PREFEITURA
ARAÇOIABA DA SERRA

PLANO DE CONTINUIDADE DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

Divisão de Tecnologia da Informação
www.aracoiaba.sp.gov.br
Av. Luane Milanda de Oliveira, 600, Jardim Salete, Araçoiaba da Serra/SP | CEP 18.190-000

Prefeito Municipal
José Carlos de Quevedo Júnior

Secretário de Governo
Jair Ferreira Duarte Neto

Secretária de Administração e Finanças
Wilma Aparecida de Cristo

Comitê Municipal de Tecnologia da Informação
Elidam Palugan dos Santos – Gerente de TI
Candemar Aparecido Pontarollo – Técnico em Informática
André Navarro – Advogado Público
Tiago Vieira Mesquita – Gerente de Compras da SME
Daila Maria Miranda – Diretora de Finanças

gov.br
Documento assinado digitalmente
ELIDAM PALUGAN DOS SANTOS
Data: 12/12/2024 14:43:17-0300
Verifique em https://validar.iti.gov.br

Versão	Data	Descrição	Responsável
1.0	12/12/2024	Elaboração de versão inicial	Elidam Palugan dos Santos

Índice

1. Apresentação

As falhas nos serviços de Tecnologia da Informação (TI) têm impactos significativos e diretos na prestação de serviços públicos à população. A dependência crescente de recursos tecnológicos em diversas atividades realizadas pela Prefeitura, através das suas unidades administrativas distribuídas por todo o município, torna a continuidade dos serviços de TI uma prioridade inadiável.

2. Objetivo

Plano de Continuidade de Serviços de Tecnologia da Informação é um documento fundamental que delineia as estratégias necessárias para assegurar a continuidade das operações dos serviços essenciais de TI, considerados críticos para a organização. Este plano tem como objetivo principal garantir que, em situações de interrupção ou desastre, os serviços possam ser rapidamente restaurados e mantidos, minimizando impactos negativos nas atividades da Prefeitura. O documento abrange a elaboração de planos de contingência, continuidade e recuperação.

3. Serviços Essenciais

Os serviços essenciais de Tecnologia da Informação (TI) são aqueles que desempenham um papel fundamental nos processos administrativos da Prefeitura Municipal de Araçoiaba da Serra, garantindo uma resposta eficaz às demandas dos munícipes. A indisponibilidade desses serviços pode impactar significativamente a capacidade da administração em fornecer serviços públicos, resultando em consequências que podem ser de natureza financeira, legal, reputacional ou operacional.

Após uma análise minuciosa realizada pelo Departamento de Tecnologia da

Informação, identificamos os seguintes serviços como essenciais para a continuidade das operações da administração municipal de Araçoiaba da Serra:

Serviço	Criticidade[1]	RPO[2]	RTO[3]	IMPACTO[4]			
				FINANCEIRO	LEGAL	IMAGEM	OPERACIONAL
Servidor de Arquivos	Alta	24h	24h	Indefinido	Médio	Médio	Médio
Servidor Web	Alta	12h	12h	Indefinido	Alto	Alto	Alto
Servidor de Dados	Alta	12h	12h	Indefinido	Alto	Alto	Alto
Link Principal	Alta	8h	4h	Indefinido	Alto	Alto	Alto
Sistema Integrado de Contabilidade Pública	Alta	12h	12h	Indefinido	Alto	Médio	Alto
Sistema Integrado de Arrecadação e Tributos	Alta	12h	12h	Indefinido	Alto	Alto	Alto
Sistema Integrado de Folha de Pagamento	Alta	12h	12h	Indefinido	Alto	Médio	Alto
Sistema de Ponto Eletrônico	Média	24h	24h	Indefinido	Médio	Médio	Médio
Sistema Integrado de Saúde	Alta	12h	6h	Indefinido	Alto	Alto	Alto
Sistema Integrado de Educação	Média	24h	24h	Indefinido	Médio	Médio	Médio
Sistema de Processos Digitais	Alta	24h	24h	Indefinido	Alto	Alto	Alto
Sistema de Geoprocessamento	Média	48h	48h	Indefinido	Médio	Médio	Médio
Nota Fiscal Eletrônica	Alta	12h	6h	Indefinido	Alto	Alto	Alto
Portal da Trânsparência	Alta	12h	12h	Indefinido	Alto	Alto	Médio
Sistema do Terceiro Setor	Baixa	48h	48h	Indefinido	Médio	Médio	Médio
Site Oficial	Alta	12h	6h	Indefinido	Médio	Alto	Médio
Imprensa Oficial	Média	24h	24h	Indefinido	Médio	Médio	Médio
E-mail Coorporativo	Média	24h	12h	Indefinido	Médio	Médio	Médio
Sistema de Backup	Baixa	48h	24h	Indefinido	Alto	Médio	Alto
Rede Cidades Digitais	Média	24h	24h	Indefinido	Baixo	Baixo	Médio
VPN	Alta	12h	12h	Indefinido	Baixo	Baixo	Médio
Internet – Setores externos	Média	24h	12h	Indefinido	Médio	Alto	Médio

