligente e unificada. O sistema irá otimizar o tempo dos operadores, automatizar processos e aumentar o engajamento da equipe através de elementos de jogos e elementos visuais que “chamem atenção”.

### **4. Solução Proposta**

A solução consiste em criar um sistema novo e mais acessível que unifica as operações e se integra com tecnologias de nuvem. O pilar da plataforma é um sistema inteligente de discagem e filtro de chamadas que diferencia automaticamente robôs e mensagens de seres humanos, direcionando apenas as chamadas válidas para os operadores.

### **5. Escopo e Módulos da Solução**

**Módulo 1: Dashboard do Operador**

* **Funcionalidades:**
  + Visualização de metas diárias/semanais (ex: número de chamadas atendidas, tempo de conversa, resoluções).
  + Sistema de "Fila Inteligente" que entrega apenas chamadas filtradas e validadas.
  + Registro simplificado de chamadas e resultados.
* **Elementos de Gamificação:**
  + **Barra de XP (Experiência):** Cada chamada bem-sucedida ou meta batida preenche uma barra de XP. Ao subir de nível, o operador desbloqueia novos avatares ou temas para sua interface.
  + **Conquistas (Badges):** Medalhas virtuais por marcos importantes ("Primeiras 100 Chamadas", "Rei da Resolução", "Operador Mais Rápido", “Eficiente”).
  + **Missões Diárias:** "Complete 50 chamadas hoje e ganhe 200 pontos”. Esses pontos poderão serem utilizados para trocar por **dayoffs** ou até mesmo por **brindes**!
  + **Conquistas:** Medalhas por marcos, sempre que resolver uma quantidade específica de problema ganha uma medalha
  + **Galeria de conquista:** Histórico visual de progresso, ao atingir um certo nível irá mostrar na plataforma.

**Módulo 2: Sistema de Discagem Inteligente.**

* **Funcionalidades:**
  + Implementação de um sistema que analisa o áudio inicial da chamada para identificar padrões de robôs, URA (Unidade de Resposta Audível) e mensagens automáticas.
  + Integração com APIs de IA para análise de voz e detecção de padrões.
  + Transferência automática e transparente das chamadas "limpas" para a fila dos operadores.
* **Elementos de Gamificação:**

**Indicador de eficiência de IA:** Mostra a % de chamada úteis recebidas

**Módulo 3: Painel do Gestor.**

* **Funcionalidades:**
  + Dashboard com métricas de desempenho em tempo real de toda a equipe.
  + Visualização de rankings de operadores (baseado em pontos de gamificação).
  + Ferramentas para criar e atribuir "Missões", “Pontos” e "Desafios" para a equipe ou para operadores individuais.
  + Relatórios de produtividade, tempo ocioso e eficiência do discador.
* **Elementos de Gamificação:**
  + **Ranking da Semana/Mês:** Exibe um pódio com os 3 melhores operadores, incentivando a competição saudável.
  + **Desafios em Equipe:** "Se a equipe inteira atingir 10.000 pontos até sexta-feira, todos ganham um bônus ou uma noite da Pizza!".
  + **Loja de Recompensas:** Os pontos acumulados pelos operadores podem ser trocados por recompensas reais (folgas, vouchers etc.) ou virtuais (customização da interface).

**Módulo 4: Integração em Nuvem e Administração**

* **Funcionalidades:**
  + Módulo para configurar a integração com outros sistemas (CRMs, bancos de dados) via APIs.
  + Gerenciamento de usuários e permissões.
  + Configuração dos parâmetros do sistema de discagem e das regras de gamificação.

### **6. Tecnologias que serão utilizadas (Stack):**

* **Frontend:** React (para criar uma interface dinâmica e reativa, ideal para dashboards em tempo real).
* **Backend:** Node.js com Express (para lidar com as requisições, lógica de negócio e integração com APIs).
* **Banco de Dados:** MySQL (para armazenar dados de usuários, chamadas e progresso da gamificação).
* **Cloud e IA:** Utilização de serviços como AWS (Amazon Web Services) ou Google Cloud para hospedar a aplicação e usar suas APIs de Machine Learning/AI para a análise de voz (ex: Amazon Transcribe, Google Speech-to-Text).

**Stakeholders do Projeto**

Nosso projeto visa uma usabilidade mais intuitiva e otimizada da plataforma para empresas do ramo de Telecom, e deste modo impactamos de forma positiva os seguintes grupos:

* **Operadores de Telecomunicações:** Os colaboradores principais são os atendentes, pois, através deles que obteremos o resultado do projeto.
* **Equipe de Desenvolvimento (Frontend/Backend/DevOps):** Pois, eles terão uma plataforma atualizada e completa, facilitando a manutenibilidade do projeto a qualquer momento.
* **Administradores do Sistema:** Responsáveis por gerenciar usuários, permissões e integrações com outros sistemas através do módulo de administração.
* **Patrocinador(es) do Projeto:** Embora não nomeado, é a pessoa ou grupo que está financiando o projeto. O interesse principal é o retorno sobre o investimento, seja por meio da redução de custos, aumento de eficiência ou modernização tecnológica.
* **Empresas/Clientes (Especialmente Startups):** O público-alvo da solução, que busca unificar processos e integrar tecnologias em nuvem de forma acessível.

### **7. Desenho do Planejamento do Projeto**

Esta seção detalha os processos de planejamento para transformar o escopo definido em um plano de ação executável.

**Definição das Atividades (Estrutura Analítica do Projeto)**

As entregas dos módulos serão decompostas/fragmentadas nas seguintes atividades:

* **Módulo 1: Dashboard do Operador**
  + 1.1. Design da Interface (UI/UX) do Dashboard.
  + 1.2. Desenvolvimento Frontend da visualização de metas.
  + 1.3. Desenvolvimento Frontend do sistema de "Fila Inteligente e gamificação".
  + 1.5. Integração do Frontend com as APIs do Backend.
* **Módulo 2: Sistema de Discagem Inteligente**
  + 2.1. Prova de Conceito (PoC) e seleção da API de IA para análise de voz.
  + 2.2. Desenvolvimento do serviço de Backend para receber e analisar o áudio das chamadas.
  + 2.3. Implementação da lógica de classificação (humano vs. robô).
  + 2.4. Desenvolvimento do sistema de transferência de chamadas "limpas" para a fila.
* **Módulo 3: Painel do Gestor**
  + 3.1. Design da Interface (UI/UX) do Painel.
  + 3.2. Desenvolvimento Frontend dos dashboards e métricas em tempo real.
  + 3.3. Desenvolvimento da ferramenta de criação de Missões e Desafios.
  + 3.4. Implementação Frontend do Ranking e da Loja de Recompensas.
  + 3.5. Desenvolvimento dos relatórios de produtividade.
* **Módulo 4: Integração em Nuvem e Administração**
  + 4.1. Configuração da infraestrutura base na nuvem (AWS/Google Cloud).
  + 4.2. Desenvolvimento do serviço de autenticação e gerenciamento de usuários/permissões.
  + 4.3. Desenvolvimento do painel de administração para configuração de regras (gamificação, discador).
  + 4.4. Criação e documentação das APIs para integração com sistemas externos (CRMs).

### **8. Sequenciamento das Atividades**

As atividades serão ordenadas com base nas suas dependências:

* **Dependência Primária:** A configuração da infraestrutura em nuvem (Atividade 4.1) é um pré-requisito para iniciar a maior parte do desenvolvimento de Backend.
* **Backend => Frontend:** O desenvolvimento das APIs do backend (Módulos 2 e 4) deve ser priorizado para que as equipes de Frontend (Módulos 1 e 3) possam consumir os dados e funcionalidades.
* **Paralelismo:** O desenvolvimento do Dashboard do Operador (Módulo 1) e do Painel do Gestor (Módulo 3) pode ocorrer em paralelo, desde que as APIs do backend estejam definidas.

