QUINTA | 16/02/2023
EDIÇÃO 337
ANO 03

# DIÁRIO OFICIAL ELETRÔNICO TUPÃ

ESTÂNCIA TURÍSTICA

TUPÃ DIGITAL



# ÍNDICE

GABINETE

OBRAS, PLANEJAMENTO E TRÂNSITO

GOVERNO

ADMINISTRAÇÃO

AGRICULTURA E MEIO AMBIENTE

RELAÇÕES INSTITUCIONAIS

ASSISTÊNCIA SOCIAL

CULTURA

ASSUNTOS JURÍDICOS

DESENVOLVIMENTO ECONÔMICO

EDUCAÇÃO

SAÚDE

ESPORTES

FINANÇAS

TURISMO

GABINETE CLIQUE NO ÍCONE PARA SER REDIRECIONADO CASO TENHA PUBLICAÇÕES

# EXPEDIENTE

**PREFEITO DA ESTÂNCIA TURÍSTICA DE TUPÃ**
Caio Kanji Pardo Aoqui

**VICE-PREFEITO DA ESTÂNCIA TURÍSTICA DE TUPÃ**
Renan Victor Pontelli

**SECRETÁRIO MUNICIPAL DE ADMINISTRAÇÃO**
Everton Nakashima

**SECRETÁRIO MUNICIPAL DE AGRICULTURA**
Anderson Luiz

**SECRETÁRIO MUNICIPAL DE ASSUNTOS JURÍDICOS**
João José Pinto

**SECRETÁRIO MUNICIPAL DE COMUNICAÇÃO**
Tiago Pettenuci

**SECRETÁRIO MUNICIPAL DE DESENVOLVIMENTO ECONÔMICO E COMÉRCIO EXTERIOR**
Newton takahara

**SECRETÁRIO MUNICIPAL DE DESENVOLVIMENTO SOCIAL E DIREITOS HUMANOS**
Telma Tulim

**SECRETÁRIO MUNICIPAL DE EDUCAÇÃO CULTURA E ESPORTE**
Valdir Berti

**SECRETÁRIO MUNICIPAL DE FINANÇAS**
Wilson Quiles Junior

**SECRETÁRIO MUNICIPAL DE GABINETE E TURISMO**
Cesar Juvenal de Faria

**SECRETÁRIO MUNICIPAL DE GOVERNO**
**Cesar Juvenal de Faria**

**SECRETÁRIO MUNICIPAL DE MEIO AMBIENTE**
José Rodrigues

**SECRETÁRIO MUNICIPAL DE PLANEJAMENTO E INFRAESTRUTURTA**
Valentim Cesar Bigesshi

**SECRETÁRIO MUNICIPAL DE SAÚDE**
Miguel Angelo de Marchi

# PODER EXECUTIVO

## Saúde

## Outros Atos

**PREFEITURA DA ESTÂNCIA TURÍSTICA DE TUPÃ**
**SECRETARIA MUNICIPAL DE SAÚDE**
**CONVITE AUDIÊNCIA PÚBLICA**

Em cumprimento ao artigo 12 da Lei nº 8689/93 e Lei Complementar 141/2012, a Secretaria Municipal de Saúde de Tupã, CONVIDA os munícipes para participarem da Audiência Pública que será realizada no dia 17/02/2023, às 09 horas, no Plenário da Câmara, rua Praça da Bandeira, 222. Serão apresentados os Relatórios Financeiros e Operacionais do Fundo Municipal de Saúde, produção e ofertas, referentes ao terceiro quadrimestre de 2022, aprovado pelo Conselho Municipal de Saúde em 13/02/2023.

Tupã (SP), 14 de fevereiro de 2023.

Miguel Ângelo De Marchi

Secretário Municipal de Saúde

## Administração

## Licitações e Contratos

## Aviso de Licitação

AVISO DE LICITAÇÃO PREGÃO PRESENCIAL Nº 018/2023 - PROCESSO LICITATÓRIO Nº 090/2023 - TIPO DE LICITAÇÃO: Menor preço por item. - OBJETO: CONTRATAÇÃO DE EMPRESA DO RAMO PARA PRESTAÇÃO DE SERVIÇOS CONTABEIS (CONTABILIDADE EM GERAL) PARA ATENDER AS DEMANDAS DA SECRETARIA MUNICIPAL DE EDUCAÇÃO, ESPORTE E CULTURA, SECRETARIA MUNICIPAL DE DESENVOLVIMENTO SOCIAL E DIREITOS HUMANOS DO MUNICÍPIO DE TUPÃ/SP, PELO PERÍODO DE 12 (DOZE) MESES. ABERTURA: 07/03/2023, às 08h30min. O edital e seus anexos encontram-se disponíveis no Depto de Licitação, no Paço Municipal, localizado na Praça da Bandeira, nº 800 (centro), nesta cidade de Tupã (SP), ou através do telefone (0XX14) 3404-1000, de segunda a sexta-feira, das 07h30min às 11h30min e dás 13h00min às 17h00min, no site www.tupa.sp.gov.br. Tupã, em 15/02/2023. Caio Kanji Pardo Aoqui, Pref. Mun.

AVISO DE LICITAÇÃO PREGÃO PRESENCIAL Nº 019/2023 - PROCESSO LICITATÓRIO Nº 092/2023 - TIPO DE LICITAÇÃO: Menor preço por item. - OBJETO: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA AQUISIÇÃO DE MOBILIÁRIOS DESTINADOS A BIBLIOTECA PÚBLICA MUNICIPAL "PROFESSOR TOBIAS RODRIGUES" DO MUNICÍPIO DE TUPÃ/SP. ABERTURA: 08/03/2023, às 14h30min. O edital e seus anexos encontram-se disponíveis no Depto de Licitação, no Paço Municipal, localizado na Praça da Bandeira, nº 800 (centro), nesta cidade de Tupã (SP), ou através do telefone (0XX14) 3404-1000, de segunda a sexta-feira, das 07h30min às 11h30min e dás 13h00min às 17h00min, no site www.tupa.sp.gov.br. Tupã, em 15/02/2023. Caio Kanji Pardo Aoqui, Pref. Mun.

## Deliberação

DELIBERAÇÃO – TOMADA DE PREÇOS n° 002/2023 - Contratação de empresa do ramo de arquitetura ou engenharia civil, para prestação de serviços de Recapeamento de vias públicas localizadas nas ruas Raphaela Bardelin, Antônio Digigow, São Carlos e São Jorge, no município de Tupã/SP com fornecimento de materiais, equipamentos e mão de obra, com recurso Estadual parcialmente oriundo de Termo de Convênio nº 103176/2022, por intermédio da Secretaria de Desenvolvimento Regional do Estado de SP. - Em continuidade aos trabalhos da Tomada de Preços n° 002/2023, em não havendo apresentação por parte dos licitantes de recurso quanto à fase de habilitação, deliberam pela designação de nova data de para a realização da sessão pública para abertura das propostas, a qual ocorrerá no dia 17 de fevereiro de 2023, às 10h00min, na Sala de Licitações localizada no Paço Municipal. Tupã, em 15/02/2023. Caio Kanji Pardo Aoqui, Pref. Mun.

## Ratificação

TERMO DE RATIFICAÇÃO – Processo nº 63/2023 – DISPENSA DE LICITAÇÃO nº 036/2023 - SECRETARIA MUNICIPAL DE SAÚDE - Contratação de empresa especializada para prestação de serviço de suporte e monitoramento do Sistema de Informação da Atenção Básica do Ministério da Saúde (E-Gestor, Sistema Terceiro (Atualmente SIS), SISAB, Auxílio Brasil, SISVAN, PSE e Informatiza APS, pelo período de 12 (doze) meses. - Diante dos elementos que instruem o processo, no uso das atribuições legais que me confere a legislação em vigor, especialmente a Lei de Licitações nº 8666/93 e suas alterações posteriores, RATIFICO a Dispensa de Licitação nº 036/2023 – Processo nº 063/2023, nos termos do inciso II, do artigo 24, da Lei nº 8.666/93, para a contratação da empresa RVMA TREINAMENTO EM TECNOLOGIA LTDA. -ME, para prestação de serviço de suporte e monitoramento do Sistema de Informação da Atenção Básica do Ministério da Saúde (E-Gestor, Sistema Terceiro (Atualmente SIS), SISAB, Auxílio Brasil, SISVAN, PSE e Informatiza APS, pelo período de 12 (doze) meses, conforme Termo de Referência, com uma despesa total estimada de R$ 17.520,00, com observação as justificativas apresentadas pela Secretaria Municipal de Saúde e demais documentos anexos ao

Processo Administrativo Eletrônico nº 1.319/2023. Tupã, 06/02/2023. Caio K. P. Aoqui, Pref. Mun.

TERMO DE RATIFICAÇÃO – Processo nº 86/2023 – DISPENSA DE LICITAÇÃO nº 054/2023 - SECRETARIA MUNICIPAL DE SAÚDE - CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS DE SUPORTE TÉCNICO E MONITORAMENTO DO SISTEMA E-SUS DESTINADO A SECRETARIA MUNICIPAL DE SAÚDE DE TUPÃ, PELO PERÍODO DE 12 (DOZE) MESES. - Diante dos elementos que instruem o processo, no uso das atribuições legais que me confere a legislação em vigor, especialmente a Lei de Licitações nº 8666/93 e suas alterações posteriores, RATIFICO a Dispensa de Licitação nº 054/2023 – Processo nº 086/2023, nos termos do inciso II, do artigo 24, da Lei nº 8.666/93, para a contratação da empresa INPULSO DIGITAL LTDA, para prestação de serviço de suporte técnico e monitoramento do Sistema E-SUS, pelo período de 12 (doze) meses, conforme Termo de Referência, com uma despesa total estimada de R$ 17.107,20, com observação as justificativas apresentadas pela Secretaria Municipal de Saúde e demais documentos anexos ao Processo Administrativo Eletrônico nº 700/2023. Tupã, 15/02/2023. Caio K. P. Aoqui, Pref. Mun.