[1] – Alto, Médio, Baixo, Indefinido.

[2] – Recovery Point Objective: Método de controle utilizado em tecnologia de informação para calcular e/ ou estimar a quantidade limite de dados que uma organização toleraria perder em casos de incidentes.

[3] – Recovery Time Objective: Diretamente relacionado ao tempo máximo que o setor de tecnologia levará para restabelecer os serviços após a parada crítica, devendo ser levado em consideração o tempo de recuperação, testes, reparos, atualizações, reinstalações, etc.

[4] – Alto, Médio, Baixo, Indefinido.

4. Principais Ameaças

Os ambientes de Tecnologia da Informação da Prefeitura Municipal de Araçoiaba da Serra estão expostos a uma variedade de ameaças que podem comprometer a disponibilidade e a integridade dos serviços essenciais. A identificação e análise dessas ameaças são fundamentais para o desenvolvimento de um robusto Plano de Continuidade de Serviços de TI. As principais ameaças mapeadas e descritas a seguir necessitam de atenção especial e estratégias de mitigação adequadas.

4.1 *Interrupção de Energia Elétrica*

A interrupção no fornecimento de energia elétrica pode ocorrer devido a fatores externos, como falhas na rede da concessionária, rompimento de cabos durante obras públicas, desastres naturais ou acidentes. Além disso, fatores internos, como um padrão elétrico insuficiente, curto-circuitos, infiltrações ou avarias nos equipamentos da rede elétrica interna da Prefeitura, podem resultar em interrupções. A falta de energia pode levar a paradas inesperadas nos serviços de TI, afetando diretamente a eficiência administrativa e a prestação de serviços ao cidadão.

4.2 *Ataques Cibernéticos*

Os ataques cibernéticos são uma ameaça crescente que pode comprometer a segurança da rede pública municipal. Esses ataques podem afetar computadores, servidores locais e na nuvem, além da rede de dados. Tais incidentes incluem malware, ransomware e tentativas de invasão que visam roubar informações sensíveis ou causar danos aos sistemas. A proteção contra esses ataques é vital para garantir a confidencialidade, integridade e disponibilidade das informações da Prefeitura.

4.3 *Falha na Climatização da Sala de Servidores*

O funcionamento adequado da sala de servidores é crítico para a proteção dos ativos de TI. O superaquecimento pode ocorrer devido a falhas no sistema de climatização, que conta com dois aparelhos de ar-condicionado em regime de redundância. A falta de refrigeração adequada pode causar danos permanentes aos equipamentos, resultando em interrupções prolongadas dos serviços e perda de dados.

4.4 *Falha Humana*

As falhas humanas constituem um risco significativo no ambiente de TI. Acidentes ao manusear equipamentos críticos, erros no processamento de dados e manuseio inadequado de servidores são exemplos de como a ação humana pode impactar negativamente a operação. Esses incidentes podem levar à perda de dados, interrupções nos serviços e até mesmo compromissos legais.

4.5 *Ataques Internos*

Os ataques internos, que podem ser maliciosos ou acidentais, representam uma ameaça considerável à segurança dos ativos da Prefeitura. Funcionários com acesso a sistemas sensíveis podem, intencionalmente ou inadvertidamente, comprometer a integridade do Data Center, computadores, servidores de arquivos e sistemas de rede de dados. A conscientização e o treinamento contínuo são essenciais para mitigar esses riscos.