### **9. Estimativa de Duração**

As durações serão estimadas em reuniões/calls de planejamento com os líderes técnicos e a equipe de desenvolvimento. Será utilizada a **Estimativa de 3 Pontos** para cada atividade principal, considerando cenários otimista, pessimista e mais provável, a fim de criar um cronograma mais resiliente.

**Desenvolvimento do Cronograma**

* **Semana 1:** Infraestrutura na nuvem configurada e Prova de Conceito da IA concluída.
* **Semana 2:** Backend do Sistema de Discagem Inteligente (v1) finalizado.
* **Semana 3:** Dashboard do Operador (v1) funcional e integrado.
* **Semana 4:** Painel do Gestor (v1) e sistema de administração concluídos.
* **Semana 5:** Fase de Testes de Aceitação do Usuário (UAT) e Correções.
* **Semana 6:** Lançamento da Plataforma.

### **10. Aplicação da ISO 27001 na TeleUp**

**Seção 5.2 – Diretrizes de Proteção de Dados**

A regra exige que a empresa crie normas de proteção de dados alinhadas ao seu objetivo, divulgadas internamente e acessíveis a todos os interessados.

**Motivo na TeleUp:** Essa exigência assegura que todos (operadores, gerentes e programadores) entendam as regras de proteção dos dados de clientes e chamadas. Essencial, pois o sistema lida com dados confidenciais de telecomunicações, e uma norma formal impede uso inadequado e falhas de adequação.

**Seção A.9.1 – Gerenciamento de Acesso**

O acesso aos sistemas e aplicativos deve ser controlado por meio de processos formais de gerenciamento de permissões, garantindo que somente usuários autorizados acessem os recursos.

**Motivo na TeleUp:** Impacta o módulo de administração, onde cada perfil (operador, gerente, administrador) tem diferentes níveis de acesso. Isso diminui chances de fraudes internas, erros humanos e acesso indevido a dados cruciais da plataforma.

**Seção A.17.1 – Garantia da Segurança da Informação**

A empresa deve criar processos para garantir o acesso às informações e sistemas em situações de incidentes ou falhas graves.

**Motivo na TeleUp:** O sistema depende de estrutura em nuvem e APIs de IA. Se um serviço parar de funcionar, a continuidade dos negócios precisa ser garantida. Ter redundância e planos de ação garante que operadores não parem, mantendo a produtividade da empresa.

**Seção A.18.1 – Respeito às Leis e Contratos**

A empresa deve identificar, registrar e manter a conformidade com as leis aplicáveis à segurança da informação.

**Motivo na TeleUp:** Como o sistema usa dados pessoais de clientes e chamadas, é obrigatório seguir a LGPD. Essa proteção garante armazenamento criptografado, descarte correto e uso transparente dos dados, protegendo a empresa de riscos legais e aumentando a confiança dos clientes.

**Seção 10.1 – Aprimoramento Contínuo do SGSI**

A empresa deve melhorar continuamente a adequação, suficiência e eficácia do Sistema de Gerenciamento da Segurança da Informação.

**Motivo na TeleUp:** No painel do gerente e nas rotinas internas, será possível analisar métricas, detectar problemas e aplicar melhorias sempre. Isso mantém o sistema atualizado contra novas ameaças, garantindo que a plataforma continue segura e competitiva no mercado de telecomunicações.

### **11. Requisitos Funcionais e Não Funcionais**

**Requisitos Funcionais Externos (Visíveis ao Usuário):**

1. O sistema deve exibir ao operador um dashboard com suas metas diárias/semanais de desempenho.
2. O operador deve poder visualizar e interagir com uma "Fila Inteligente" que lhe entrega apenas as chamadas válidas. (Alto Risco)
3. O operador deve poder visualizar o progresso de sua barra de XP e o seu nível atual na interface.
4. O operador deve ter acesso a uma galeria visual para ver todas as medalhas e títulos que já conquistou.
5. O gestor deve poder visualizar um dashboard com as métricas de desempenho de toda a equipe em tempo real. (Alto Risco)
6. O gestor deve poder visualizar um ranking com os melhores operadores da semana ou do mês.
7. O gestor deve ter uma ferramenta em seu painel para criar e atribuir missões e desafios para a equipe. (Alto Risco)
8. O gestor deve poder gerar relatórios de produtividade, tempo ocioso e eficiência do discador.
9. O operador deve poder acessar uma "Loja de Recompensas" para trocar seus pontos acumulados por prêmios ou até mesmo Day-offs.
10. O operador deve poder customizar seu avatar ou aplicar temas para personalizar sua interface ao subir de nível.

**Requisitos Funcionais Internos (Processos do Sistema):**

1. O sistema deve integrar-se com APIs de IA para analisar o conteúdo de áudio das chamadas recebidas. (Alto Risco)
2. O sistema deve aplicar uma lógica de classificação para diferenciar automaticamente chamadas de "seres humanos" de "robôs/URAs".
3. O sistema deve rotear as chamadas classificadas como "limpas" para a fila de operadores disponíveis. (Alto Risco)
4. O sistema deve calcular e atribuir pontos de experiência (XP) e recompensas com base em regras de gamificação configuradas.
5. O sistema deve processar a troca de pontos por recompensas, atualizando o saldo do operador e registrando a transação em tempo real.
6. O sistema deve permitir que um administrador cadastre, edite e remova usuários, além de gerenciar seus níveis de permissão.
7. O sistema deve permitir que um administrador configure os parâmetros do discador inteligente através de um painel de controle.
8. O sistema deve registrar em banco de dados o histórico de chamadas, incluindo resultados/tabulação e duração, para a geração de relatórios.
9. O sistema deve autenticar usuários com base em suas credenciais e permissões antes de conceder acesso aos módulos.
10. O sistema deve fornecer endpoints de API’s documentados para permitir a integração com sistemas externos, como CRMs.

**Requisitos Não Funcionais (RNF)**

**Requisitos Não Funcionais Externos (Percebidos pelo Usuário)**

1. A interface do operador deve ser intuitiva, exigindo o mínimo de treinamento para o uso das funções principais.
2. Os elementos de gamificação (barras de XP, badges) devem ser visualmente claros e compreensíveis para o usuário.
3. As métricas no dashboard do gestor devem ser atualizadas em tempo real, com uma latência máxima de 5 segundos.
4. O tempo entre o fim de uma chamada e a entrega da próxima na "Fila Inteligente" não deve exceder 10 segundos. (Alto Risco)
5. A plataforma deve estar disponível para os usuários durante 99.5% do tempo em horário comercial. (Alto Risco)
6. O sistema não deve perder o registro de progresso de gamificação (XP, missões, pontos) de um operador, mesmo em caso de falha momentânea. (Alto Risco)
7. A interface web deve ser reativa, funcionando de forma fluida em navegadores modernos (Chrome, Firefox, Edge).
8. O sistema deve fornecer confirmações visuais imediatas para ações do usuário (ex: "Missão criada com sucesso!").
9. O usuário deve perceber uma mudança visual imediata em sua interface ao selecionar um novo tema ou avatar desbloqueado.
10. A interface deve seguir as diretrizes básicas da WCAG (Web Content Accessibility Guidelines) para garantir o uso por pessoas com deficiências visuais ou motoras.