TERMO DE RATIFICAÇÃO – Processo nº 89/2023 – DISPENSA DE LICITAÇÃO nº 057/2023 - SECRETARIA MUNICIPAL DE SAÚDE - Aquisição, em caráter emergencial, de insumos de enfermagem para atender às demandas das Unidades Básicas de Saúde do Município de Tupã/SP. - Diante dos elementos que instruem o processo, destacando-se o teor do r. parecer exarado pela douta Secretaria Municipal de Assuntos Jurídicos, cujas conclusões acolho, por seus próprios e jurídicos fundamentos, e toda documentação anexa ao processo, RATIFICO, nos termos do artigo 26, “caput”, da Lei de Licitações nº 8.666/93, a dispensa de licitação, em caráter emergencial, com base no artigo 24, IV da Lei nº 8.666/93, para a aquisição de insumos de enfermagem para atender às demandas das Unidades Básicas de Saúde do Município de Tupã/SP, tendo em vista o baixo estoque dos materiais requisitados, pelo período suficiente para realização de novo procedimento licitatório, conforme justificativas apresentadas pela Secretaria Municipal de Saúde, com observação aos princípios norteadores da Administração Pública, em especial, aos Princípio da Continuidade do Serviço Público, Princípio do Interesse Público e Princípio da Eficiência. DESPESA TOTAL ESTIMADA NO VALOR DE R$ 28.858,80, com disponibilidade de recursos orçamentários. EMPRESAS VENCEDORAS: COMERCIAL PABLOS LTDA. -ME, itens 3, 4 e 9, pelos valore unitários de, respectivamente, R$ 24,90, R$ 16,60 e R$ 14,80; INOVA COMERCIAL HOSPITALAR EIRELI LTDA, itens 1, 2, 5 e 8, pelos valores unitários de, respectivamente, R$ 8,68, R$ 13,80, R$ 0,51 e R$ 8,50; MANZATOS FARMA LTDA. -EPP, itens 6 e 7, pelos valores unitários de, respectivamente, R$ 1,89 e R$ 5,65; DROGARIA TAMOIOS DE TUPÃ LTDA. -EPP, itens 10 e 11, pelos valores unitários de, respectivamente, R$ 6,00 e R$ 7,00. Tupã, 15/02/2023. Caio K. P. Aoqui, Pref. Mun.

Atos Administrativos

Outros atos administrativos

Prefeitura Municipal da Estância Turística de Tupã
Departamento de Tecnologia e Processos

# GESTÃO DE RISCOS DE TI

Dezembro/2022

# Sumário

## Índice de conteúdos

Histórico de Alterações ..... 2
Histórico de Revisões ..... 2
Histórico de Aprovações ..... 2
1. APRESENTAÇÃO ..... 3
1.1. Princípios da Gestão de Riscos ..... 3
2. PROCESSO DA GESTÃO DE RISCOS ..... 3
2.1 Estabelecimento do Contexto ..... 4
2.2 Processo de Avaliação de Riscos ..... 4
2.2.1 Identificação de Riscos ..... 4
2.2.2 Análise de Riscos ..... 5
2.2.3 Avaliação de Riscos ..... 7
2.3 Tratamento de Riscos ..... 8
2.4 Monitoramento e Análise Crítica ..... 12
2.5 Comunicação e Consulta ..... 12
3. RECURSOS ..... 13
4. PAPÉIS E RESPONSABILIDADE ..... 13

## Histórico de Alterações

| Versão | Descrição | Modelo | Período | Responsável | Local |
|---|---|---|---|---|---|
| 1.0.0 | Criação do Plano de Gestão de Riscos deTI | 1.0.0 | Dezembro /2022 | Flavio Fagoti Pelim sistemas@tupa.sp.gov.br | DTP-PMETT |
| | | | | | |

## Histórico de Revisões

| Versão | Revisor | Período da Revisão | Próxima Revisão | Local |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

## Histórico de Aprovações

| Versão | Aprovação (Carimbo/Assinatura) | Data |
|---|---|---|
| 1.0 | Everton Nakashima | 13/02/2023 |
| | | |
| | | |
| | | |

# 1. APRESENTAÇÃO

O plano de gestão de riscos é um esquema dentro da estrutura de gestão de riscos que especifica a abordagem, os recursos a serem aplicados para gerenciar riscos e os componentes de gestão, incluindo procedimentos, práticas, sequência e cronologia das atividades e atribuição de responsabilidades.

## 1.1. Princípios da Gestão de Riscos

Os princípios da gestão de riscos fornecem orientações sobre as características de uma gestão de riscos eficaz e eficiente, comunicando seu valor e explicando sua intenção e propósito. Os princípios são a base para gerenciar riscos e convém que sejam considerados no Plano de Gestão de Riscos da organização. Os princípios direcionam uma abordagem: integrada; estruturada e abrangente; personalizada; inclusiva; dinâmica; baseada na melhor informação disponível; baseada em fatores humanos e culturais.

# 2. PROCESSO DA GESTÃO DE RISCOS

O processo de Gestão de Riscos da PMETT possui as seguintes etapas:

- Estabelecimento do Contexto;
- Processo de Avaliação de Riscos;
- Tratamento de Riscos;
- Monitoramento e Análise Crítica;
- Comunicação e Consulta.

### 2.1 Estabelecimento do Contexto

Ao iniciar as atividades para a elaboração do plano de gestão de riscos, a primeira tarefa consiste em compreender o ambiente no qual o trabalho será desenvolvido, definir o escopo e critérios a serem considerados no processo de gestão de riscos. Nesta etapa, a equipe que realiza a gestão de risco deve identificar todos os processos e atividades críticas sujeitas a vulnerabilidades de forma que os riscos possam ser gerenciados.

### 2.2 Processo de Avaliação de Riscos

O Processo de Avaliação de Riscos de Tecnologia da Informação possui as seguintes etapas:

- identificação de riscos;
- análise de riscos;
- avaliação de riscos.

#### 2.2.1 Identificação de Riscos

Uma vez definidos os serviços críticos para a estratégia da Prefeitura Municipal da Estância Turística de Tupã (PMETT), a ação prática do gestor do ativo nesta etapa deve ser identificar os ativos de TI que suportam a execução desses serviços críticos. Tal atividade dá início a etapa de identificação dos riscos de TI.

As ameaças e as vulnerabilidades associadas a cada ativo que suporta um serviço crítico devem ser levantadas conforme o estabelecido na norma ISO 27005, permitindo, assim, uma identificação mais apropriada dos riscos de TI.

### 2.2.2 Análise de Riscos

Na análise de riscos, para cada um dos riscos identificados na etapa anterior, a ação prática do gestor de risco deve ser avaliar a probabilidade, risco e o nível desse risco.

**Probabilidade** - é a chance de um evento ocorrer dentro do prazo previsto para se alcançar o resultado ou objetivo. Por exemplo, se o objeto da gestão de riscos é um projeto, estima-se a probabilidade da ocorrência do risco durante o prazo previsto para entrega do seu produto final. Para estimar a probabilidade será usada uma escala qualitativa de cinco níveis, conforme a seguir.

| Escala de Probabilidade | |
|---|---|
| Muito baixa | Acontece apenas em situações excepcionais. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência. |
| Baixa | o histórico conhecido aponta para baixa frequência de ocorrência no prazo associado ao objetivo |
| Média | Repete-se com frequência razoável no prazo associado ao objetivo ou há indícios que possa ocorrer nesse horizonte |
| Alta | Repete-se com elevada frequência no prazo associado ao objetivo ou há muitos indícios que ocorrerão nesse horizonte. |
| Muito alta | Ocorrência quase garantida no prazo associado ao objetivo. |

**Impacto** - o impacto mede o potencial comprometimento do objetivo ou resultado. Por exemplo, um risco com potencial para comprometer um objetivo na sua totalidade ou na sua quase totalidade é considerado um risco de alto impacto. Segue abaixo a escala para impacto.

| Escala de Impacto | |
|---|---|
| Muito baixo | Compromete minimamente o atingimento do objetivo; para fins práticos, nãoaltera o alcance do objetivo/resultado. |
| Baixo | Compromete em alguma medida o alcance do objetivo, mas não impede oalcance da maior parte do objetivo/resultado. |
| Médio | Compromete razoavelmente o alcance do objetivo/resultado. |
| Alto | Compromete a maior parte do atingimento do objetivo/resultado |
| Muito alto | Compromete totalmente ou quase totalmente o atingimento doobjetivo/resultado. |

**Nível de Risco** - O nível de risco é calculado a partir da combinação das escalas de probabilidade e de impacto. Para definir o nível de risco, deve ser usada a matriz a seguir:

| | | | | | | |
|---|---|---|---|---|---|---|
| Impacto | Muito alto | 15 | 19 | 22<br>Risco (b) | 24 | 25 |
| | Alto | 10 | 14<br>Risco (a) | 18 | 21 | 23 |
| | Médio | 6 | 9 | 13 | 17 | 20 |
| | Baixo | 3 | 5 | 8 | 12 | 16 |
| | Muito baixo | 1 | 2 | 4 | 7 | 11 |
| Legenda Nível Risco<br>Alto<br>Médio<br>Baixo | | Muito Baixa | Baixa | Média | Alta | Muito alta |
| | | Probabilidade | | | | |

**Figura 1:** Matriz probabilidade e impacto

Segue um exemplo de análise de risco para melhor entendimento:

a) Indisponibilidade da rede de dados;
- Impacto: alto
- Probabilidade: baixa

b) Perda da base de dados, sem possibilidade de recuperação.
- Impacto: muito alto
- Probabilidade: média

Olhando para a tabela acima é possível deduzir o nível de risco de cada um dos dois eventos: o nível de risco de (a) é 14 e o de (b) é 22. O nível de risco é dado pelo número inscrito em cada célula da matriz, não sendo obtido por qualquer fórmula matemática. São 25 possíveis níveis de risco, em que cada nível está associado a uma estimativa de probabilidade e de impacto. A matriz ordena os possíveis níveis de risco, desde o mais baixo, ao qual é atribuído o nível 1 (evento muito raro, de impacto muito baixo), até o mais elevado, ao qual se atribui o nível 25 (probabilidade muito alta, evento praticamente certo, e de impacto muito alto).