4.6 *Incêndios*

Incêndios constituem uma ameaça real e potencialmente devastadora para a infraestrutura de TI. Eles podem ocasionar danos parciais ou totais aos sistemas de Tecnologia da Informação e Comunicação da Prefeitura. A implementação de medidas preventivas, como sistemas de detecção e combate a incêndios, é crucial para proteger os ativos e garantir a continuidade das operações.

4.7 *Desastres Naturais*

Desastres naturais, como tempestades, alagamentos e outros eventos fortuitos, podem causar interrupções significativas nos serviços de TI. Esses eventos podem danificar equipamentos, interromper o fornecimento de energia e afetar a infraestrutura de redes. O planejamento para a resposta a desastres naturais é essencial para garantir a resiliência dos serviços.

4.8 *Falha de Hardware*

Falhas de hardware em equipamentos essenciais podem ocorrer, exigindo a reposição de peças, reparos ou, em casos críticos, a substituição completa do equipamento. Este processo frequentemente requer licitação, o que pode atrasar a recuperação dos serviços afetados. A manutenção preventiva e a atualização dos equipamentos são estratégias importantes para minimizar esses riscos.

5. Papeis e Responsabilidades

5.1 *Comitê Municipal de Tecnologia da Informação*

O Comitê Municipal de Tecnologia da Informação (CMTI) desempenha um papel fundamental na gestão de crises relacionadas à Tecnologia da Informação (TI) dentro do município. A seguir, destacam-se suas responsabilidades e estrutura:

a) Avaliação do Plano de Continuidade de TI:

O CMTI é responsável por realizar revisões periódicas do plano de continuidade de TI, garantindo que este permaneça eficaz e alinhado às necessidades atuais da administração municipal.

b) Acionamento do Plano:

O comitê tem a autoridade para decidir sobre a ativação do plano em situações de desastres, assegurando uma resposta rápida e coordenada para mitigar impactos.

c) Comunicação:

O CMTI gerencia toda a comunicação durante eventos de desastre, direcionando informações a:

- Funcionários municipais
- Munícipes
- Autoridades competentes
- Fornecedores, conforme necessário

d) Estrutura do CMTI:

O CMTI, instituido pelo Decreto Municipal nº 2.588/2022, composto por uma equipe multidisciplinar, presidido pelo Gerente de Tecnologia da Informação, membros descritos a seguir:

- **Elidam Palugan dos Santos** – Gerente de Tecnologia da Informação
- **Candemar Aparecido Pontarollo** – Técnico em Informática
- **André Navarro** – Advogado Público
- **Tiago Vieira Mesquita** – Gerente de Compras
- **Daila Maria Miranda** – Diretora de Finanças

5.2 *Equipe Técnica*

A equipe técnica da Prefeitura de Araçoiaba da Serra desempenha um papel essencial na gestão das instalações físicas que suportam os sistemas de Tecnologia da Informação (TI). Assegurando que as estruturas de substituição sejam mantidas em condições adequadas, suas principais responsabilidades incluem:

- Gerenciamento das instalações físicas
- Avaliação dos danos
- Infraestrutura dos servidores
- Validação de desempenho
- Fornecimento de ferramentas
- Análise de perdas e recuperação

ACIONAMENTO DE CONTATOS			
Área	**Responsável**	**Telefone**	**Contato**
Infraestrutura	Elidam Palugan dos Santos **Gerente de TI**	(15) 3281-7036	suporte@aracoiaba.sp.gov.br elidam@aracoiaba.sp.gov.br candemar@aracoiaba.sp.gov.br
Redes			
Aplicações			
Segurança da Informação			
Operações			
Backup			

5.3 *Invocação do Plano*

O plano de continuidade de serviços de TI da Prefeitura de Araçoiaba da Serra será acionado em resposta a qualquer ocorrência relacionada a cenários de desastres, riscos desconhecidos ou vulnerabilidades que apresentem potencial de exploração. Este plano não apenas se destina a situações de emergência, mas também poderá ser utilizado para a realização de testes que visem validar os processos envolvidos, assegurando que as estratégias estejam efetivas e prontas para implementação em situações reais.