**4. Requisitos Não Funcionais Internos (Técnicos e de Qualidade)**

1. O sistema deve implementar os controles da norma ISO 27001 para garantir a gestão da segurança da informação. (Alto Risco)
2. A comunicação entre o Frontend e o backend deve ser criptografada utilizando TLS (Transport Layer Security).
3. A arquitetura em nuvem (AWS/Google Cloud) deve ser capaz de escalar horizontalmente para suportar um aumento de 50% no número de operadores sem degradação de performance.
4. O código-fonte deve seguir os padrões de estilo e boas práticas da linguagem utilizada (Javascript/TypeScript) para facilitar a manutenção.
5. O banco de dados deve usar constraints (chaves estrangeiras, checagens) para garantir a integridade referencial dos dados.
6. O backend desenvolvido com Node.js deve ser conteinerizado (ex: Docker) para garantir a portabilidade entre diferentes ambientes de nuvem.
7. O sistema deve ter rotinas de backup diárias e um plano de recuperação de desastres para o banco de dados.
8. O projeto deve ter uma cobertura de testes unitários de, no mínimo, 70% para as lógicas de negócio críticas no backend.
9. Documentação da API de integração deve ser gerada automaticamente e estar sempre sincronizada com o código.
10. O sistema deve manter logs detalhados de todas as operações críticas realizadas no painel de administração para fins de auditoria.

### **12. Planos de contingências**

### **Plano de Contingência 1: Análise de Áudio por API de IA:**

**1. OBJETIVO:** Garantir a continuidade da operação e a integridade da análise de chamadas, minimizando o impacto de falhas na integração com as APIs de IA. O objetivo é assegurar que, mesmo com a indisponibilidade ou degradação do serviço de análise de áudio, as operações de atendimento e análise de dados possam prosseguir de forma controlada.

**2. ESCOPO E ABRANGÊNCIA:** Este plano cobre as falhas que ocorrem na integração entre a plataforma e as APIs de Inteligência Artificial responsáveis pela análise de áudio das chamadas.

**3. CENÁRIOS DE RISCO COBERTOS:**

* **Falha Total da API:** A API de IA para de responder às requisições, retornando erros (e.g., 5xx, 4xx) ou timeouts, impedindo completamente a análise de áudio.
* **Degradação Severa de Performance (Alta Latência):** O tempo de resposta da API aumenta significativamente, causando atrasos inaceitáveis no processamento das chamadas.
* **Análises Incorretas ou Inconsistentes:** A API retorna análises de baixa qualidade, dados sem sentido ou classificações errôneas que comprometem a operação.
* **Falha de Segurança ou Vazamento de Dados:** Detecção de uma violação de segurança na comunicação com a API ou na própria API, colocando em risco a confidencialidade dos dados de áudio.

**4. GATILHOS PARA ATIVAÇÃO DO PLANO:**

* **Alerta de Monitoramento:** Recebimento de um alerta crítico indicando uma taxa de erro superior a 10% nas chamadas à API, ou latência média acima do limite predefinido por mais de 5 minutos.
* **Validação Manual de Inconsistência:** Confirmação pela equipe de qualidade ou operações de que 5 ou mais chamadas consecutivas tiveram suas análises retornadas de forma incorreta.
* **Notificação Oficial do Provedor da API:** Recebimento de um comunicado do fornecedor da API informando sobre uma indisponibilidade.

**5. PAPÉIS E RESPONSABILIDADES:**

* **Ativar plano e investigar causa:**
  + **Responsável:** Líder Técnico de TI
* **Declarar incidente e comunicar severidade:**
  + **Responsável:** Líder Técnico de TI
* **Anunciar modo de contingência a stakeholders:**
  + **Responsável:** Gerente de Produto
* **Contatar suporte do provedor da API:**
  + **Responsável:** Líder Técnico de TI

**6. AÇÕES IMEDIATAS (CHECKLIST 0-15 MINUTOS):**

* **Passo 1:**
  + **Ação:** Validar a abrangência da falha (geral, intermitente ou isolada) através dos dashboards de monitoramento.
  + **Responsável:** Líder Técnico de TI.
* **Passo 2:**
  + **Ação:** Notificar o Gerente de Produto e a Gerência de Operações declarando o início do incidente e o nível de severidade.
  + **Responsável:** Líder Técnico de TI.
* **Passo 3:**
  + **Ação:** Anunciar à equipe de análise e stakeholders a ativação do "Modo de Contingência" e o plano a ser seguido (B ou C).
  + **Responsável:** Gerente de Produto.
* **Passo 4:**
  + **Ação:** Iniciar a investigação da causa raiz do problema e o contato com o suporte técnico do provedor da API.
  + **Responsável:** Líder Técnico de TI.

**7. ESTRATÉGIAS DE CONTINGÊNCIA:**

**PLANO B: MODO DE PROCESSAMENTO ASSÍNCRONO (TOLERÂNCIA À LATÊNCIA)**

* **Descrição:** Plano preferencial para cenários de alta latência. O sistema desacopla a análise de áudio do fluxo principal da chamada, que é finalizada normalmente. O áudio é colocado em uma fila para ser analisado posteriormente.
* **Ação Técnica:** Executar o procedimento para desviar o fluxo de análise de síncrono para assíncrono, utilizando uma fila de processamento.
* **Ação Operacional:** Comunicar às áreas de negócio que as análises das chamadas do período estarão disponíveis com atraso.

**PLANO C: MODO DE BYPASS (DESATIVAÇÃO TEMPORÁRIA)**

* **Descrição:** Utilizado em caso de falha total ou de análises incorretas da API, onde a integração é completamente desativada.
* **Ação Técnica:** Alterar a configuração do sistema para desativar a chamada à API de análise de áudio. As gravações das chamadas são armazenadas para possível análise futura.
* **Ação Operacional:** Instruir a equipe de qualidade e operações a realizar análises manuais por amostragem, caso necessário. O negócio deve ser informado sobre a ausência total de dados de análise de IA durante o período.

**8. PLANO DE COMUNICAÇÃO:**

* **Público: Equipe Técnica**
  + **Canal:** Canal dedicado (Slack/Teams)
  + **Frequência:** Tempo Real
  + **Responsável:** Líder Técnico de TI
* **Público: Gestores/Stakeholders**
  + **Canal:** E-mail/Grupo de Status
  + **Frequência:** A cada 60 min
  + **Responsável:** Gerente do Produto
* **Público: Provedor API**
  + **Canal:** Portal de suporte / e-mail
  + **Frequência:** Conforme necessário
  + **Responsável:** Líder Técnico de TI

**9. PROCESSO DE RETORNO À NORMALIDADE:**

1. **Validação da Correção:** A equipe de TI, em conjunto com o provedor da API, válida a resolução da falha em um ambiente de homologação ou através de testes controlados.
2. **Ativação Gradual (Canary Release):** A integração com a API de IA é reativada para um percentual baixo do tráfego (e.g., 5% das chamadas) para monitoramento de estabilidade.
3. **Reativação Total:** Após a confirmação da estabilidade, a funcionalidade é reativada para 100% das chamadas.
4. **Processamento Retroativo:** Caso o Plano B tenha sido ativado, a fila de chamadas pendentes de análise é processada.
5. **Comunicação de Encerramento:** O Líder Técnico de TI e o Gerente de Produto comunicam o fim do incidente a todos os stakeholders.

**10. PÓS-INCIDENTE:**

* Realizar reunião de post-mortem em até 48 horas após a resolução do incidente.
* Analisar a causa raiz detalhada da falha.
* Avaliar a eficácia do plano de contingência executado e o tempo de resposta.
* Identificar e documentar melhorias no sistema (e.g., timeouts mais agressivos, Circuit breaker aprimorado) e no próprio plano para evitar recorrências.