Algumas considerações importantes sobre o uso das matrizes de impacto e probabilidade:

- O impacto é a dimensão mais importante: um evento de impacto muito alto e de probabilidade de ocorrência muito baixa deve preocupar o gestor muito mais do que o oposto, um evento de probabilidade muito alta e impacto muito baixo – se o impacto é mínimo, logo a preocupação deve ser menor.
- Atribuição de valores arbitrários: deve-se evitar o uso de matrizes que “calculam” o nível do risco pela soma ou multiplicação desses valores, dado o risco de distorção trazido por matrizes simétricas, que consideraram como do mesmo nível os riscos descritos no item anterior. Na matriz acima apresentada, um risco com probabilidade muito baixa e impacto muito alto é classificado como de nível 15, enquanto outro risco de probabilidade muito alta e impacto muito baixo é considerado de nível 11, ou seja, é bem menos prioritário para a ação do gestor do que o de nível 15.
- Fazer a avaliação dos riscos considerando a situação real da PMETT (considerando os controles existentes e em funcionamento).

### 2.2.3 Avaliação de Riscos

A avaliação do risco envolve a comparação do nível de risco dos ativos da PMETT com o limite de exposição a riscos, a fim de determinar que riscos a Prefeitura está disposta a aceitar. O limite de exposição a riscos representa o nível de risco acima

do qual é desejável o tratamento do risco. Espera- se que com os resultados do tratamento o nível de risco real fique abaixo do limite de exposição tolerável.

A ação prática do gestor de risco nesta fase deve ser: identificar, na matriz probabilidade e impacto, os riscos cujos níveis estão acima do limite de exposição a riscos (faixa vermelha) e, para esses riscos, identificar as respectivas fontes, causas e consequências; os riscos que estão na faixa amarela, abaixo do limite de exposição a riscos, deverão ser monitorados os riscos que estão na faixa verde, também abaixo do limite de exposição, podem ser aceitos sem que nenhuma providência tenha que ser tomada. Para retratar o exposto neste parágrafo, segue uma tabela na sequência.

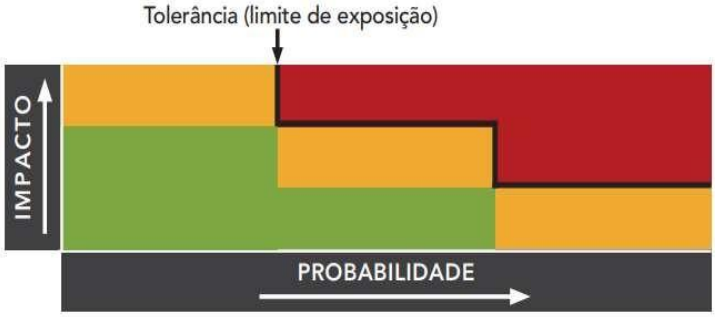



**Figura 2**: Matriz de avaliação dos riscos

## 2.3 Tratamento de Riscos

O tratamento de riscos está relacionado à resposta a riscos encontrados. Envolve decidir se o risco vai ser tratado ou não, promovendo a priorização de tratamento dos riscos. A estratégia de tratamento de risco adotada pela PMETT é composta pelas opções: modificar o risco, aceitar o risco, evitar o risco e compartilhar o risco, conforme descrito na tabela a seguir:

| RESPOST AO RISCO | DESCRIÇÃO |
|---|---|
| Modificar | O risco precisa ser gerenciado pela inclusão, exclusão ou alteração de controles, para que o risco residual possa ser reavaliado e consideradoaceitável. |
| Aceitar | O objetivo dessa resposta é avaliar se os demais tipos de respostas ao risco são viáveis. Em algumas situações, como: risco de baixo nível ou custo desproporcional ao benefício do tratamento, a opção mais adequada é aceitar ou reter o risco. |
| Evitar | Inclui basicamente a descontinuação das atividades que geram os riscos. Evitar riscos pode implicar a descontinuação de um software, a alienação de um equipamento ou a extinção de uma divisão ou processo de trabalho. |
| Compartilhar | Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco. As técnicas comuns compreendem a aquisição de produtos de seguro, a terceirização de umaatividade e outras. |

Conhecendo os riscos envolvidos em suas áreas de atuação e o resultado de suas análises, cada gestor deve levar em consideração o nível de tolerância ao risco e com isso tomar sua decisão sobre o tratamento dos riscos.

No Tratamento de Risco, a ação prática do gestor de risco é prover ações (respostas) para reduzir o nível de risco mapeado nos passos anteriores. Essas ações podem envolver controles, capacitação, redesenho de processo, realocação de pessoas, aperfeiçoamento de soluções de TI, etc. que, ao final, irão modificar, evitar, aceitar ou compartilhar os riscos.

Para colocar em prática o tratamento de riscos, é apresentada a seguir uma ferramenta chamada *What If*, que foi adaptada para este Plano. Ela não serve apenas para tratar os riscos, mas também permite tratar todas as etapas já discutidas anteriormente, como identificação, análise e avaliação dos riscos, podendo, portanto, ser usada pelo gestor para colocar tudo em prática a partir de um só lugar.

| | | | | | |
|---|---|---|---|---|---|
| | De 1 a 6 = risco baixo | | De 7 a 19 = risco médio | | De 20 a 25 = risco alto |

| Serviços / Sistemas | E se | Efeito | Probab. | Impacto | Risco | Controles Atuais | Ações Recomendadas | Resp. | Prazo | Implan. | Nova Probab. | Novo Impacto | Risco Residual |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bases de dados críticas | Ocorresse perda dos dados sem possibilidade de recuperação | Interrupção de serviços essenciais. Perda de Dados críticos. | Média | Multo Alto | 22 | Realização de backup local.<br>Teste de backup. | Backups remotos e em serviços de nuvem.<br>Backups protegidos por segurança física ou criptografia ao transferir pela rede. | T.I. | | SIM | Muito Baixa | Médio | 6 |
| Datacenter da PMETT | Acabasse a energia | Interrupção de serviços essenciais.<br>Danos ao hardware de servidores.<br>Danos a bancos de dados de sistemas. | Alta | Alto | 21 | No-Break | Gerador de Energia | T.I. | | NAO | Alta | Muito Baixo | 7 |
| Servidores do datacenter da PMETT | Surgisse um ransomware em um ou mais servidores | Interrupção de serviços essenciais.<br>Perda de dados críticos.<br>Comprometimento de todos os dados da rede. | Baixa | Muito Alto | 19 | Boas soluções de antivirus pago nos servidores.<br>Backups. | Boa solução de antivirus pago em todas as maquinas clientes.<br>Backup frio periodico.<br>Restringir acesso aos servidores. | T.I. | | NAO | Muito Baixa | Médio | 6 |
| Estações cliente da PMETT | Surgisse um ransomware em uma ou mais estações | Comprometimento dos dados da maquina cliente e de toda a rede. | Média | Alto | 18 | Soluções gratuitas de antivirus.<br>Criação de usuários no domino ou local sem privilégio de administrador | Boa solução de antivirus pago em todas as maquinas clientes. | T.I. | | NAO | Muito Baixa | Alto | 10 |
| Servidores do datacenter da PMETT | Um ou mais discos rigidos apresentassem defeito | Interrupção de serviços essenciais.<br>Perda de dados críticos | Baixa | Alto | 14 | Raid 0.<br>Backup variados. | Discos rigidos sobressalentes.<br>Min de 20% do total. | T.I. | | NAO | Baixa | Baixo | 5 |
| Servidores do datacenter da PMETT | Um ou mais sistemas operacionais não estiverem iniciando | Interrupção de serviços essenciais. | Baixa | Médio | 9 | Backups variados. | Maquina fisica ou virtual pronta para receber os dados e retomar o serviço.<br>Restringir acesso. | T.I. | | NAO | Muito Baixa | Baixo | 3 |
| Servidores do datacenter da PMETT | A maquina (hardware) de um ou mais servidores não estiver iniciando | Interrupção de serviços essenciais. | Baixa | Médio | 9 | Backups variados. | Maquina fisica ou virtual pronta para receber os dados e retomar o serviço. | T.I. | | NAO | Baixa | Baixo | 5 |
| Switches do datacenter da PMETT | Apresentasse defeito | Interrupção de serviços essenciais. | Baixa | Alto | 14 | | Switches sobressalentes. | T.I. | | NAO | Baixa | Muito Baixo | 2 |
| Rede de dados | O trafego de rede de dados de um local apresentasse falha | Interrupção de serviços locais. | Média | Médio | 13 | | Roteador inteligente ou firewall em cada ponto. | T.I. | | NAO | Média | Baixo | 8 |
| Rede de dados | O trafego de rede de dados geral apresentasse falhas | Interrupção de serviços locais, gerais e essenciais. | Média | Alto | 18 | Conexoes concentradas em um roteador inteligente com logs. | | T.I. | | SIM | Média | Baixo | 8 |
| Sistemas em datacenters terceirizados | Houvesse indisponibilidade de um ou mais sistemas de terceiros | Interrupção de serviços essenciais. | Baixa | Alto | 14 | | Exigir redundancia ou sla em contrato. | T.I. | | NAO | Baixa | Médio | 5 |
| Sistemas essenciais | Um ou mais bancos de dados fossem corrompidos | Interrupção de serviços essenciais. | Muito Baixa | Muito Alto | 15 | Backups diversos | Backups mais frequentes | T.I. | | NAO | Muito Baixa | Alto | 10 |
| Sistemas essenciais | Bancos de dados fossem roubados ou destruidos por usuarios internos | Interrupção de serviços essenciais. | Baixa | Muito Alto | 19 | Backups diversos | Restringir acessos.<br>Backups mais frequentes | T.I. | | NAO | Muito Baixa | Alto | 10 |
| Datacenter da PMETT | Houvesse um incendio | Interrupção de serviços essenciais.<br>Perda de dados críticos. | Muito Baixa | Muito Alto | 15 | | Sistema antiincendio | T.I. | | NAO | Muito Baixa | Baixo | 3 |
| Ar | O ar condicionado | Danos a equipamentos | Baixa | Alto | 14 | | Segundo ar condicionado | T.I. | | SIM | Baixa | Muito | 2 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| condicionado do datacenter da PMETT | principal do datacenter parar | caros. Indisponibilidade ou queda de performance em serviços essenciais. | | | | | | | | | | Baixo | |
| Ar condicionado do datacenter da PMETT | Os dois ar condicionados pararem | Danos a equipamentos caros. Indisponibilidade ou queda de performance em serviços essenciais. | Muito Baixa | Muito Alto | 15 | | Ar condicionado portatil Migrar serviços para nuvem | T.I. | | NAO | Muito Baixa | Muito Baixo | 1 |
| Internet | Houvesse uma interrupção no serviço de internet principal | Interrupção de serviços essenciais. | Baixa | Alto | 14 | | Link redundante | T.I. | | SIM | Baixa | Muito Baixo | 2 |
| Internet | Houvesse indisponibilidade de internet nos dois provedores | Interrupção dos serviços prestados | Baixa | Alto | 14 | Link Redundante | Contratação de um terceiro provedor | T.I. | | NAO | Muito Baixa | Baixo | 3 |
| Internet | Houvesse uma quebra de senha em um ou mais sistemas | Perda de dados críticos. | Baixa | Alto | 14 | Logs Backups diversos | Restringir acessos. Backups mais frequentes | T.I. | | NAO | Muito Baixa | Alto | 10 |