Os membros da equipe técnica terão a responsabilidade de acionar os contatos e partes interessadas, priorizando a comunicação através de telefone ou, sempre que possível, de forma pessoal. Essa abordagem garantirá uma comunicação rápida e eficaz, essencial para a gestão de crises e para a continuidade das operações da Prefeitura, minimizando os impactos sobre os serviços essenciais prestados à comunidade.

A estrutura do plano assegura que todos os procedimentos estejam claramente definidos e que a equipe técnica esteja devidamente preparada para atuar de maneira coordenada, garantindo a resiliência dos serviços de TI em momentos críticos.

5.4 *Macroprocessos do Plano*

A execução do plano de continuidade de serviços de TI da Prefeitura de Araçoiaba da Serra é baseada nos seguintes macroprocessos, que se desdobram em planos específicos para cada área de atuação:

↓	Identificação de Ocorrência de Desastre
↓	Iniciar Plano de Continuidade
↓	Acionar Solução de Contingência
↓	Reestabelecer Serviços de TI
↓	Reparar o Ambiente de Desastre
↓	Reestabelecer Operação Normal

6. Estratégias do Plano de Continuidade de Serviços de TI

Com base nos ativos atuais à disposição da Divisão de Tecnologia da Informação serão utilizadas as estratégias de redundância e recuperação conforme apresentadas a seguir:

6.1 *Backup*

Definição de uma política de backup da Prefeitura de Araçoiaba da Serra, sendo o mínimo aceitável: completo com arranjos incrementais bem como a criação de snapshots para emergências. Política de backup essa publicada no portal oficial do município.

6.2 *Redundância de Links*

A Prefeitura de Araçoiaba da Serra conta com redundância de links de Internet em seu Data Center. Isso significa que há links de segmentos de rede distintos que chegam ao local por caminhos separados, visando evitar interrupções em caso de rompimento acidental de cabos. Essa estratégia de redundância é crucial para garantir a continuidade dos serviços e a estabilidade das operações, minimizando o risco de downtime e assegurando que os serviços essenciais permaneçam disponíveis para a comunidade.

6.3 *Redundância de Discos*

Atualmente, a Prefeitura de Araçoiaba da Serra opera com um sistema de armazenamento que combina discos físicos e virtuais, garantindo a segurança e a continuidade dos serviços de TI. Os servidores de aplicação utilizam a tecnologia RAID 1, que proporciona redundância de discos. Essa configuração permite a criação de cópias em tempo real em discos de dados distintos, assegurando que, em caso de falha de um disco, não haja perda de dados nem interrupção dos serviços. Com essa abordagem, que abrange tanto discos físicos quanto virtuais, a Prefeitura garante a integridade das informações e a continuidade das operações, mesmo diante de falhas inesperadas.

6.4 *Ações de Contingência / Recuperação*

Identificação da perda de dados e ativos, recuperação de toda a infraestrutura afetada e, após restabelecer o ambiente principal, execução da recuperação dos dados a partir dos backups. As ações de contingência e recuperação são descritas a

seguir.

6.5 *Plano de Continuidade Operacional*

Este plano estabelece os cenários de inoperância e os procedimentos alternativos planejados, delineando as atividades prioritárias necessárias para assegurar a continuidade dos serviços essenciais. O objetivo central é viabilizar ações de continuidade durante e após a ocorrência de uma crise ou cenário de desastre, concentrando-se nas medidas de contingência definidas na estratégia de Continuidade Operacional (PCO). Os objetivos do PCO incluem:

Manutenção da Operação dos Serviços Críticos: Prover mecanismos que garantam o funcionamento ininterrupto dos serviços essenciais e das operações dos sistemas críticos.

Estabelecimento de Procedimentos Alternativos: Definir protocolos, controles e diretrizes que possibilitem a continuidade operacional em situações de crise ou desastre.

Definição da Documentação Necessária: Elaborar formulários, checklists e relatórios que devem ser preenchidos pelas equipes durante a execução das ações de contingência, assegurando a rastreabilidade e a conformidade.

Minimização de Impactos: Reduzir os transtornos associados às consequências de um incidente, estimulando a colaboração entre as equipes para a superação da crise.

Orientação a Servidores e Partes Interessadas: Fornecer informações claras e procedimentos detalhados sobre as condutas a serem adotadas durante a crise.