1. **TESTES E SIMULAÇÕES:**

O plano deverá ser testado semestralmente através de simulações de falhas controladas para validar a eficácia dos procedimentos e tempos de resposta.

### **Plano de Contingência 2: Fila Inteligente de Atendimento**

**Funcionalidade:** Fila Inteligente de Atendimento

**1.OBJETIVO:** Garantir a continuidade da operação de atendimento, minimizando o tempo de inatividade dos operadores e o impacto no cliente final, caso a funcionalidade "Fila Inteligente" apresente falhas que impeçam a distribuição de chamadas válidas.

**2. ESCOPO E ABRANGÊNCIA** Este plano cobre falhas totais ou parciais na funcionalidade "Fila Inteligente" que impeçam a correta distribuição de chamadas aos operadores.

**3. CENÁRIOS DE RISCO COBERTOS**

* **Falha Total:** A Fila Inteligente para completamente de entregar chamadas aos operadores.
* **Falha de Filtragem (Envenenamento da Fila):** A fila entrega chamadas inválidas (robôs, chamadas mudas etc.), reduzindo a eficiência da equipe.
* **Degradação Severa de Performance:** A fila entrega chamadas com um atraso significativo, deixando os operadores ociosos.
* **Falha na Interface do Usuário (UI):** Os operadores não conseguem visualizar, receber ou interagir com as chamadas na fila.

**4. GATILHOS PARA ATIVAÇÃO DO PLANO**

* **Alerta de Monitoramento:** Recebimento de um alerta crítico do sistema de monitoramento de TI relacionado à API ou ao serviço da Fila Inteligente.
* **Relatos de Múltiplos Operadores:** Confirmação de que 3 ou mais operadores estão relatando o mesmo problema de indisponibilidade.
* **Queda de KPIs em Tempo Real:** Detecção de uma queda abrupta (> 30%) em indicadores chave como "Chamadas Atendidas por Hora" ou "Taxa de Ocupação dos Operadores".

**5. PAPÉIS E RESPONSABILIDADES**

* **Ativar plano de contingência:**
  + **Responsável:** Supervisor de Operações ou Líder Técnico de TI
* **Validar falha e notificar gerência:**
  + **Responsável:** Supervisor de Operações
* **Anunciar modo de contingência à equipe:**
  + **Responsável:** Supervisor de Operações
* **Iniciar investigação da causa raiz:**
  + **Responsável:** Líder Técnico de TI

**6. AÇÕES IMEDIATAS (CHECKLIST 0-15 MINUTOS)**

* **Passo 1:**
  + **Ação:** Validar a abrangência da falha (se é geral ou isolada).
  + **Responsável:** Supervisor de Operações.
* **Passo 2:**
  + **Ação:** Notificar o Líder Técnico de TI e a Gerência de Operações declarando o início do incidente.
  + **Responsável:** Supervisor de Operações.
* **Passo 3:**
  + **Ação:** Anunciar à equipe de atendimento a ativação do "Modo de Contingência" e o plano a ser seguido (B ou C).
  + **Responsável:** Supervisor de Operações.
* **Passo 4:**
  + **Ação:** Iniciar a investigação da causa raiz do problema em paralelo.
  + **Responsável:** Líder Técnico de TI.

**7. ESTRATÉGIAS DE CONTINGÊNCIA:**

**PLANO B: MODO DE BYPASS (FILA "NÃO INTELIGENTE")**

* **Descrição:** Plano preferencial. A camada de "inteligência" (filtragem) é desativada, e o sistema passa a operar como uma fila tradicional, entregando todas as chamadas recebidas aos operadores.
* **Ação Técnica:** Executar o procedimento para desativar o módulo de classificação de chamadas.
* **Ação Operacional:** Instruir os operadores a classificar manualmente chamadas inválidas e encerrá-las rapidamente.

**PLANO C: MODO DE ROTEAMENTO DIRETO (ÚLTIMO RECURSO)**

* **Descrição:** Utilizado se todo o sistema de filas falhar. A central telefônica é reconfigurada para distribuir chamadas diretamente para grupos de ramais.
* **Ação Técnica:** Alterar a rota de entrada das chamadas diretamente na central telefônica.
* **Ação Operacional:** Instruir os operadores a atenderem chamadas diretamente em seus ramais. O controle de produtividade passa a ser manual.

**8. PLANO DE COMUNICAÇÃO**

* **Público: Equipe de Operações**
  + **Canal:** Chat em grupo / Verbal
  + **Frequência:** Imediata e conforme necessário
  + **Responsável:** Supervisor de Operações
* **Público: Gestores / Stakeholders**
  + **Canal:** E-mail
  + **Frequência:** A cada 60 min. ou em marcos importantes
  + **Responsável:** Gerente de Operações
* **Público: Equipe Técnica**
  + **Canal:** Canal dedicado (Slack/Teams)
  + **Frequência:** Tempo real
  + **Responsável:** Líder Técnico de TI

**9. PROCESSO DE RETORNO À NORMALIDADE**

1. **Validação da Correção:** A equipe de TI corrige a falha em um ambiente de homologação.
2. **Ativação Gradual (Canary Release):** A Fila Inteligente é reativada para um pequeno grupo de operadores "piloto" para monitoramento de estabilidade.
3. **Reativação Total:** Após a confirmação da estabilidade, a funcionalidade é reativada para todos os operadores.
4. **Comunicação de Encerramento:** O Supervisor de Operações e o Gerente de Operações comunicam o fim do incidente.

**10. PÓS-INCIDENTE**

* Realizar reunião de post-mortem em até 48 horas após a resolução do incidente.
* Analisar a causa raiz da falha.
* Avaliar a eficácia do plano de contingência executado.
* Identificar e documentar melhorias no sistema e no próprio plano para evitar recorrências.

1. **TESTES E SIMULAÇÕES:**

O plano deverá ser testado semestralmente através de simulações de falhas controladas para validar a eficácia dos procedimentos e tempos de resposta.

### **Plano de Contingência 3: Roteamento de Chamadas "Limpas":**

**FUNCIONALIDADE:** Roteamento de chamadas "Limpas"

**1. OBJETIVO:** Garantir a continuidade do roteamento de chamadas "limpas" para os operadores, assegurando a disponibilidade do atendimento mesmo em situações de falha técnica ou indisponibilidade do sistema.

**2. ESCOPO E ABRANGÊNCIA** Este plano cobre falhas no sistema de roteamento automático de chamadas, desde a classificação pela IA até a entrega na fila dos operadores.

**3. CENÁRIOS DE RISCO COBERTOS**

* **Falha no Roteamento Automático:** O sistema falha em direcionar as chamadas classificadas como "limpas" para a fila de operadores disponíveis. O impacto inclui a interrupção do atendimento e o aumento do tempo ocioso dos operadores.
* **Indisponibilidade da API de IA:** A API usada para análise de chamadas fica indisponível.
* **Erro de Classificação:** Ocorre erro na diferenciação entre chamadas humanas e robôs (falso positivo/negativo).
* **Falha de Integração ou Conectividade:** Ocorrem falhas na comunicação entre o backend e a fila de operadores ou entre módulos do sistema.

**4. GATILHOS PARA ATIVAÇÃO DO PLANO**

* **Alerta de Monitoramento:** Alertas indicando indisponibilidade da API de IA ou gargalos na fila de atendimento.
* **Falha de Classificação:** Detecção de erros de classificação em chamadas pela equipe de operações.
* **Interrupção do Fluxo:** Ausência de novas chamadas sendo entregues aos operadores por um período anômalo.