**Figura 3:** Ferramenta What If adaptada

A ferramenta *What If* é genérica o que permite seu uso em diversas áreas: processos, etapas de processo, objetivos, resultados, produtos, serviços, sistemas, projetos, ações, etc. conforme foi descrito na primeira coluna da tabela acima. Nessa tabela foram colocados dois exemplos de serviços (nas duas primeiras linhas), meramente ilustrativos: Base de dados críticas e Serviço de Internet. Uma outra coluna interessante é a de risco (nível de risco). Por exemplo, para encontrá-la basta conferir a probabilidade e impacto do cenário “Houvesse perda de dados de sistemas críticos, sem possibilidade de recuperação” se materializar. A coluna “CONTROLES ATUAIS” refere-se a controles que foram implantados, ou seja, a realidade atual. A coluna “AÇÕES RECOMENDADAS” pode ser um ou alguns controles melhores ou simplesmente melhorias a serem implantadas no futuro e uma vez implantadas, deve nos levar a um novo nível de risco (Risco Residual), o que se espera que seja menor, já que novos controles foram colocados em prática.

### 2.4 Monitoramento e Análise Crítica

O monitoramento trata da revisão e avaliação periódica da gestão de riscos, objetivando aprimorarcontinuamente a instituição. O monitoramento tem finalidade de:

- Garantir que os controles sejam eficazes e eficientes no projeto e na operação.
- Obter informações adicionais para melhorar a avaliação dos riscos.
- Analisar os eventos e mudanças e aprender com o sucesso ou fracasso do tratamento dos riscos.
- Detectar mudanças nos contextos externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que poderão exigir a revisão da forma de tratar os riscos e das prioridades.
- Identificar os riscos emergentes, que poderão surgir após o processo de análise crítica, reiniciando ociclo do processo de gestão de riscos.

Convém que os resultados do monitoramento e da análise crítica sejam registrados e reportados periodicamente.

### 2.5 Comunicação e Consulta

A comunicação e a consulta constituem o fluxo de informações entre as partes envolvidas no processo de gestão de riscos a fim de assegurar a compreensão necessária à tomada de decisão, devendo durante todas as fases do processo de gestão de riscos. As informações devem estar consolidadas e organizadas de forma que seja fácil e inteligível o acompanhamento de todo o processo.

A consulta consiste na disponibilização das informações consolidadas em local de fácil acesso, como o portal corporativo da PMETT. A comunicação consiste no envio periódico das informações disponibilizadas na consulta para todos os envolvidos.

## 3. RECURSOS

Faz-se necessário que a PMETT aloque recursos apropriados para a gestão de riscos. Tais recursos podem ser pessoas, processos, produtos, comunicação e treinamento.

## 4. PAPÉIS E RESPONSABILIDADE

Para gerenciar o processo de gestão de riscos institucional, os integrantes de governança e gestão de riscos de TI da PMETT serão as seguintes unidades organizacionais:

a) Departamento de Tecnologia e Processos
b) Comitê Gestor do Plano Diretor de TI
c) Gestores de riscos.

# PLANO DE CONTINUIDADE DE TI

PMETT 2023

*Conservação, ininterrupção dos sistemas essenciais de TI da Prefeitura Municipal da Estância Turística de Tupã*

SUMÁRIO

HISTÓRICO DE VERSÕES ..... 2
REGISTRO DE ACIONAMENTO DO PCTI ..... 3
1. PLANO DE CONTINUIDADE DE TI (PCTI) ..... 4
1.1. JUSTIFICATIVA E OBJETIVO ..... 4
1.2. ESCOPO ..... 4
1.3. SERVIÇOS DE TI ESSENCIAIS ..... 4
1.4. ÁREA ..... 6
1.5. PRINCIPAIS RISCOS ..... 6
1.6. PAPÉIS E RESPONSABILIDADES ..... 7
1.7. INVOCAÇÃO DO PLANO ..... 9
1.8. MACROPROCESSOS DE T.I. ..... 10
1.9. ESTRATÉGIAS DE CONTINUIDADE ..... 12
2. PLANO DE CONTINUIDADE OPERACIONAL (PCO) ..... 13
2.1. DESCRIÇÃO ..... 13
2.2. OBJETIVO E ESCOPO ..... 13
2.3. GESTÃO ..... 13
2.4. EXECUÇÃO DO PLANO ..... 14
2.4.1. Avaliação de Impacto de Desastre ..... 14
2.4.2. Acionamento do plano ..... 14
2.4.3. Contingência de Warm Site T1 ..... 14
2.5. ENCERRAMENTO DO PCO ..... 15
3. PLANO DE ADMINISTRAÇÃO DE CRISES (PAC) ..... 16
3.1. DESCRIÇÃO ..... 16
3.2. OBJETIVO ..... 16
3.3. EXECUÇÃO DO PLANO ..... 16
3.4. COMUNICAR RETORNO DAS OPERAÇÕES ..... 20
3.5. ENCERRAMENTO DO PAC ..... 20
4 PLANO DE RECUPERAÇÃO DE DESASTRES (PRD) ..... 21
4.1. DESCRIÇÃO ..... 21
4.2. OBJETIVO E ESCOPO ..... 21
4.3. EXECUÇÃO DO PLANO ..... 21
4.4. ENCERRAMENTO DO PRD ..... 23
5 VALIDAÇÃO E TESTE DE PCTI ..... 24
6 APROVAÇÃO DO PCTI ..... 25

HISTÓRICO DE VERSÕES

| Versão | Descrição | Responsável |
|---|---|---|
| 1.0 | Criação da primeira versão do PCTI | Flávio Fagoti Pelim |
| 1.0 | Aprovação | Everton Nakashima |
| 1.0 | Publicação | Prefeitura Municipal da Estância Turística de Tupã |
| | | |
| | | |
| | | |
| | | |

HISTÓRICO DE ALTERAÇÃO E INCLUSÃO

| Data | Inclusão/Alteração | Modificado por |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

REGISTRO DE ACIONAMENTO DO PCTI

| | | | |
|---|---|---|---|
| Data/Hora _____/___/____ | | Data/Hora | ___/___/___ |
| Início _____:____ | | Fim | ___:____ |
| **Descrição** | | | |
| **Resultado** | | | |

| | | | |
|---|---|---|---|
| Data/Hora _____/___/____ | | Data/Hora | ___/___/___ |
| Início _____:____ | | Fim | ___:____ |
| **Descrição** | | | |
| **Resultado** | | | |

| | | | |
|---|---|---|---|
| Data/Hora _____/___/____ | | Data/Hora | ___/___/___ |
| Início _____:____ | | Fim | ___:____ |
| **Descrição** | | | |
| **Resultado** | | | |

# 1. PLANO DE CONTINUIDADE DE TI (PCTI)

## 1.1. JUSTIFICATIVA E OBJETIVO

Uma vez que falhas nos serviços de TIC impactam diretamente a continuidade da prestação dos serviços públicos, almeja-se com este plano prover medidas de proteção rápidas e eficazes para os processos críticos de TI relacionados aos sistemas essenciais em casos de incidentes graves ou desastres.

