Prefeitura do Município de Pariquera-Açu
Estado de São Paulo
Rua XV de Novembro, 686, Centro - Pariquera-Açu CEP: 11.930-000
Fone: (13) 3856-7100 E-mail: gabinete@pariqueraacu.sp.gov.br

Gerenciamento de Riscos de TI

PROGRAMA DE PRIVACIDADE E SEGURANÇADA INFORMAÇÃO

GERENCIAMENTO DE RISCOS DE TI

Versão 1.0
Pariquera-Açu, Agosto de 2023

Sumário

Gerenciamento de Risco de TIC

PREFEITURA MUNICIPAL DE PARIQUERA-AÇU

WAGNER BENTO DA COSTA

PREFEITO

DEPARTAMENTO DE ADMINISTRAÇÃO MUNICIPAL

JOÃO BATISTA DE ANDRADE

DIRETOR ADMINISTRATIVO

GESTOR DE TECNOLOGIA DA INFORMAÇÃO

TONE ALEX GUERRA

GESTOR TI

EQUIPE DE ELABORAÇÃO

TONE ALEX GUERRA

EQUIPE REVISORA

SIMONE SILVA MELCHER

MARCELO PIO PIRES

1. Versão, Revisão e Aprovação

Versão	Data	Descrição	Responsável
1.0	17/08/2023	Criação da versão para divulgação.	Tone Alex Guerra

2. Apresentação

O Plano de Gerenciamento de Risco (PGR) ou Programa de Gerenciamento de Risco é um documento técnico composto por um diagnóstico da situação da empresa em relação aos riscos e medidas para evitá-los ou minimizá-los, com o cronograma de adequação.

a) Princípios do Gerenciamento de Riscos

O gerenciamentos de risco visa orientar ações de forma eficiente, eficaz e contínua através da comunicação mensurada de seu valor, intenção e propósito.

A ISO 31000:2018 em seu item 4, apresenta com objetivo da gestão de risco:

“O propósito da gestão de riscos é a criação e proteção de valor. Ela melhora o desempenho, encoraja a inovação e apoia o alcance de objetivos”

Para isso, a 31000 propõe 8 princípios básicos. Segundo a norma, eles são “a base para gerenciar riscos e convém que sejam considerados […]”. Abaixo, segue figura retirada da própria 31000.

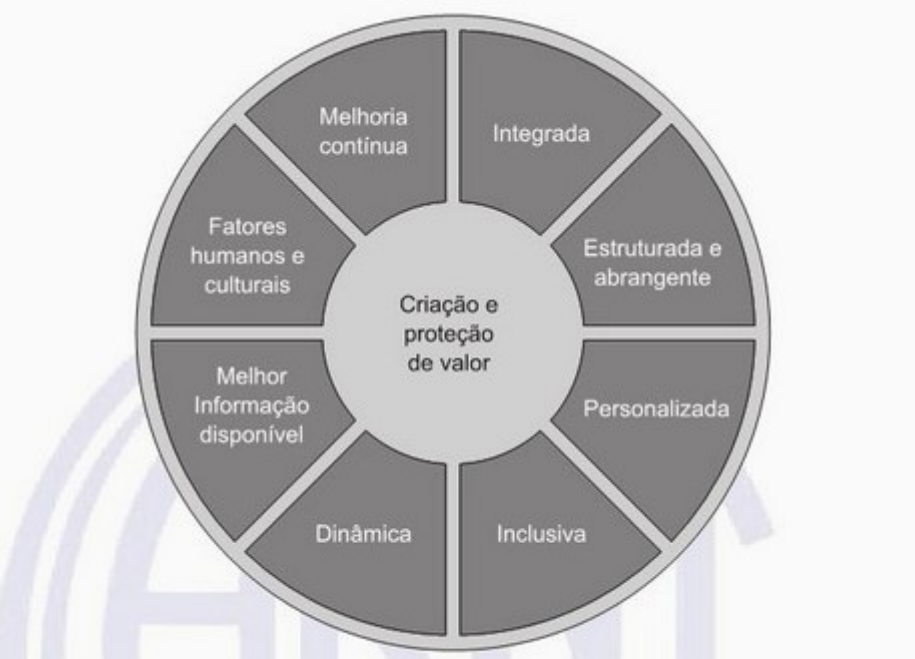

Figura 2 – Princípios

Fonte: ISO 31000:2018

i. Integrada;

A gestão de riscos deve ser vista como "parte integrante" de TODOS os processos e atividades da empresa e não de um serviço ou aréa específico.

ii. Estruturada e Abrangente;

Deve ser claro em definir os processos bem como abrangente, contribuindo para haja resultados mensuráveis, consistentes e comparáveis.

iii. Personalizada;

É adaptativa aos objetivos da organização ou ao contexto em que é submetida, tornando-a adequada ao alcance da exiquibilidade.

iv. Inclusiva;