**5. PAPÉIS E RESPONSABILIDADES**

* **Identificação e correção de falhas técnicas:**
  + **Responsável:** Equipe de Tecnologia (Backend/DevOps)
* **Execução do plano de fallback manual:**
  + **Responsável:** Equipe de Operações
* **Comunicação com stakeholders em incidente crítico:**
  + **Responsável:** Gerente de Projeto

**6. AÇÕES IMEDIATAS (CHECKLIST 0-15 MINUTOS)**

* **Passo 1:**
  + **Ação:** Validar a falha através dos sistemas de monitoramento.
  + **Responsável:** Equipe de Tecnologia.
* **Passo 2:**
  + **Ação:** Notificar a Equipe de Operações e o Gerente de Projeto sobre o incidente.
  + **Responsável:** Equipe de Tecnologia.
* **Passo 3:**
  + **Ação:** Decidir e anunciar qual plano de contingência será ativado (B ou C).
  + **Responsável:** Equipe de Tecnologia.
* **Passo 4:**
  + **Ação:** Iniciar a investigação da causa raiz e registrar todas as ações.
  + **Responsável:** Equipe de Tecnologia.

**7. ESTRATÉGIAS DE CONTINGÊNCIA**

**PLANO B: MODO DE DEGRADAÇÃO CONTROLADA (PLANO PREFERENCIAL)**

* **Descrição:** Utiliza mecanismos automáticos para contornar falhas parciais e manter o fluxo de chamadas.
* **Ação Técnica 1 (Troca de Provedor):** Se a API de IA principal falhar, o sistema automaticamente comuta para a API alternativa configurada.
* **Ação Técnica 2 (Roteamento Padrão):** Caso a IA não consiga classificar uma chamada, ela será tratada como "limpa" por padrão e direcionada à fila para evitar a perda do contato.

**PLANO C: MODO DE INTERVENÇÃO MANUAL (ÚLTIMO RECURSO)**

* **Descrição:** Utilizado em caso de falha total do roteamento automático.
* **Ação Técnica:** Redirecionar as chamadas "limpas" para um ponto de distribuição centralizado.
* **Ação Operacional (Fallback Manual):** As chamadas são redirecionadas para um supervisor ou operador dedicado, que fará a distribuição manual para a equipe.

**8. PLANO DE COMUNICAÇÃO**

* **Público: Equipe Técnica**
  + **Canal:** Canal dedicado (Slack/Teams)
  + **Frequência:** Tempo Real
  + **Responsável:** Equipe de Tecnologia
* **Público: Equipe de Operações**
  + **Canal:** Chat em grupo
  + **Frequência:** Imediata e conforme necessário
  + **Responsável:** Equipe de Operações
* **Público: Gestores / Stakeholders**
  + **Canal:** E-mail
  + **Frequência:** Conforme necessário em incidente crítico
  + **Responsável:** Gerente de Projeto

**9. PROCESSO DE RETORNO À NORMALIDADE**

1. **Validação da Correção:** A equipe de tecnologia verifica os logs para rastrear a causa da falha e aplica a correção em ambiente de teste.
2. **Ativação Gradual:** O sistema de roteamento automático é reativado de forma controlada.
3. **Monitoramento Contínuo:** A fila e a taxa de classificação são monitoradas para garantir a estabilidade.
4. **Comunicação de Encerramento:** O Gerente de Projeto comunica o fim do incidente.

**10. PÓS-INCIDENTE**

* Verificar os logs para rastrear a causa da falha.
* Atualizar a documentação e as métricas para prevenir reincidência.
* Comunicar os clientes impactados, se necessário.
* Analisar o cumprimento das métricas de sucesso, como MTTR inferior a 30 minutos e menos de 5% de chamadas perdidas.

1. **TESTES E SIMULAÇÕES:**

O plano deverá ser testado semestralmente através de simulações de falhas controladas para validar a eficácia dos procedimentos e tempos de resposta.

### **Plano de Contingência 4: Disponibilidade da Plataforma e Integridade dos Dados de Gamificação:**

**FUNCIONALIDADE:** Disponibilidade da Plataforma e Integridade dos Dados de Gamificação

**1. OBJETIVO:** Garantir a continuidade operacional da plataforma durante o horário comercial, assegurando disponibilidade mínima de 99,5% e prevenindo a perda de dados de gamificação (XP, missões, pontos) em caso de falhas técnicas.

**2. ESCOPO E ABRANGÊNCIA:** Este plano aplica-se aos serviços principais da plataforma, incluindo autenticação de usuários e processamento de eventos de gamificação. Não estão contemplados aspectos de suporte ao cliente e incidentes fora do horário comercial.

**3. CENÁRIOS DE RISCO COBERTOS:**

* **Indisponibilidade da plataforma:** Queda total ou parcial que impeça o acesso dos usuários.
* **Falha no registro de gamificação:** Perda momentânea de dados de progresso (XP, missões, pontos) devido a falhas de sistema.
* **Degradação severa de performance:** Lentidão crítica que afete a experiência do usuário e o registro de dados.

**4. GATILHOS PARA ATIVAÇÃO DO PLANO:**

* **Monitoramento de SLA:** Alerta de disponibilidade abaixo de 99,5% em horário comercial.
* **Falha no banco de dados de gamificação:** Indicação de perda de dados ou inconsistência.
* **Relatos de usuários:** Múltiplos operadores relatam perda de progresso ou indisponibilidade.

**5. PAPÉIS E RESPONSABILIDADES:**

* **Atividade: Ativar plano de contingência**
  + **Responsável (R):** Líder Técnico de TI
  + **Aprovador (A):** Gerente de Operações
  + **Consultado (C):** Equipe Técnica
  + **Informado (I):** Equipe de Operações
* **Atividade: Comunicação do incidente**
  + **Responsável (R):** Supervisor de Operações
  + **Aprovador (A):** Gerente de Operações
  + **Consultado (C):** Equipe Técnica
  + **Informado (I):** Usuários-chave
* **Atividade: Recuperação de dados**
  + **Responsável (R):** Equipe Técnica de TI
  + **Aprovador (A):** Líder Técnico de TI
  + **Consultado (C):** Suporte do provedor de nuvem
  + **Informado (I):** Gerência
* **Atividade: Validação de retorno à normalidade**
  + **Responsável (R):** Equipe Técnica de TI
  + **Aprovador (A):** Gerente de Operações
  + **Consultado (C):** Supervisor de Operações
  + **Informado (I):** Todos os envolvidos

**6. AÇÕES IMEDIATAS (CHECKLIST 0-15 MINUTOS)**

* **Passo 1:**
  + **Ação:** Validar escopo da falha (disponibilidade, perda de dados ou ambos).
  + **Responsável:** Líder Técnico de TI.
* **Passo 2:**
  + **Ação:** Notificar equipe de operações e gerência sobre o incidente.
  + **Responsável:** Supervisor de Operações.
* **Passo 3:**
  + **Ação:** Ativar modo de contingência (Plano B ou C).
  + **Responsável:** Líder Técnico de TI.
* **Passo 4:**
  + **Ação:** Iniciar investigação da causa raiz.
  + **Responsável:** Equipe Técnica de TI.

**7. ESTRATÉGIAS DE CONTINGÊNCIA**

**PLANO B: MODO DE ALTA DISPONIBILIDADE**

* **Descrição:** Redirecionar tráfego para infraestrutura secundária (ex.: servidores em outra região).
* **Ação Técnica:** Ativar balanceador de carga e replicação de banco de dados em tempo real.
* **Ação Operacional:** Monitorar métricas de disponibilidade e integridade dos dados.