## 1.2. ESCOPO

O Plano de Continuidade de TI (PCTI) abrange as estratégias necessárias à continuidade dos serviços de TI essenciais: contingência, continuidade e recuperação. Está voltado a conceder continuidade aos processos definidos como críticos para a TI da Prefeitura Municipal da Estância Turística de Tupã.

## 1.3. SERVIÇOS DE TI ESSENCIAIS

São os seguintes os serviços essenciais, por ordem de priorização*, para o acionamento e execução do PCTI.

| Serviço | Criticidade | RPO* | RTO* | Impacto* | | | |
|---|---|---|---|---|---|---|---|
| | | | | Financeiro | Legal | Imagem | Operacional |
| **SISTEMA DE SAUDE** | Alta | 4 horas | 4 horas | Irrelevante | Alto | Crítico | Alto |
| **ESUS** | Alta | 4 horas | 4 horas | Irrelevante | Alto | Alto | Médio |
| **AR DATACENTER** | Alta | 1 dia | 2 horas | Alto | N/D | N/D | Alto |
| **INTERNET PAÇO** | Alta | 4 horas | 2 horas | Alto | N/D | N/D | Crítico |
| **SWITCHES PAÇO** | Alta | 4 horas | 4 horas | Médio | N/D | N/D | Crítico |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **SERVIÇOS AO CONTRIBUINTE** | Alta | | | Crítico | Crítico | Crítico | Crítico |
| **SIA** | Alta | 2 dias | 2 horas | Crítico | Alto | Crítico | Médio |
| **NOTA FISCAL ELETRONICA** | Alta | 2 dias | 2 horas | Crítico | Alto | Crítico | Baixo |
| **SCPI** | Alta | 2 dias | 2 horas | Médio | N/D | N/D | Alto |
| **1DOC** | Alta | 2 dias | 2 horas | Baixo | Médio | Médio | Alto |
| **DOMINIO** | Alta | 2 dias | 2 horas | Baixo | N/D | N/D | Alto |
| **EMAIL** | Alta | 1 dia | 2 horas | Baixo | Baixo | Alto | Alto |
| **SIP** | Média | 2 dias | 2 horas | Irrelevante | N/D | N/D | Médio |
| **SAS** | Média | 2 dias | 2 horas | Irrelevante | Médio | Médio | Médio |
| **GSA** | Média | 2 dias | 2 horas | Irrelevante | Baixo | Médio | Médio |
| **ABASTECIMENTOS** | Média | 2 dias | 2 horas | Irrelevante | N/D | N/D | Alto |
| **CHE** | Baixa | 2 dias | 2 horas | Irrelevante | N/D | N/D | Médio |
| **CAMERAS PAÇO** | Baixa | 3 dias | 8 horas | Baixo | N/D | Baixo | Baixo |
| **SBB** | Baixa | 2 dias | 2 horas | Irrelevante | Baixo | Baixo | Baixo |
| **PORTAL PREFEITURA** | Baixa | 2 dias | 2 horas | Médio | Baixo | Alto | Baixo |
| **TRANSPARENCIA** | Baixa | 2 dias | 2 horas | Irrelevante | Crítico | Crítico | Baixo |
| **NOBREAK PAÇO** | Baixa | 7 dias | 6 horas | Irrelevante | N/D | N/D | Baixo |
| **SENHAS CENTRAL** | Baixa | 1 dia | 20 min | Irrelevante | N/D | Médio | Baixo |

- **RPO** – ponto em uma linha de tempo em que os dados devem ser recuperados após a ocorrência de uma ruptura

- **RTO** – período de tempo dentro do qual os níveis mínimos dos serviços e/ou sistemas devem ser recuperados após a ocorrência de uma interrupção.

CONSIDERAÇÕES:

i. Os sistemas essenciais estão detalhados nos documentos anexos do PCTI: MAPEAMENTO DOS SISTEMAS ESSENCIAIS.

---

ii. A priorização dos serviços essenciais, os níveis de impacto no negócio e tempos toleráveis de recuperação serão definidos a partir da Análise de Impacto de Negócio (AIN).

### 1.4. ÁREA

O PCTI será administrado, avaliado e acionado no âmbito do Departamento de Tecnologia e Processos tendo sua manutenção, organização e melhoria revistas e atualizadas periodicamente pela Comissão de Plano Diretor de TI.

### 1.5. PRINCIPAIS RISCOS

O PCTI foi desenvolvido para ser acionado quando da ocorrência de cenários de desastres que apresentam risco à continuidade dos serviços essenciais. O quadro abaixo define estes riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência.

| EVENTO DE DESASTRE | POSSÍVEIS CAUSAS |
|---|---|
| **01- Interrupção de energia elétrica** | Causada por fator externo à rede elétrica do prédio ou de sua localidadecom duração da interrupção superior a 12 horas.<br>Causada por fator interno que comprometa a rede elétrica do prédio comcurto-circuitos, incêndio e infiltrações.<br>Impossibilidade de acionar o Grupo Moto-gerador no momento de umaqueda de energia. |
| **02 - Falha Climatização da sala cofre** | Superaquecimento dos ativos devido a falha no dimensionamento decarga na sala cofre |

| | |
|---|---|
| **03 - Indisponibilidade de rede/circuitos** | Rompimento de fibra ótica decorrente de execução obras públicas,desastres ou acidentes. |
| **04 - Falha humana** | Acidente ao manusear equipamentos, ou abastecimento do tanque de combustível. |
| **05 - Ataques internos (funcionários insatisfeitos)** | Ataque aos ativos do DataCenter. |
| **06 – Incêndio** | Criminoso.<br>Curto circuito.<br>Vazamento de gas. |
| **07 – Desastres Naturais** | Alagamento |
| **08 - Falha de hardware** | Falha que necessite reposição de peça ou reparo cujo reparo ou aquisição dependa de processo licitatório |
| **09 – Ataque Cibernético** | Ataque virtual que comprometa o desempenho, os dados ou configuração dos serviços essenciais. |

## 1.6. PAPÉIS E RESPONSABILIDADES

**COMITÊ DE DISASTER / RECOVERY (DR):**

- Avaliar o plano periodicamente e decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas.
- Inclui autoridades em nível institucional e tomadores de decisão do DTP (Departamento de Tecnologia e Processos).

**EQUIPE DE INSTALAÇÕES / AMBIENTE:**

- Responsável pelas instalações físicas que abrigam sistemas de TI e pela garantia que as instalações de alternativa são mantidas adequadamente. Avalia os danos e supervisiona os reparos para o local principal no caso de a localização primária sofra da destruição ou danos.
- O líder desta equipe administrará e manterá o Plano de Recuperação de Desastre.

**EQUIPE DE REDE:**

- Avaliar os danos específicos de qualquer infra-estrutura de rede e para fornecer dados e conectividade de rede de voz, incluindo WAN, LAN e quaisquer conexões de telefonia internamente dentro da PMETT ou de infraestrutura externa junto aos prestadores de serviço.

**EQUIPE DE SERVIDORES / APLICAÇÕES:**

- Fornecer a infraestrutura de servidor físico e virtuais necessária para que a TI execute suas operações e processos essenciais durante um desastre.
- Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre. Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais.

**EQUIPE DE OPERAÇÕES:**

- Fornecer aos funcionários as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível. Eles precisarão provisionar todos os funcionários da PMETT na solução de contingência e aqueles que trabalham remotamente com as ferramentas específicas à sua atuação.
- O líder desta equipe administrará e manterá o Plano de Continuidade Operacional.

**EQUIPE DE COMUNICAÇÃO:**

- Responsável por todas as comunicações durante um desastre. Especificamente, eles se comunicarão com os funcionários, clientes, autoridades, fornecedores e até mesmo com a mídia, se necessário.
- O líder desta equipe administrará e manterá o Plano de Administração de Crise.

**EQUIPE DE BACKUP:**

- Analisar as perdas e mapear a quantidade de dados perdidos, tempo de recuperação desses dados e formular estratégia de recuperação de dados de acordo com as políticas pré-estabelecidas.

**EQUIPE DE SEGURANÇA DA INFORMAÇÃO:**

- Prover mecanismos de segurança no ambiente principal e alternativo. Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade, cuja proteção estará contida na política de segurança.

O Departamento de Tecnologia da PMETT e seu corpo de funcionários, se encarregarão das atividades de quaisquer equipes acima ainda não estiverem formalmente definidas.

## 1.7. INVOCAÇÃO DO PLANO

O PCTI será acionado quando da ocorrência de algum dos cenários de desastres [5], a insurgência ou ocorrência de um risco desconhecido ou caso uma vulnerabilidade tenha grande possibilidade de ser explorada.

O plano também poderá ser invocado em casos de testes ou por determinação do COMITÊ DE DR em conjunto com a alta administração da PMETT.

Os integrantes da EQUIPE DE COMUNICAÇÃO serão responsáveis por acionar os contatos e partes interessadas, prioritariamente por telefone, ou pessoalmente caso seja possível.