Execução do Plano

Avaliação de Impacto de Desastre: Na identificação de um incidente ou crise, o responsável deve conduzir uma análise de impacto, avaliando a extensão do dano, os riscos associados e os possíveis desdobramentos do evento, utilizando metodologias de análise de impacto nos negócios (BIA).

Acionamento do Plano: Deve ser convocada uma reunião de emergência para

coordenar as ações de contingência, estabelecer prazos e orquestrar as atividades necessárias. Nesta reunião, serão informados todos os envolvidos sobre as medidas a serem implementadas, priorizando os serviços críticos e assegurando a comunicação eficaz.

Contingência de Backup: As seguintes ações de contingência e continuidade devem ser adotadas para cada processo ou serviço essencial, de acordo com as melhores práticas de gestão de continuidade de negócios:

Implementação de estratégias de backup e recuperação de dados.

Estabelecimento de redundâncias em infraestrutura crítica.

Execução de testes de recuperação para validar os procedimentos.

Essas diretrizes são fundamentais para garantir que a Prefeitura de Araçoiaba da Serra esteja preparada para responder de forma eficaz a qualquer evento adverso, assegurando a continuidade dos serviços públicos e a proteção das informações.

Encerramento do PCO: Formalizar documentalmente todas as atividades executadas e dar publicidade para conhecimento de todos.

6.6 *Plano de Administração de Desastre*

Este plano estabelece as ações necessárias para a gestão de cenários de desastres, visando a mitigação, administração e neutralização dos impactos associados ao relacionamento entre os agentes envolvidos e/ou afetados. O objetivo é assegurar a superação da crise por meio de uma orquestração coordenada de ações e uma comunicação eficaz.

Execução do Plano

Comunicação na Ocorrência de um Desastre: Na eventualidade de um desastre, é fundamental estabelecer contato imediato com diversas áreas, especialmente aquelas diretamente afetadas, para informá-las sobre os impactos na continuidade dos serviços e as estimativas de tempo para a recuperação. A prioridade deve ser notificar os responsáveis pelas áreas impactadas, fornecendo informações detalhadas sobre a situação do desastre, os serviços afetados e a previsão para o

restabelecimento.

Quando um serviço impactado afeta usuários externos, a área responsável pela Comunicação deve ser acionada para providenciar a divulgação de uma nota informativa sobre a indisponibilidade do serviço ao público em geral. É essencial estabelecer um meio de contato específico para garantir que todas as unidades administrativas estejam cientes da ocorrência do desastre, da inatividade dos serviços essenciais de TI e das ações de contingência em andamento para a restauração das operações.

Encerramento do Plano

Após a validação do funcionamento dos sistemas essenciais e a estabilização dos servidores, os departamentos e demais partes interessadas mencionadas neste plano deverão ser contatados. Serão fornecidas informações detalhadas sobre o retorno das operações e dos serviços essenciais.

O Departamento de TI também deverá elaborar um relatório abrangente que inclua as atividades realizadas após a ocorrência do desastre, como o remanejamento dos canais de informação e a abertura e acompanhamento de chamados relacionados ao incidente. Este relatório servirá como documento de referência para futuras análises e melhorias nos processos de resposta a desastres.

6.7 *Plano de Recuperação de Desastre*

Este plano descreve os cenários de inoperância e seus respectivos procedimentos planejados, definindo as atividades prioritárias para restabelecer o nível de operação dos serviços no ambiente afetado, dentro de um prazo tolerável. São objetivos do Plano de Recuperação de Desastres:

- Avaliar danos aos ativos e conexões dos sistemas afetados e prover meios para sua recuperação operacional;
- Evitar desdobramento de outros incidentes na infraestrutura principal;
- Restabelecer os sistemas afetados dentro de um prazo aceitável por ordem de prioridade definida, se for o caso.

