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

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:

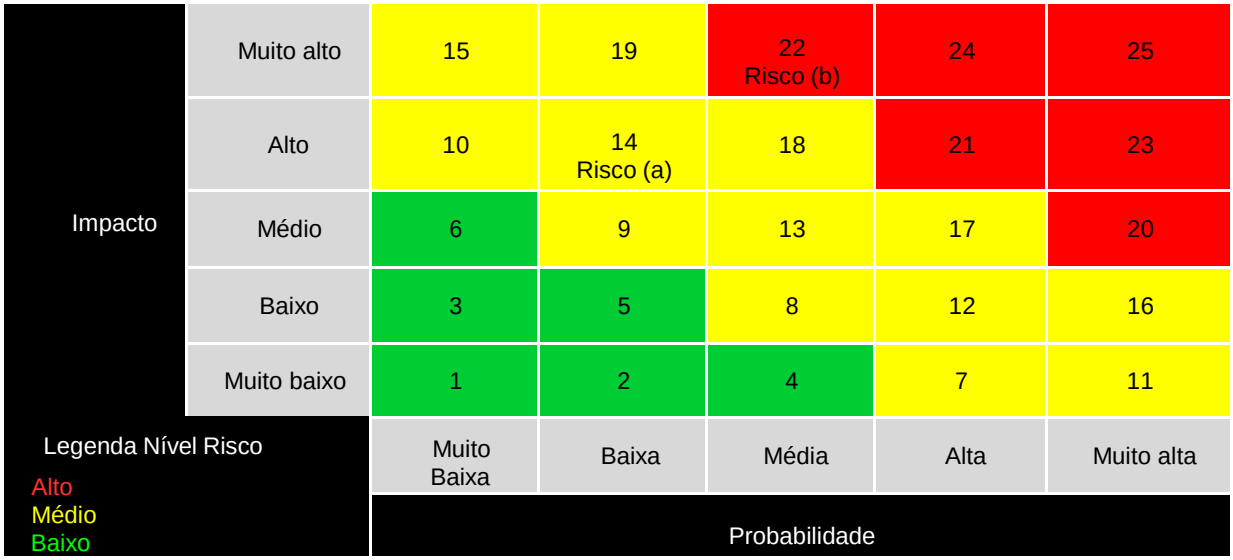

Figura 1: Matriz probabilidade e impacto

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.

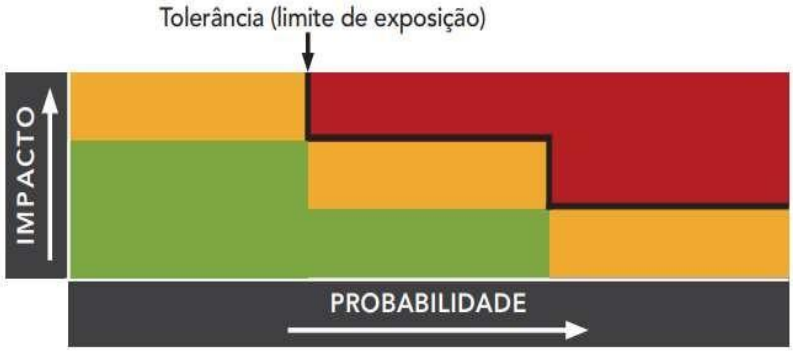

Figura 2: Matriz de avaliação dos riscos

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. Teste de backup.	Backups remotos e em serviços de nuvem. 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. Danos ao hardware de servidores. 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. Perda de dados críticos. Comprometimento de todos os dados da rede.	Baixa	Muito Alto	19	Boas soluções de antivirus pago nos servidores. Backups.	Boa solução de antivirus pago em todas as maquinas clientes. Backup frio periodico. 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. 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. Perda de dados críticos	Baixa	Alto	14	Raid 0. Backup variados.	Discos rigidos sobressalentes. 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. 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. Backups mais frequentes	T.I.		NAO	Muito Baixa	Alto	10
Datacenter da PMETT	Houvesse um incendio	Interrupção de serviços essenciais. 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.