**ÁRVORE DE ACIONAMENTO DE CONTATOS**

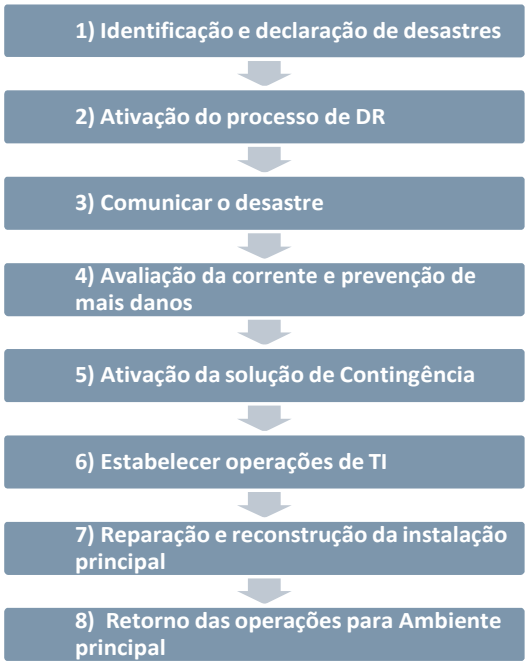
| EQUIPES | | RAMAL | TELEFONE | CONTATO SECUNDARIO |
|---|---|---|---|---|
| LIDER - COMITE DE DISASTER/RECOVERY (DR) | | 1055 | 34041000 | |
| | EQUIPE DE REDES | 1058 | 34041000 | |
| | EQUIPE DE SERVIDORES / APLICAÇÕES | 1058 | 34041000 | |
| | EQUIPE DE APLICAÇÕES | 1058 | 34041000 | |
| | EQUIPE DE OPERAÇÕES | 1058 | 34041000 | |
| | EQUIPE DE COMUNICAÇÕES | 1058 | 34041000 | |
| | EQUIPE DE BACKUP | 1067 | 34041000 | |
| | EQUIPE DE SEGURANÇA DA INFORMAÇÃO | 1067 | 34041000 | |

**CONSIDERAÇÕES:**

i. Ao acionar os contatos informar qual ponto de encontro mais próximo, local e detalhes para reunir as equipes.

## 1.8. MACROPROCESSOS DE T.I.

O PCTI tem seus macroprocessos definidos nas atividades a seguir e se desmembra em planos específicos para cada área de atuação quando da ocorrência de um desastre.




Os sub-planos do PCTI consistem em:

- Plano de Continuidade Operacional (PCO):
  - Garantir a continuidade dos serviços essenciais de TI críticos na ocorrência de um desastres, enquanto recupera-se o ambiente principal.

- Plano de Administração de Crise (PAC):
  - Definir a atividade das equipes envolvidas e orquestrar as ações de contingência e comunicaçãodurante e após a ocorrência de um desastre, com intuito de minimizar impactos até a superação da crise.

- Plano de Recuperação de Desastre (PRD):
  - O Planejar e agir para que, uma vez controlada a contingência e passada a crise, a TI da PMETT retome seus níveis originais de operação no ambiente principal.

## 1.9. ESTRATÉGIAS DE CONTINUIDADE

A estratégia de continuidade para o cenário atual da TI e serviços essenciais, está estabelecida da seguinte forma:

**TIPO :** Warm site T1

**DESCRIÇÃO:**

- Cópias de backup dos sistemas essenciais armazenadas em local alternativo (Nuvem ou outro local que não o datacenter principal).
- Não possui qualquer tipo de hardware configurado no local.
- Não dispõe de conexão redundante
- Downtime médio-alto*

**AÇÕES DE CONTINGÊNCIA/RECUPERAÇÃO:**

- Mapear perda de dados e ativos, reestabelecer toda a estrutura afetadae, após o ambiente principal estar operacional, prover a recuperação dos dados em backups.

**OBSERVAÇÕES:**

- As ações de contingência e recuperação são detalhadas nos subplanos a seguir.

# 2. PLANO DE CONTINUIDADE OPERACIONAL (PCO)

## 2.1. DESCRIÇÃO

Este plano descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços essenciais.

## 2.2. OBJETIVO E ESCOPO

É escopo deste plano garantir ações de continuidade durante e depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas das ações de contingência definidas na estratégia.

São objetivos PCO:

- Prover meios para manter o funcionamento dos principais serviços de TI e a continuidade das operações de TI, dos sistemas essenciais.
- Estabelecer procedimentos, controles e regras alternativas que possibilitem a continuidade das operações de TI durante uma crise ou cenário de desastre.
- Estabelecer uma equipe para cada plano PCO PRD e PAC
- Definir os formulários, checklists e relatórios a serem entregues pelas equipes ao executar a contingência.

## 2.3. GESTÃO

A Comissão Técnica do Plano Diretor de TI é a unidade responsável por implementar, manter e melhorar o PCO e toda documentação inerente.

## 2.4. EXECUÇÃO DO PLANO

### 2.4.1. Avaliação de Impacto de Desastre

Identificada a ocorrência de um incidente ou crise o Líder da Equipe de Operação e Backup deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido e divulgar a informação a todas as equipes envolvidas.

### 2.4.2. Acionamento do plano

Dado o aval pelo COMITÊ DE DR ao acionamento do plano, a EQUIPE DE OPERAÇÕES convocará reunião de emergência com os líderes do PRD e PAC com o intuito de:

- Coordenar prazos e orquestrar as ações de contingência.
- Informar as equipes ações de contingência com a priorização dos serviços essenciais.

### 2.4.3. Contingência de Warm Site T1

Devem ser adotadas as seguintes ações de contingência e continuidade por processo ou serviço essencial.

| Id | Instrução | Duração | Observação | Resultado |
|---|---|---|---|---|
| 1 | Verificar status da aplicação de backup e estimar impacto de perda dados (janela) | | | |
| 2 | Identificar discos cujos dados em questão foram afetados | | | |
| 3 | Mapear blocos a serem recuperados | | | |

| | | | | |
|---|---|---|---|---|
| 4 | Estimar volume de dados a serem recuperados, tempo de recuperação dos dados e possíveis perdas operacionais | | | |
| 5 | Atestar retorno do funcionamento do ambiente principalcom Líder do PRD | | | |
| 6 | Teste de aplicação de backup após desastre | | | |
| 7 | Validar policies implementadas | | | |
| 8 | Prover recovery dos dados às aplicações | | | |

## 2.5. ENCERRAMENTO DO PCO

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenterdeverá ser emitido um parecer ao comitê relatando as atividades realizadas neste PCO.

Informar à equipe de COMUNICAÇÃO o retorno das atividades.

# 3. PLANO DE ADMINISTRAÇÃO DE CRISES (PAC)

## 3.1. DESCRIÇÃO

Este plano especifica as ações ante os cenários de desastres. As ações incluem gerir, administrar, eliminar ou neutralizar os impactos, inerente ao relacionamento entre os agentes envolvidos e/ou afetados, até a superação da crise, através da orquestração das ações e de uma comunicação eficaz.

## 3.2. OBJETIVO

O objetivo deste plano é garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de uma catástrofe.

São objetivos específicos do PAC:

- Garantir a segurança à vida das pessoas;
- Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise.
- Orientar os funcionários e demais colaboradores com informações e procedimentos de conduta.
- Informar a sociedade em tempo e com esclarecimentos condizentes com o ocorrido.

## 3.3. EXECUÇÃO DO PLANO

Na ocorrência de um desastre será necessário entrar em contato com diversas áreas, principalmente as afetadas para informá-las de seu efeito na continuidade dos serviços e tempo de recuperação. A equipe de comunicação será responsável por contatar estas unidades e passar as informações pertinentes a cada grupo, setor ou seguimento.

Após reunião com líderes do PRD e PCO, a equipe de comunicação elaborará um breve programa de comunicação para acionar as partes envolvidas e afetadas de modo a manter todos bem informados e passar a todos a perspectiva dos esforços necessários para o reestabelecimento dos serviços inativos.

A comunicação com cada parte ocorrerá da seguinte forma:

3.3.1. COMUNICAR ÀS AUTORIDADES

A prioridade da equipe de comunicação será assegurar que as autoridades competentes tenham sido notificadas da catástrofe, principalmente se envolver risco às pessoas, fornecendo as seguintes informações delocalização, natureza, magnitude e impacto do desastre.

| **Autoridade** | **Número** | **Data /Hora do registro** | **Num. Ocorrência** |
|---|---|---|---|
| *Polícia* | *190* | | |
| *Bombeiros* | *193* | | |
| ***SAMU*** | ***192*** | | |

3.3.2. COMUNICAÇÃO COM OS FUNCIONÁRIOS

A equipe de comunicação deverá prover um meio de contato específico para este fim, com intuito de que as unidades da PMETT mantenham-se informadas da ocorrência de um desastre e da inatividade dos serviços essenciais de TI. Números de Contato a serem disponibilizados:

- Telefone: (14) 34041000
- E-mail: sistemas@tupa.sp.gov.br
- Central de Serviços (Whatsapp): 14 9 9812 9447

Caso não haja conectividade ou linha telefônica disponível, ceder estas informações por meio de publicações, ou outra estratégia definida no momento.