**PLANO C: MODO DE RECUPERAÇÃO DE DADOS**

* **Descrição:** Recuperar dados de gamificação a partir de backups ou filas de mensagens.
* **Ação Técnica:** Restaurar backup mais recente ou reprocessar eventos via Kafka/RabbitMQ.
* **Ação Operacional:** Validar consistência dos dados antes do retorno à normalidade.

**8. PLANO DE COMUNICAÇÃO**

* **Público: Equipe de Operações**
  + **Canal:** Chat/Slack
  + **Frequência:** Imediato e atualizações
  + **Responsável:** Supervisor de Operações
* **Público: Gerência**
  + **Canal:** E-mail
  + **Frequência:** A cada 60 minutos
  + **Responsável:** Gerente de Operações
* **Público: Equipe Técnica**
  + **Canal:** Canal dedicado (TI)
  + **Frequência:** Tempo real
  + **Responsável:** Líder Técnico de TI

**9. PROCESSO DE RETORNO À NORMALIDADE**

1. **Validação da Correção:** Equipe de TI confirma que a falha foi resolvida em ambiente de teste.
2. **Ativação Gradual:** Serviços são restaurados gradualmente (ex.: Canary Release).
3. **Monitoramento Contínuo:** Verificar disponibilidade e integridade dos dados por 1 hora.
4. **Comunicação de Encerramento:** Supervisor de Operações anuncia o fim do incidente.

**10. PÓS-INCIDENTE**

* Realizar reunião de post-mortem em até 48 horas.
* Documentar causas raiz e ações preventivas futuras.
* Atualizar plano de contingência conforme necessário.

1. **TESTES E SIMULAÇÕES:**

O plano deverá ser testado semestralmente através de simulações de falhas controladas, validando a eficácia dos procedimentos e tempos de resposta.

### **Plano de Contingência 5: Implementação dos Controles ISO 27001:**

**FUNCIONALIDADE:** Implementação dos Controles ISO 27001

**1. OBJETIVO:** Garantir a continuidade das operações críticas relacionadas à gestão da segurança da informação, conforme requisitos da ISO/IEC 27001, minimizando impactos de incidentes, falhas técnicas ou ataques cibernéticos e assegurando a confidencialidade, integridade e disponibilidade dos dados.

**2. ESCOPO E ABRANGÊNCIA:** Este plano aplica-se a qualquer incidente que afete a segurança da informação da plataforma, incluindo falhas em controles de segurança, sistemas, infraestrutura e processos relacionados à ISO 27001.

**3. CENÁRIOS DE RISCO COBERTOS**

* **Falhas tecnológicas:** indisponibilidade de servidores, banco de dados, rede ou firewalls.
* **Ataques cibernéticos:** ransonware, DDoS, phishing, SQL injection ou malware.
* **Acessos não autorizados:** violação de credenciais, elevação de privilégios.
* **Vazamento de dados:** exposição de informações críticas/confidenciais.
* **Erros humanos:** configurações incorretas, exclusões acidentais ou falhas operacionais.
* **Parada operacional:** indisponibilidade por manutenção não planejada, energia ou falha em nuvem.

**4. GATILHOS PARA ATIVAÇÃO DO PLANO**

* Interrupção de sistemas críticos por mais de 5 minutos.
* Identificação de incidente de segurança com risco à integridade/confidencialidade da informação.
* Falha em controles essenciais exigidos pela ISO 27001.
* Tentativa de ataque confirmada (via SIEM, IDS/IPS ou SOC).
* Solicitação formal da equipe de segurança da informação ou do gestor responsável.

**5. PAPÉIS E RESPONSABILIDADES**

* **Ativar plano de contingência:**
  + **Responsável:** Equipe de segurança ou Gestor responsável
* **Comunicação interna:**
  + **Responsável:** Equipe de TI, Segurança da Informação, Gestores de Área
* **Comunicação externa (se aplicável):**
  + **Responsável:** Gestor responsável
* **Execução das ações técnicas:**
  + **Responsável:** Equipe de segurança, Equipe de TI

**6. AÇÕES IMEDIATAS (CHECKLIST 0-15 MINUTOS)**

* **Passo 1 (0–5 min):**
  + **Ação:** Acionar equipe de segurança e gestores responsáveis.
  + **Responsável:** Equipe de Segurança.
* **Passo 2 (0–5 min):**
  + **Ação:** Isolar o sistema afetado (rede, máquina virtual, conta de usuário).
  + **Responsável:** Equipe de TI.
* **Passo 3 (5–10 min):**
  + **Ação:** Analisar logs e eventos em SIEM para identificar o incidente.
  + **Responsável:** Equipe de Segurança.
* **Passo 4 (5–10 min):**
  + **Ação:** Avaliar impacto (confidencialidade, integridade, disponibilidade).
  + **Responsável:** Equipe de Segurança.
* **Passo 5 (10–15 min):**
  + **Ação:** Decidir se ativa Plano B (assíncrono) ou Plano C (bypass).
  + **Responsável:** Gestor responsável.
* **Passo 6 (10–15 min):**
  + **Ação:** Documentar todas as ações no registro de incidentes.
  + **Responsável:** Equipe de Segurança.

**7. ESTRATÉGIAS DE CONTINGÊNCIA**

**PLANO B: MODO DE PROCESSAMENTO ASSÍNCRONO (TOLERÂNCIA À LATÊNCIA)**

* **Descrição:** Utiliza sistemas secundários para garantir a continuidade com possível lentidão.
* **Ação Técnica:** Redirecionar dados críticos para filas assíncronas. Ativar servidores redundantes ou serviços em nuvem de backup.
* **Ação Operacional:** Comunicar usuários sobre possível lentidão temporária. Garantir que todos os logs continuem sendo armazenados para auditoria.

**PLANO C: MODO DE BYPASS (DESATIVAÇÃO TEMPORÁRIA)**

* **Descrição:** Desativa controles não essenciais para manter a operação mínima segura.
* **Ação Técnica:** Desativar temporariamente controles de auditoria em tempo real ou autenticações adicionais. Ativar mecanismos mínimos de segurança (firewall, ACLs, segmentação de rede).
* **Ação Operacional:** Formalizar justificativa do bypass para compliance. Reprocessar logs e reativar controles após normalização.

**8. PLANO DE COMUNICAÇÃO**

* **Público: Interno (TI, Segurança, Gestores)**
  + **Canal:** Telefone, E-mail, Canal de incidentes (Teams/Slack)
  + **Frequência:** Relatórios de status a cada 30 minutos
* **Público: Externo (se aplicável)**
  + **Canal:** A definir
  + **Frequência:** Conforme necessidade
* **Público: Usuários finais**
  + **Canal:** E-mail, Intranet, Alerta no sistema
  + **Frequência:** Comunicado inicial e de resolução

**9. PROCESSO DE RETORNO À NORMALIDADE**

1. **Validação da Correção:** Validar restauração de sistemas com testes de integridade.
2. **Ativação Gradual:** Reativar controles de segurança desativados no Plano C.
3. **Sincronização:** Sincronizar logs de auditoria e validar consistência dos dados.
4. **Monitoramento Contínuo:** Confirmar estabilidade antes de liberar uso para todos os usuários.
5. **Comunicação de Encerramento:** Encerrar incidente formalmente no sistema de gestão.

**10. PÓS-INCIDENTE**

* Análise de causa raiz (RCA) para identificar vulnerabilidades ou falhas.
* Gerar relatório final (impacto, ações, tempo de resposta, custo, lições).
* Revisar e atualizar políticas, plano de contingência e procedimentos.
* Realizar treinamento da equipe para evitar reincidência.
* Executar auditoria interna para validar aderência às normas ISO 27001.