Execução do Plano

- Identificação de ativos danificados ou comprometidos: A equipe técnica deverá identificar e listar todos os ativos danificados da ocorrência do desastre.
- Identificação de acessos comprometidos: A equipe deverá identificar as interrupções de conexões e acessos gerados após o desastre, relatando se trata de um problema interno ou externo ao ambiente, bem como o fornecimento das informações quanto aos sistemas afetados em caso de terceiros.
- Listagem dos serviços descontinuados: A equipe técnica deverá mapear quais serviços foram descontinuados, contendo as informações de perda de ativo e de conexão, com intuito de documentar e corrigir os serviços. O relatório deverá abranger todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, firewall, storage, roteadores e switches, bem como respectivas configurações de proxy, DNS, rotas, VLANS, etc.
- Elaboração de cronograma de recuperação: Após o mapeamento das perdas e impactos, a equipe técnica elaborará um breve cronograma de recuperação de aplicações, levando em consideração:
    - A priorização dos serviços essenciais, ou determinação de nível institucional;
    - O RTO definido para cada serviço essencial;
    - A força de trabalho disponível.
- Substituição de ativos: Em caso de perda de ativos, deverá ser imediatamente informado a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. Deverá ser mensurado quanto tempo o processo licitatório irá impactar o RTO de cada serviço, comunicando os responsáveis se houver alguma solução alternativa a ser tomada enquanto é realizada a aquisição. Deverá ser analisado para os ativos danificados, as coberturas contratuais e/ ou garantias.
- Reconfiguração de ativos: A equipe deverá verificar que as configurações dos ativos reparados ou substituídos estão em pleno funcionamento. Caso não

estejam, deverá prover cronograma estimado para configurar estes ativos. Ambiente de testes: Deve ser elaborado um ambiente para testes de recuperação garantindo o pleno restabelecimento da aplicação/ serviços afetados pelo incidente e/ ou desastre ocorrido. Os testes incluem a garantia dos níveis de capacidade e disponibilidade dos serviços.

- Recuperação dos dados do backup: Proceder a recuperação dos dados para as aplicações afetadas. Validar as configurações e funcionalidades dos sistemas. A validação pode ser realizada pelos testes automatizados de monitoramento dos serviços ou por equipe designada.
- Encerramento do Plano de Recuperação de Desastres: Ao término do procedimento de recuperação, as informações serão consolidadas em parecer específico informando o horário de restabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

7. Processo de Revisão

O Plano de Continuidade dos Serviços de TI deverão ser revisados pelo Comitê Municipal de Tecnologia da Informação, em conjunto com a Divisão de Tecnologia da Informação sempre que necessário.

Deverá ser acompanhada dos fatores de risco e novas necessidades mapeadas, não dispensando a revisão para inserção de melhorias de estratégias na execução do plano.

8. Fatores Críticos para Execução do Plano de Continuidade dos Serviços de Tecnologia da Informação

São considerados fatores fundamentais para a execução das atividades previstas neste Plano:

- Acompanhamento dos riscos e necessidades pela Divisão de TI;

O envolvimento das Secretarias para sustentar as decisões necessárias para atingir os objetivos deste plano;

- O correto alinhamento entre os departamentos técnicos, administrativos e a gestão envolvidos no Plano;
- Capacitação dos profissionais de TI e dos usuários dos ativos de TI em geral;
- Disponibilidade orçamentária.

9. Conclusão

O Plano de Continuidade de Serviços de Tecnologia da Informação, implementado pela Divisão de Tecnologia da Informação da Prefeitura de Araçoiaba da Serra, é uma ferramenta fundamental que funcionará como um guia estratégico para mitigar ao máximo as paralisações que podem ocorrer devido a desastres ou fatores de risco identificados neste documento. Seu objetivo é garantir o reestabelecimento dos serviços essenciais em um tempo reduzido e com o menor impacto possível, tanto para a administração pública quanto para os munícipes que dependem, de maneira direta ou indireta, dos serviços de tecnologia da informação e comunicação oferecidos pelo município.

A eficácia deste plano está intrinsicamente ligada ao seu alinhamento com o núcleo administrativo da Prefeitura. É imprescindível que haja um compromisso conjunto para assegurar a alocação de recursos adequados, permitindo a constante evolução das ferramentas de TI utilizadas na administração municipal. Isso não apenas contribuirá para a redução dos riscos associados a falhas de sistema, mas também ajudará a prevenir a ocorrência de desastres que poderiam exigir a ativação deste plano. Assim, a Prefeitura de Araçoiaba da Serra se posiciona de forma proativa, fortalecendo a resiliência de sua infraestrutura de TI e, consequentemente, melhorando a qualidade dos serviços prestados à comunidade.