As informações a serem dadas irão se referir a:

- Se é seguro para eles entrarem no ambiente afetado
- Onde eles devem ir se não puderem ter acesso ao PMETT.
- Que serviços ainda estão disponíveis para eles
- Expectativas de trabalho durante o desastre

3.3.3. COMUNICAR UNIDADES E SETORES DO PMETT

- Acionar diretamente às unidade afetadas pelo desastre e fornecer contato
- Natureza, impacto e abrangência da catástrofe
- Ações de contingência em andamento
- Processos/sistemas e serviços cobertos pelo plano de continuidade (serviços essenciais)

| **Setor/Unidade** | **Número / CONTATO** | **Data /Hora do CONTATO** | **Local** |
|---|---|---|---|
| *Secretaria de Administração* | | | |
| Secretaria de Governo | | | |
| Secretaria de Finanças | | | |
| Secretaria de Assuntos Jurídicos | | | |
| Secretaria de Saúde | | | |
| Secretaria de Educação, Cultura e Esporte | | | |
| Secretaria de Relações Institucionais | | | |
| Secretaria de Turismo | | | |
| Secretaria de Assistencia Social | | | |

### 3.3.4. COMUNICAR FORNECEDORES E PRESTADORES DE SERVIÇO

| **LISTA DOS PRINCIPAIS FORNECEDORES** | |
|---|---|
| Empresa**: FIORILLI**<br>Nº Contato: | **Pessoa/Contato:** _____<br>**Data/Hora Acionamento:**<br>_____/_____/_____ ___:___:___ |
| Empresa**: SIMPLISS**<br>Nº Contato: | **Pessoa/Contato:**<br>**Data/Hora Acionamento:**<br>_____/_____/_____ ___:___:___ |
| Empresa**: INTEGRATIVA**<br>Nº Contato: | **Pessoa/Contato:** _____<br>**Data/Hora Acionamento:**<br>_____/_____/_____ ___:___:___ |
| Empresa**: GSA**<br>Nº Contato: | **Pessoa/Contato:** _____<br>**Data/Hora Acionamento:**<br>_____/_____/_____ _____:_____:_____ |
| Empresa**: BITTURBO**<br>Contato: | **Pessoa/Contato:** _____<br>**Data/Hora Acionamento:**<br>_____/_____/_____ ___:___:___ |
| Empresa**: CABONNET**<br>Contato: | **Pessoa/Contato:** _____<br>**Data/Hora Acionamento:**<br>_____/_____/_____ ___:___:___ |
| Empresa**: SOS IMPRESSORAS**<br>Contato: | **Pessoa/Contato:** _____<br>**Data/Hora Acionamento:**<br>_____/_____/_____ ___:___:___ |

### 3.3.5. COLABORADORES EXTERNOS, CIDADÃOS E MÍDIA

A equipe de comunicação, em consonância com a Assessoria de Comunicação do PMETT, deverá fornecer informações pertinentes aos colabores externos: Advogados, cidadãos e outros órgãos.

- Validar a situação passada de acordo com o cenário
- Buscar publicar em meios oficiais e de ampla divulgação, com aval do comitê decontinuidade e institucional, informações sobre o ocorrido.

| **Colaborador/ Rede/ Empresa/Pessoa** | **Contato** | **Publicação** | **E-mail** |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

## 3.4. COMUNICAR RETORNO DAS OPERAÇÕES

Comunicar a todas as partes acima supracitadas quando ocorrer o retorno das operações à normalidade

## 3.5. ENCERRAMENTO DO PAC

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do datacenter a EQUIPE DE COMUNICAÇÃO entrará em contato com as partes descritas neste plano provendo as informações de retorno das operações com as informações de status dos serviços essenciais.

Compor relatório com relação das atividades necessárias após a ocorrência do desastrescomo remanejamento dos canais de informação, abertura e acompanhamento de chamados correlatos ao ocorrido.

# 4 PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

## 4.1. DESCRIÇÃO

Este plano descreve os cenários de inoperância e seus respectivos procedimentos planejados, definindo as atividades prioritárias para reestabelecer o nível de operação dos serviços no ambiente afetado dentro de um prazo tolerável.

## 4.2. OBJETIVO E ESCOPO

É escopo deste plano garantir o retorno das operações do ambiente principal depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas dos ativos, conexões e configurações deste ambiente.

São objetivos PRD:

- Avaliar danos aos ativos e conexões do datacenter e prover meios para sua recuperação.
- Evitar desdobramentos de outros incidentes na facilidade principal.
- Reestabelecer o datacenter dentro do prazo tolerável

## 4.3. EXECUÇÃO DO PLANO

**Identificar ativos danificados**

As equipes de INSTALAÇÃO/BACKUP/SERVIDORES/REDE deverão identificar e listar todos os ativos danificados da ocorrência do desastre. As informações de cada ativos encontram-se no MAPA PMETT.

**Identificar acessos interrompidos**

A EQUIPE DE REDE deverá identificar as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, rede WAN ou com o provedor de serviços.

**Listar serviços descontinuados**

A equipe do PRD deverá mapear quais serviços foram descontinuados contendo as informações de perda de ativo e de conexão com intuito de levar ao conhecimento do COMITÊ DE DR. O relatório deverá abranger todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, firewall, storage, routers e switches, bem como respectivas configurações de proxy, dns, rotas, vlans etc.

**Elaborar cronograma de recuperação**

O líder do PRD após o mapeamento das perdas e impactos elaborará um breve cronogramade recuperação das aplicações levando em consideração:

- A priorização dos serviços essenciais, ou de acordo com determinação de nívelinstitucional.
- O RTO definido para cada serviço essencial.
- A força de trabalho disponível.

**Substituição de ativos e equipamentos**

Em caso de perda de ativos, deverá ser imediatamente informado ao comitê de DR a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. A equipe irá mensurar quanto tempo a aquisição irá impactar o RTO de cada serviço comunicando ao COMITÊ DE DR se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição.

A equipe de INSTALAÇÕES deve verificar quais ativos foram danificados estão cobertos por garantia e se poderá ser acionada neste caso através da lista de fornecedores.

As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes do PCO e PAC.

**Reconfiguração de ativos e equipamento**

A equipe de INSTALAÇÕES deverão verificar que as configurações dos ativos reparados ou substituídos estão em funcionamento pleno. Caso não estejam, prover cronograma estimado para configurar estes ativos informando à EQUIPE DE COMUNICAÇÃO e COMITÊ DE DR.

**Teste de ambiente**

O ambiente principal do datacenter antes do recovery dos dados do backup deverá ser testado afim de garantir que o processo de recuperação ocorra conforme o planejado.

Os testes incluem:

- Garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre.
- Validar as configurações

**Recuperar dados do backup**

Proceder a recuperação dos dados para as aplicações, seja do storage ou discos de backup.

## 4.4. ENCERRAMENTO DO PRD

Ao término do procedimento de recovery, as informações da recuperação de serviços serão consolidadas em parecer específico informando horário de reestabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

# 5 VALIDAÇÃO E TESTE DE PCTI

O PCTI será testado e validado em reunião entre os líderes de cada subplano a cada ano ou com a insurgência de novos fatores de risco, mudança na análise de impacto, ou com a inclusão de um novo serviço no plano de continuidade.

**Tipos de testes a serem realizados:**

- Teste de mesa:
- Caminho percorrido: Assegurar que cada integrante de processo crítico se familiarize com o PCTI
- Simulação: Simular uma situação realde interrupção.

**Status:**

- Programado
- Executado
- Planejado
- Agendado

| Data | Tipo | Motivo | Status |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

# 6 APROVAÇÃO DO PCTI

A versão 1.0 do PCTI fica aprovada em 13/02/2023 por deliberação das partes envolvidas.

.

| | |
|---|---|
| Flavio Fagoti Pelim | Everton Nakashima |
| Departamento de Tecnologia e Processos | Secretaria de Administração |

# Política de Backup

# PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Versão 1.0

Tupã, Dezembro de 2022

POLÍTICA DE CONTROLE DE BACKUP

**PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE TUPÃ**

**CAIO AOQUI**

Prefeito

**SECRETARIA DE ADMINISTRAÇÃO**

**Everton Nakashima**

Secretário de Administração

**DEPARTAMENTO DE TECNOLOGIA E PROCESSOS**

**Flávio Fagoti Pelim**

Analista de Projetos de T.I.

**Equipe Técnica de Elaboração**

Flávio Fagoti Pelim

**Equipe Revisora**

Aguinaldo Redi dos Reis

Carlos Henrique Ghiraldeli Saes Lopes

Ricardo Barbosa

# Sumário

Histórico de Versões ....3
Histórico de Revisão....3
Esclarecimentos ....4
Introdução....5
Política de Backup e Restauração de Dados Digitais ....5
Propósito....6
Escopo....6
**Termos e Definições**....6
Referência legal e de boas práticas ....7
Declarações da política ....8
Dos princípios gerais ....8
Não conformidade .... 13
Concordância.... 14

**Histórico de Versões**

| Data | Versão | Descrição | Autor |
|---|---|---|---|
| 08/12/2022 | 1.0 | Modelo de Política de Backup | Equipe Técnica de Elaboração |
| | | | |
| | | | |
| | | | |

**Histórico de Revisão**

| ID da versão | Data da Mudança | Autor |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

# Esclarecimentos

O objetivo deste documento é fornecer ao Departamento de Tecnologia e Processos e à Secretaria de Administração, orientações para mitigação de possíveis riscos ligados às temáticas de privacidade e segurança da informação, relativos aos seus sistemas informatizados, contratos administrativos e processos de trabalho da instituição.

O documento foi construído a partir de análises de pontos relevantes dos sistemas informatizados críticos de Tecnologia da Informação, realizadas pelo Departamento de Tecnologia e Processos.

# Introdução

No contexto da transformação digital do Estado brasileiro, o Governo Federal publicou em 29 de abril de 2020, por meio do Decreto nº 10.332, a Estratégia de Governo Digital, iniciativa que se encontra em plena execução. Ela norteia as ações de todos os órgãos federais, com o objetivo de transformar o governo pelo Digital, oferecendo políticas públicas e serviços de melhor qualidade, mais simples, acessíveis de qualquer lugar e a um custo menor para o cidadão.

Hoje, mais do que em qualquer outro momento da história, o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados

Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entidades como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

A proteção dessas informações pelo Governo enquanto agente de tratamento está designada no **Art.46. da Lei Geral de Proteção de Dados**, sancionada em 14 de agosto de 2018 – “Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.”

A sua não observância pode impactar diretamente a capacidade do governo federal de cumprir suas missões precípuas de promover uma gestão pública eficiente, ampliar o acesso à cidadania, estimular uma economia brasileira crescentemente digitalizada, dinâmica, produtiva e competitiva, e em última instancia, impedir a geração de valor público para o cidadão.