1. **TESTES E SIMULAÇÕES:**

O plano deverá ser testado semestralmente através de simulações de falhas controladas para validar a eficácia dos procedimentos e tempos de resposta.

### **Plano de Contingência 6: Dashboard em Tempo Real de Métricas da Equipe:**

**FUNCIONALIDADE:** Dashboard em tempo real de métricas da equipe

**1. OBJETIVO:** Garantir que o gestor tenha acesso a informações de desempenho da equipe, mesmo em caso de falhas no dashboard em tempo real.

**2. ESCOPO E ABRANGÊNCIA** Este plano cobre falhas no acesso, na atualização e na integridade dos dados exibidos no dashboard de métricas.

**3. CENÁRIOS DE RISCO COBERTOS**

* Indisponibilidade total do dashboard
* Lentidão excessiva na atualização
* Dados incorretos ou defasados
* Falha de integração com sistemas de origem
* Problemas de segurança ou acessos não autorizados

**4. GATILHOS PARA ATIVAÇÃO DO PLANO**

* **Monitoramento:** Dashboard fora do ar por mais de 5 minutos ou erros acima de 10% nas consultas.
* **Relatos de Usuários:** Múltiplos gestores relatam divergência de dados.
* **Notificação Externa:** Notificação do provedor ou da infraestrutura sobre uma falha.

**5. PAPÉIS E RESPONSABILIDADES**

* **Coordenação técnica do incidente:**
  + **Responsável:** Líder Técnico de TI
* **Validação das métricas e dados:**
  + **Responsável:** Equipe de Dados
* **Comunicação com gestores e stakeholders:**
  + **Responsável:** Gerente de Produto
* **Execução das ações técnicas:**
  + **Responsável:** Equipe técnica

**6. AÇÕES IMEDIATAS (CHECKLIST 0-15 MINUTOS)**

* **Passo 1:**
  + **Ação:** Verificar a extensão da falha (identificar sistemas/serviços afetados).
  + **Responsável:** Equipe técnica.
* **Passo 2:**
  + **Ação:** Notificar gestores sobre o incidente via alerta imediato.
  + **Responsável:** Coordenador de TI.
* **Passo 3:**
  + **Ação:** Decidir e ativar o plano de contingência adequado (B ou C).
  + **Responsável:** Líder Técnico de TI.
* **Passo 4:**
  + **Ação:** Acionar equipe técnica para investigação e iniciar diagnóstico.
  + **Responsável:** Equipe técnica.

**7. ESTRATÉGIAS DE CONTINGÊNCIA**

**PLANO B: MODO DE ATUALIZAÇÃO PERIÓDICA**

* **Descrição:** Plano preferencial para cenários de lentidão ou falhas parciais.
* **Ação Técnica:** Alterar a configuração do sistema para ativar a atualização periódica (ex.: a cada 15 minutos) em vez de tempo real.
* **Ação Operacional:** Comunicar aos gestores sobre o atraso temporário na visualização dos dados.

**PLANO C: RELATÓRIOS ALTERNATIVOS**

* **Descrição:** Utilizado em caso de indisponibilidade total do dashboard.
* **Ação Técnica:** Equipe de dados gera relatórios estáticos em PDF/Excel a partir do banco de dados.
* **Ação Operacional:** Distribuir os relatórios para os gestores em intervalos de tempo definidos (ex: a cada hora) até o restabelecimento do sistema.

**8. PLANO DE COMUNICAÇÃO**

* **Público: Equipe técnica**
  + **Canal:** canais internos (Slack/Teams)
  + **Frequência:** tempo real
* **Público: Gestores**
  + **Canal:** e-mail
  + **Frequência:** a cada 60 minutos com status
* **Público: Fornecedor**
  + **Canal:** contato conforme necessidade
  + **Frequência:** conforme necessidade

**9. PROCESSO DE RETORNO À NORMALIDADE**

1. **Validação da Correção:** A equipe técnica válida a correção em um ambiente de teste.
2. **Ativação Gradual:** A atualização em tempo real é reativada gradualmente.
3. **Monitoramento Contínuo:** A equipe de dados confirma a consistência dos dados exibidos.
4. **Comunicação de Encerramento:** O Gerente de Produto comunica o encerramento do incidente aos gestores.

**10. PÓS-INCIDENTE**

* Realizar reunião de post-mortem em até 48 horas.
* Analisar e documentar a causa raiz da falha.
* Avaliar a eficácia do plano de contingência executado.
* Identificar e registrar ações de melhoria no sistema e no próprio plano.

1. **TESTES E SIMULAÇÕES:**

O plano deverá ser testado semestralmente através de simulações de falhas controladas para validar a eficácia dos procedimentos e tempos de resposta.

### **Plano de Contingência 7: Painel do Gestor - Criação e Designação de Tarefas/Desafios:**

**FUNCIONALIDADE:** Painel do Gestor- Criação e Designação de Tarefas/Desafios

**1. OBJETIVO:** Assegurar que os gestores consigam manter o engajamento e o acompanhamento da equipe, mesmo diante de uma falha parcial ou total na funcionalidade de criação/atribuição de missões no painel.

**2. ESCOPO E ABRANGÊNCIA:** Este plano cobre todas as falhas relacionadas à criação, designação, salvamento, sincronização e visualização de missões e desafios no painel do gestor.

**3. CENÁRIOS DE RISCO COBERTOS:**

* **Falha Total:** O painel não possibilita a criação ou designação de missões.
* **Falha Parcial:** O gestor consegue criar uma missão, mas não a atribuir ou salvá-la corretamente.
* **Falha de Sincronização:** As missões criadas não são exibidas para os operadores ou são exibidas em duplicidade.
* **Falha de Interface:** O backend registra a missão, porém o gestor não consegue vê-la no painel.

**4. GATILHOS PARA ATIVAÇÃO DO PLANO**

* **Alerta de Monitoramento:** Aviso do sistema apontando um erro crítico na API de "Missões/Desafios".
* **Relatos de Múltiplos Usuários:** Dois ou mais gestores relatando erro simultâneo na ferramenta.
* **Inconsistência de Dados:** Identificação de inconsistências como missões desaparecendo, duplicadas ou não sendo atribuídas.

**5. PAPÉIS E RESPONSABILIDADES**

* **Validar falha e notificar partes interessadas:**
  + **Responsável:** Supervisor de Operações
* **Iniciar investigação técnica:**
  + **Responsável:** Líder Técnico de TI
* **Executar ações de contingência operacional:**
  + **Responsável:** Gestores / Equipe de Operações
* **Executar ações de contingência técnica:**
  + **Responsável:** Equipe Técnica

**6. AÇÕES IMEDIATAS (CHECKLIST 0-15 MINUTOS)**

* **Passo 1:**
  + **Ação:** Validar se a falha é geral ou isolada.
  + **Responsável:** Supervisor de Operações.
* **Passo 2:**
  + **Ação:** Notificar equipe técnica e gerência.
  + **Responsável:** Supervisor de Operações.
* **Passo 3:**
  + **Ação:** Comunicar gestores que será acionado o modo de contingência.
  + **Responsável:** Supervisor de Operações.
* **Passo 4:**
  + **Ação:** Iniciar investigação técnica paralela.
  + **Responsável:** Líder Técnico de TI.

**7. ESTRATÉGIAS DE CONTINGÊNCIA**

**PLANO B: REGISTRO MANUAL TEMPORÁRIO**

* **Descrição:** Plano preferencial para manter o registro e o acompanhamento das missões fora do sistema.
* **Ação Técnica:** Exportar registros e disponibilizar uma planilha provisória para monitoramento das missões.
* **Ação Operacional:** Gestores criam ou designam tarefas por meio de um formulário interno (Google Forms, Excel online etc.), que é transmitido manual aos operadores.