Sempre deve estar aberta à incluir partes interessadas na gestão de riscos, tornando-a cada vez mais fundamentada, aumentando os níveis de conscientização dos colaboradores.

v. Dinâmica;

Riscos mudam, sejam fatores internos ou externos. Por isso uma boa gestão deve passar por revisão compreendendo novos riscos, ou revalidando impactos de riscos já conhecidos.

vi. Melhor Informação Disponível;

Para uma boa tomada de decisão é necessário que esta seja tomada com base em dados e fatos, por isso, as entradas para uma boa gestão de riscos deve se basear em um cenário real atual, bem como em expectativas futuras.

vii. Fatores Humanos e Culturais;

Sem dúvidas, gerir riscos é saber lidar com pessoas. O comportamento e a cultura influenciam significativamente todos os aspectos de riscos em cada nível e estágio.

viii. Melhoria Contínua;

Para que cada vez mais a gestão de risco cumpra seu papel sendo preditiva, crinando valor, é preciso que ela se adapte, evolua e melhore sempre. E isso é feito através da expertize adquirida pelas experiências, sejam de boas práticas de mercado externo ou principalmente pela resultante das próprias demandas aprendidas dentro da própria empresa.

3. Processo do Gerenciamento de Riscos

O processo do Gerenciamento de Riscos da PMPA, será estabelecido conforme as seguintes etapas:

- Definição de Contexto;
- Processo de Avaliação de Riscos;
- Tratamento de Riscos

- Monitoramento e Análise Crítica;
- Comunicação e Consulta;

a) Definição de Contexto

Nesta primeira etapa para elaboração do plano de gerenciamento de riscos, deve-se compreender o ambiente no qual o trabalho será desenvolvido, definir escopo e critérios a serem considerado no processo da gestão. Para isso, a equipe busca reconhecer todos os processos atividades e serviços críticos sujeitas a vulnerabilidades de forma que os riscos possam ser gerenciados.

b) Processo de Análise e Avaliação de Riscos

A avaliação de riscos de tecnologia da informação consiste em uma segunda etapa, onde após reconhecidos os processos, submetê-los à:

- Identificação de riscos;
  - São determinados os eventos que podem causar perdas potenciais;
- Análise de riscos;
  - Determina-se a probabilidade de ocorrência dos eventos;
- Avaliação de riscos.
  - Ordena os riscos de acordo com os critérios de avaliação estabelecidos na definição de contexto

i. Identificação de riscos

Uma vez conhecidos os processos críticos que compreendem riscos à execução integrada da atividade, deve-se identificar os ativos de TI que suportam a execução desses serviços críticos. Tal atividade dá início à etapa de identificação de riscos de TI.

Ameaças e vulnerabilidades associadas a cada ativo que suporta um serviço crítico, devem ser levantadas, permitindo uma identificação mais apropriada dos riscos de TI

Ativo é qualquer elemento com valor para a organização que necessite de proteção. A entrada desse processo são os resultados da etapa de definição do escopo, a ação a ser realizada é o desenvolvimento da atividade de identificação dos ativos. É importante definir “quem é o seu responsável?” por determinado ativo.

Além disso, os ativos dividem-se em primários, processos e atividades de negócios e a informação e ativos de suporte e infraestrutura, são compostos por elementos físicos (hardware) que suportam os processos, programas (software) que contribuem para a operação de um sistema, aplicações de negócios, dispositivos de telecomunicações (redes), recursos humanos, instalações físicas, entre outros.

ii. Análise de riscos

Cada item idenficado na etapa anterior é submetido à avaliação de propabilidade e impacto, **definindo assim o nível do risco** para o ativo.

Probalibidade: chance do evento ocorrer dentro de um prazo previsto. Para estimar a probabilidade será utilizada uma escala qualitativa de cinco níveis:

Escala de Probabilidade	
Improvável	Acontece apenas em situações excepcionais. Não há histórico conhecido do evento ou não há indícios que sinalizem sua ocorrência.
Remoto	O histórico conhecido aponta para baixa frequência de ocorrência no prazo associado ao objetivo.
Ocasional	Repete-se com frequência razoável no prazo associado ao objetivo ou há indícios que possa ocorrer nesse horizonte.
Provável	Repete-se com elevada frequência no prazo associado ao objetivo ou hámuitos indícios que ocorrerão nesse horizonte.
Frequente	Ocorrência quase garantida no prazo associado ao objetivo.

Impacto: o impacto mensura 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 do objetivo/resultado.

Nível de Risco: o nível de risco é calculado através do cruzamento combinatório das escalas de probabilidade e de impacto.