# Política de Backup e Restauração de Dados Digitais

| | |
|---|---|
| **Responsável** | Departamento de Tecnologia e Processos. |
| **Aprovado por:** | Secretaria de Administração |
| **Políticas Relacionadas** | Gestão de riscos. |
| **Localização de armazenamento** | Tupa.sp.gov.br |
| **Data da Aprovação** | |
| **Data de revisão** | 01/12/2024 |

# Propósito

A Política de Backup e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelo Departamento de Tecnologia e Processos e formalmente definidos como de necessária salvaguarda na Prefeitura Municipal, para se manter a continuidade do negócio. No sentido de assegurar sua missão é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças. O presente documento apresenta a Política de Backup e Restauração de Dados Digitais, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

# Escopo

- Esta política se aplica a todos os dados no âmbito da Prefeitura Municipal da Estância Turística de Tupã, incluindo dados fora dela, armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem bancos de dados de diversos sistemas, códigos fonte, arquivos compartilhados específicos e emails. A definição de dados críticos e o escopo desta política de backup serão revisados bienalmente.
- Os serviços de TI críticos da PMETT devem ser formalmente elencados pelo Comitê de gestão de políticas de TI.
- Já ficam previamente estabelecidos os bancos de dados de todos os sistemas como serviços críticos da PMETT.
- Esta política se aplica aos agentes públicos que podem ser criadores e/ou usuários de tais dados. A política também se aplica a terceiros que acessam e usam na PMETT sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade da PMETT.
- Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).
- A salvaguarda dos dados em formato digital pertencentes a serviços de TI da PMETT mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

# Termos e Definições

BACKUP OU CÓPIA DE SEGURANÇA - Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

CUSTODIANTE DA INFORMAÇÃO - Qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação;

ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

MÍDIA - Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

INFRAESTRUTURA CRÍTICA – instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;

Recovery Point Objective (RPO): ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

Recovery Time Objective (RTO): tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente;

## Referência legal e de boas práticas

| Orientação | Secção |
|---|---|
| Acórdão 1.889/2020-TCU-Plenário | Relatório de Levantamento de Auditoria Páginas 30-32 |
| Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022 | Em sua íntegra |
| Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD) | Art. 2, XXIII |
| Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER) | Anexo, Item 2.3.4 e 2.3.5 |
| Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) | Anexo Art.3, Inciso I, II e V |
| Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI) | CAPÍTULO I - Art.2, Incisos III e IV<br>CAPÍTULO II - Art.3, Inciso III, IV, VIII XI<br>CAPÍTULO VI - Seção IV – Art.15 |
| Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI; | v4.1: DS11: Gerenciar Dados<br>v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06 |
| Framework de segurança cibernética do CIS 8 | Salvaguardas do controle 11 (Data Recovery Capabilities) |
| Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI; | Gestão da Segurança da Informação |

| | |
|---|---|
| Guias Operacionais SGD | Todos |
| Instrução Normativa 01/GSI/PR | Art.12, Inciso IV, alínea g, h |
| Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021 | Capítulo IV |
| Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados | CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50 |
| Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI) | Em sua íntegra |
| Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemasde gestão de segurança da informação - Requisitos; | A.12.3 Cópias de segurança |
| Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação; | 12.3 Cópias de segurança |
| Portaria GSI/PR nº 93, de 18 de outubro de 2021 | Em sua íntegra |

# Declarações da política

**Dos princípios gerais**

1. A Política de Backup e Restauração de Dados deve estar alinhada com a Política de Segurança da Informação da PMETT.
2. A Política de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
3. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.
4. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
5. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.
6. O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.
7. A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.
8. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
9. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

**Da frequência e retenção dos dados**

10. Os backups dos serviços de TI críticos da PMETT devem ser realizados utilizando-se as seguintes frequências temporais:

    I – Diária;

    II – Anual;

11. Os serviços de TI críticos da PMETT devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

    I – Diária: 1 mês;

    II – Anual: 3 anos.

12. Os serviços de TI NÃO críticos da PMETT devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

    I – Diária: 1 mes;

    II – Anual: 2 anos.

13. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

14. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

15. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada por funcionários do Departamento de Tecnologia e Processos com a anuência prévia e formal do Diretor do Departamento de Tecnologia e Processos, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

    I – Escopo (dados digitais a serem salvaguardados);

    II – Tipo de *backup* (completo, incremental, diferencial);

    III – Frequência temporal de realização do backup (diária, semanal, mensal, anual);

    IV – Retenção;

    V – RPO (ponto em uma linha de tempo em que o s dados devem ser recuperados após a ocorrência de uma ruptura);

    VI – RTO (período de tempo dentro do qual os níveis mínimos dos serviços e/ou sistemas devem ser recuperados após a ocorrência de uma interrupção).

16. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao funcionário responsável pela manutenção dos backups. A aprovação para execução da alteração depende da anuência do Diretor do Departamento de Tecnologia e Processos.

17. Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

**Tipo de backup**

I – Completo (*full*);

II – Incremental;

III – Diferencial.

Salvo indicação em contrário, o backup dos dados do sistema será feito de acordo com a seguinte programação padrão:

18. Backup incremental diário (segunda a sábado), armazenado no local e em nuvem.
19. Os backups devem ser programados para uma faixa de horário que não afete o horário comercial de funcionamento da PMETT.

**Do uso da rede**

20. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da PMETT, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da PMETT.
21. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.
22. O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a área técnica responsável pela administração da rede de dados da PMETT.

**Do transporte e armazenamento**

23. As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

    I – A criticidade do dado salvaguardado;

    II – O tempo de retenção do dado;

    III – A probabilidade de necessidade de restauração;

    IV – O tempo esperado para restauração;

    V – O custo de aquisição da unidade de armazenamento de backup;

    VI – A vida útil da unidade de armazenamento de backup.
24. O administrador de backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.
25. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.
26. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.
27. No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo, 30 dias. Após esse período os arquivos poderão ser excluídos a qualquer tempo.
28. As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso

restrito a pessoas autorizadas pelo administrador de backup. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

29. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

As midias de backup serão transportadas e armazenadas conforme descrito neste documento:

- Todos os backups serão gravados em mídias reutilizáveis, SSDS OU HDDS.
- A mídia será claramente identificada e armazenada em uma área segura acessível apenas para pessoa(s) autorizada(s) ou o fornecedor de armazenamento seguro de mídia externo, contratado pela PMETT.
- A mídia não será deixada sem supervisão durante o transporte.
- Backups diários completos dos bancos de dados e incrementais de arquivamentos, serão mantidos por 1 semana e armazenado no local e na nuvem.
- Backups completos anuais dos dados arquivados serão mantidos por 3 anos. Após esse período, as midias serão reutilizadas ou destruídas.

**Dos testes de backup**

30. Os backups serão verificados periodicamente:
    - Diariamente os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.
    - Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.
    - A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política.
    - Os testes devem ser realizados em todos os backups produzidos independente do ambiente.
31. Os testes de restauração dos backups devem ser realizados, por amostragem uma vez ao mës, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos.
32. Verificar se foi atendido os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.
33. Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso
34. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo comitê de gestão de políticas de TI.

**Procedimento de restauração de backup**

35. O atendimento de solicitações de restauração de arquivos, e-mails e demais formas de dados deverá obedecer às seguintes orientações:

    a. A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de chamado técnico utilizando a ferramenta/sistema que for o padrão de aberturas do tipo na PMETT naquele momento.

    b. A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.

    c. A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.

    d. O operador de backup terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

36. O cronograma de restauração de dados:

    a. O tempo de restauração é proporcional ao volume de dados necessários para a restauração. As estimativas a seguir são do tempo de atendimento do Departamento de Tecnologia e Processos, não contemplando o tempo antes ou após o pedido a equipe:

        - A cada 1 GB de dados de arquivos compartilhados não criptografados, o tempo de restauração é de 30 minutos.
        - A cada 1GB de dados de bancos de dados de sistemas, o tempo de restauração é de 1 hora.
        - A cada 1GB de dados de arquivos compartilhados criptografados, o tempo de restauração é de 90 minutos.

    b. Backups externos serão disponibilizados em aproximadamente 1 dia de uma falha catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um;

    c. Backups externos serão disponibilizados em aproximadamente 4 horas de uma falha não catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um.

37. A restauração de dados seguirá as seguintes diretrizes:

    a) Será realizada em uma estação dedicada a essa tarefa.

    b) Restaurações não críticas serão realizadas fora de horário de expediente.

    c) O processo deverá ser documentado quanto a seu inicio, termino e ocorrências quando houver.

**Do Descarte da Mídia**

38. A mídia de backup será retirada e descartada conforme descrito neste documento:

    a. A TI garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.

b. A TI garantirá a destruição física da mídia antes do descarte.

c. Uma vez destruída a mídia, esta será encaminhada para o setor responsável por descarte de lixo eletrônico.

**Das Responsabilidades**

39. O administrador de backup e o operador de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

São atribuições do administrador de backup:

I – Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela organização;
II – Providenciar a criação e manutenção dos backups;
III – Configurar as soluções de backup;
IV – Manter as unidades de armazenamento de backups preservadas, funcionais e seguras;
V – Definir os procedimentos de restauração e neles auxiliar;

## Não conformidade

Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

1. Processo Administrativo Disciplinar de acordo com a legislação aplicável
2. Exoneração.
3. Ação judicial de acordo com as leis aplicáveis e acordos contratuais.
4. Rescisão contratual ao bem do serviço público.

# Concordância

Eu li e entendi a Política de Backup e Restauração de Dados Digitais do PMETT. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais e/ou disciplinares de acordo com as leis aplicáveis e as normas internas da PMETT.

_____
Nome do Servidor/Empregado

_____
Assinatura do funcionário Data