**PLANO C: COMUNICAÇÃO DIRETA (ÚLTIMO RECURSO)**

* **Descrição:** Utilizado em caso de falha total e impossibilidade de usar o Plano B.
* **Ação Técnica:** Desativar temporariamente o módulo de missões.
* **Ação Operacional:** Gestores comunicam as missões por canais alternativos (e-mail, Teams, Slack, Trello). Os operadores atualizam seu progresso manualmente.

**8. PLANO DE COMUNICAÇÃO**

* **Público: Equipe de Operações**
  + **Canal:** Chat em grupo / verbal
  + **Frequência:** Imediato
* **Público: Gestores e Stakeholders**
  + **Canal:** E-mail
  + **Frequência:** A cada 60 min.
* **Público: Equipe Técnica**
  + **Canal:** Canal dedicado (Slack/Teams)
  + **Frequência:** Tempo real

**9. PROCESSO DE RETORNO À NORMALIDADE**

1. **Validação da Correção:** Confirmar a precisão da correção em um ambiente de testes.
2. **Ativação Gradual:** Reativar o módulo de missões de forma gradual (teste com um gestor).
3. **Reativação Total:** Após a confirmação de estabilidade, expandir para todos.
4. **Comunicação de Encerramento:** Informar sobre a finalização do incidente.

**10. PÓS-INCIDENTE**

* Executar post-mortem no prazo de 48 horas.
* Analisar registros de erros e verificar a consistência dos dados.
* Analisar a eficácia do plano e atualizar o documento.

1. **TESTES E SIMULAÇÕES:**

O plano deverá ser testado semestralmente através de simulações de falhas controladas para validar a eficácia dos procedimentos e tempos de resposta.

### **Plano de Contingência 8: Latência na Entrega de Chamadas da Fila Inteligente:**

**FUNCIONALIDADE:** Fila Inteligente – Tempo entre chamadas

**1. OBJETIVO:** Garantir a continuidade e a eficiência da operação, assegurando que o tempo entre o fim de uma chamada e a entrega da próxima na "Fila Inteligente" não exceda o limite de 10 segundos, minimizando o tempo ocioso dos operadores e o impacto no cliente final.

**2. ESCOPO E ABRANGÊNCIA:** Este plano cobre todas as falhas técnicas e de performance que resultem em latência excessiva no sistema de distribuição de chamadas. Ele abrange desde a infraestrutura de nuvem e serviços de backend até a lógica de roteamento que afeta diretamente o tempo de entrega das chamadas aos operadores.

**3. CENÁRIOS DE RISCO COBERTOS:**

* **Falha Total:** A Fila Inteligente para completamente de entregar chamadas aos operadores.
* **Latência Excessiva:** O tempo de entrega entre chamadas ultrapassa consistentemente o limite de 10 segundos.
* **Sobrecarga de Infraestrutura:** O volume de tráfego excede a capacidade de processamento dos servidores, gerando atrasos.
* **Falhas de Backend ou Banco de Dados:** Problemas na lógica de negócio, consultas ou serviços que afetam a distribuição das chamadas.
* **Indisponibilidade Parcial:** Falhas em APIs externas ou serviços de nuvem que impactam o roteamento.

**4. GATILHOS PARA ATIVAÇÃO DO PLANO:**

* **Alerta de Monitoramento:** Recebimento de um alerta crítico indicando que a latência da fila ultrapassou o limite de 10 segundos por mais de 2 minutos.
* **Relatos de Múltiplos Operadores:** Confirmação de que 3 ou mais operadores estão relatando atraso excessivo na recepção de chamadas.
* **Queda de KPIs em Tempo Real:** Detecção de uma queda abrupta em indicadores chave como "Taxa de Ocupação dos Operadores".

**5. PAPÉIS E RESPONSABILIDADES:**

* **Ativar plano de contingência:**
  + **Responsável:** Supervisor de Operações ou Líder Técnico de TI
* **Validar falha e notificar gerência:**
  + **Responsável:** Supervisor de Operações
* **Anunciar modo de contingência à equipe:**
  + **Responsável:** Supervisor de Operações
* **Iniciar investigação da causa raiz:**
  + **Responsável:** Líder Técnico de TI / Equipe DevOps

**6. AÇÕES IMEDIATAS (CHECKLIST 0-15 MINUTOS)**

* **Passo 1:**
  + **Ação:** Validar a extensão da falha (se é geral ou isolada) com base nos relatos e dashboards.
  + **Responsável:** Supervisor de Operações.
* **Passo 2:**
  + **Ação:** Notificar o Líder Técnico de TI e a Gerência de Operações, declarando o início do incidente.
  + **Responsável:** Supervisor de Operações.
* **Passo 3:**
  + **Ação:** Verificar o status dos servidores, logs e tempo de resposta de APIs para identificar gargalos ou falhas.
  + **Responsável:** Equipe Técnica (Backend/DevOps).
* **Passo 4:**
  + **Ação:** Anunciar à equipe de atendimento a ativação do "Modo de Contingência" e o plano a ser seguido (B ou C).
  + **Responsável:** Supervisor de Operações.

**7. ESTRATÉGIAS DE CONTINGÊNCIA**

#### **PLANO B: MODO SIMPLIFICADO (PLANO PREFERENCIAL)**

* **Descrição:** A camada de "inteligência" da fila é parcialmente desativada, e o sistema passa a rotear chamadas usando uma lógica mais simples, focada apenas na disponibilidade dos operadores.
* **Ação Técnica:** Alterar a configuração do backend para ativar a lógica simplificada de roteamento.
* **Ação Operacional:** Instruir os operadores a classificar manualmente as chamadas inválidas (robôs etc.) e encerrá-las rapidamente.

#### **PLANO C: ROTEAMENTO MANUAL (ÚLTIMO RECURSO)**

* **Descrição:** Utilizado em caso de falha crítica e generalizada do sistema de filas.
* **Ação Técnica:** Reconfigurar o sistema para redirecionar as chamadas para um grupo de supervisores ou ramais predefinidos.
* **Ação Operacional:** Os supervisores recebem as chamadas e as redistribuem manualmente para os operadores disponíveis.

**8. PLANO DE COMUNICAÇÃO**

**Público:** Equipe de Operações

**Canal:** Chat interno / Verbal

**Frequência:** Imediata e conforme necessário

**Responsável:** Supervisor de Operações

**9. PROCESSO DE RETORNO À NORMALIDADE**

1. **Validação da Correção:** A equipe de TI corrige a falha e a válida em um ambiente de homologação com simulação de carga.
2. **Ativação Gradual (Canary Release):** A Fila Inteligente é reativada para um pequeno grupo de operadores "piloto" para monitoramento de estabilidade.
3. **Monitoramento Contínuo:** A equipe confirma que o tempo médio entre chamadas retornou ao limite de 10 segundos.
4. **Comunicação de Encerramento:** O Supervisor de Operações comunica formalmente o fim do incidente a todos os envolvidos.

**10. PÓS-INCIDENTE**

* Realizar reunião de *post-mortem* em até 48 horas para identificar a causa raiz da falha.
* Avaliar a eficácia do plano de contingência executado e identificar pontos de melhoria.
* Documentar e priorizar melhorias técnicas ou operacionais para prevenir novas ocorrências.

**11. TESTES E SIMULAÇÕES:**

O plano deverá ser testado semestralmente através de simulações de falhas controladas para validar a eficácia dos procedimentos e tempos de resposta.