Abaixo temos a matriz estabelecida

IMPACTO	**Muito Alto**	15	19	22	24	25
	Alto	10	14	18	21	23
	Médio	6	9	13	17	20
	Baixo	3	5	8	12	16
	Muito Baixo	1	2	4	7	11
Legenda Nível de Risco		**Improvável**	**Remoto**	**Ocasional**	**Provável**	**Frequente**
Alto		**PROBABILIDADE**				

Médio Baixo	

Para um bom uso da matriz de nível de risco, vamos considerar alguns fatores relevantes:

- O impacto é a dimensão mais importante de um evento. Portanto um alto impacto para um evento de probabilidade improvável, deve preocuar o gestor muito mais do que o oposto (impacto baixo com probabilidade frequente).
- Atribuição de valores arbitrários ou irreais: matrizes que "normatizam" o risco por soma ou multiplicação, ocasionam distorção analítica por simetria, considerando mesmo impacto e probabilidade dentro de um mesmo nível.

Note a relação:

impacto muito baixo - probabilidade frequente : 11

impacto muito alto- probabilidade improvável: 15

Se tivessemos uma relação escalar simétrica, ambos teriam valoração iguais.

iii. Avaliação de riscos

A fase de avaliação de riscos é auxiliar nas decisões tendo como base os resultados da análise de riscos. Esta fase da gestão de riscos tem por objetivo comparar os níveis de riscos identificados na fase anterior com os critérios de avaliação e aceitação de riscos. Estes critérios são definidos durante a definição do contexto e deverão estar alinhados aos objetivos da organização.

Nesta fase a equipe de análise junto a organização devem comparar os riscos estimados com os critérios de avaliação definidos durante a fase de contexto. A organização deverá tomar as decisões desta fase com base no nível de risco aceitável. Porém, fatores como consequências, probabilidade e confiança também deverão ser considerados para melhor orientar as tomadas de decisão.

c) Tratamento e Aceitação 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 PMPA é composta pelas opções: modificar o risco, aceitar o risco, evitar o risco e compartilhar o risco, conforme descrito na tabela a seguir:

Tratamento e Resposta 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.

d) 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.

e) 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 da transparência. A comunicação consiste no envio periódico das informações disponibilizadas na consulta para todos os envolvidos.

4. Recursos

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

5. Papéis e Responsabilidade

Para gestão do processo de gerenciamento de riscos de TI, deve-se instituir uma comissão, que se reunirá periodicamente para planejamento e execução na identificação, análise, resposta e produção do resultante do processo de gerenciamento de riscos.

Sugere-se como parte integrante da comissão:

- Gestor de Tecnologia da Informação;
- Integrante representante técnico administrativo do Departamento de Saúde;
- Integrante representante técnico administrativo do Departamento de Educação;

6. Conclusão

A gestão de riscos é um processo que sempre trará benefícios para a organização. A melhoria das condições de segurança dos ativos passa obrigatoriamente pelo conhecimento das fraquezas e vulnerabilidades que podem ser exploradas para que as ameaças se concretizem e a melhor forma de fazer isso é através da gestão de riscos.

A gestão em si não é um processo individual separado das principais atividades e processos da organização. A gestão faz parte das responsabilidades da administração e é parte integrante de todos os processos organizacionais, incluindo o planejamento estratégico e todos os processos de gestão de projetos e gestão de mudanças [ISO 31000]. Dessa forma, é fundamental que os gestores lidem com a gestão de riscos de TIC como meio para alcançar os objetivos e efetuar as diretrizes propostas na missão, visão e valores da organização.

Assim como a implementação dos controles internos neste plano descritos, quando devidamente implementada na Prefeitura Municipal de Pariquera-Açu, se apresenta como um elemento essencial para a boa governança. Porém deve-se ressaltar que um processo bem estruturado de gerenciamento de riscos não está totalmente imune a incertezas, mas certamente o impacto e a probabilidade de eventuais riscos e ameaças serão substancialmente reduzidos.

7. Anexo I

Para elaboração do projeto resultante do desenvolvimento do Processo de Gerenciamento de Riscos, utilizar-se-á a Ferramenta What IF, que por ser genérica possibilita a adaptação afim de atender a apresentação do resultado das análises de risco.

Abaixo segue modelo com dados de exemplo do preenchimento e uso da Ferramenta What IF

	1 a 6 = Risco Baixo		7 a 19 = Risco Médio		20 a 25= Risco Alto

Serviços / Sistemas	E se	Efeito	Probabilidade	Impacto	Risco	Controles Atuais	Ações Recomendadas	Resp	Prazo	Implantado	Prob. Residual	Impac. Residual	Risco Residual
Base de Dados Criticas	Ocorrer perda dos dados sem possibilidade de recuperação	Interrupção de serviços essenciais. Perda de dados críticos	Ocasional	Muito Alto	22	Realização de Backup Local	Backups Remotos e em serviços de Núvem	TI		SIM	Improvável	Médio	6
Estações Cliente/Desktop	Surgisse um ransoware em um ou mais equipamentos	Interrupção de serviços essenciais. Perda de dadps críticos. Comprometimento de todos os dados da rede	Ocasional	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	TI		NÃO	Improvável	Alto	10

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 Ataque ransoware.

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.