

PDTIC

2023

**Plano
Diretor de
Tecnologia da
Informação e
Comunicação**

emgea
empresa gestora de ativos



HISTÓRICO DE REVISÃO

Data	Versão	Descrição	Documento Autorizativo
23/06/2023	1.0	Versão original	Nota Técnica nº 278/2023 - SUTEC aprovado pelo Conselho de Administração em 29.6.2023 (Ata nº 278/2023)

Brasília, 23 de junho de 2023

SUMÁRIO

1. APRESENTAÇÃO	4
1.1. OBJETIVO DO PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PDTIC	4
1.2. VIGÊNCIA DO PDTIC	4
1.3. ELABORAÇÃO E APROVAÇÃO	4
1.4. CLASSIFICAÇÃO DA INFORMAÇÃO	4
2. O MODELO DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO DA EMGEA.....	5
3. METODOLOGIA DE ELABORAÇÃO DO PLANEJAMENTO ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO	5
4. ANÁLISE DE AMBIENTE.....	7
5. INVENTÁRIO DAS NECESSIDADES	9
6. OBJETIVOS ESTRATÉGICOS DE TECNOLOGIA DA INFORMAÇÃO E INICIATIVAS ESTRATÉGICAS	9
7. ANÁLISE DE RISCOS	10
8. MONITORAMENTO: METAS E INDICADORES DE DESEMPENHO	10

1. APRESENTAÇÃO

1.1. Objetivo do Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC

O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) tem como objetivo relacionar as ações de tecnologia da informação a serem realizadas no ano de 2023, necessárias para o cumprimento das iniciativas estratégicas e atingimento dos objetivos estratégicos da Empresa, em alinhamento com o Planejamento Estratégico da EMGEA para 2023.

1.2. Vigência do PDTIC

Este PDTIC tem validade para o ano de 2023, alinhado com o Planejamento Estratégico da Empresa para o mesmo período.

Caso, eventualmente, alterações no cronograma posterguem a alienação das carteiras para além do previsto, uma nova revisão do PDTIC deverá ser efetuada, em linha com o novo Planejamento Estratégico de Tecnologia da Informação.

1.3. Elaboração e Aprovação

O PDTIC é elaborado pela Superintendência de Tecnologia (SUTEC), apreciado preliminarmente pelo Comitê Gestor de Tecnologia da Informação (CGTI) e, na sequência, pelo Comitê Executivo de Tecnologia da Informação (CETI), que o encaminha para a Diretoria Executiva da EMGEA, a quem compete a aprovação.

Após aprovação, uma versão resumida do PDTIC será publicada no sítio da EMGEA (www.emgea.gov.br > A Empresa > Governança de TI).

1.4. Classificação da Informação

Versão completa: #I – Interno

Versão resumida a ser publicado no sítio: #P - Público

2. O MODELO DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO DA EMGEA

Para o gerenciamento dos ativos e dos serviços de tecnologia da informação, a Empresa conta com uma infraestrutura alinhada com às ferramentas utilizadas no mercado. Essa estrutura permite a produção e a otimização de ferramentas para o suporte à gestão dos seus processos e produtos, além do monitoramento de sistemas, serviços e ativos utilizados no ambiente de tecnologia.

O modelo de governança de TI adotado pela EMGEA possui em sua estrutura a Superintendência de Tecnologia (SUTEC), unidade organizacional responsável pela gestão do processo de tecnologia da informação, subordinada à Diretoria de Administração (DIRAD), e com três Comitês, que atuam como órgãos de apoio à gestão: Comitê Executivo de Tecnologia da Informação (CETI), Comitê Gestor de Tecnologia da Informação (CGTI) e Comitê de Segurança da Informação, Proteção de Dados Pessoais e Privacidade (CSI), cujas competências estão definidas em seus respectivos Regimentos Internos.

A SUTEC é composta por três Gerências: Gerência de Manutenção de Sistemas (GEDES), Gerência de Inovação e Desenvolvimento de Sistemas (GERIN) e Gerência de Redes e Suporte (GERED), com competências definidas no Regimento Interno da EMGEA.

Os colaboradores lotados na GERED compõem a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR, cuja missão é facilitar e coordenar as atividades de prevenção, tratamento e resposta a incidentes na rede computacional da EMGEA, assim como coordenar a recuperação de sistemas, a análise de ataques e intrusões e a cooperação com outras equipes (Normativo de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - SI.NOR.005).

A ETIR tem o seguinte escopo de atuação:

- a) comunicar qualquer incidente de segurança da informação à Diretoria Executiva e ao CSI; e
- b) reportar os incidentes de segurança da informação detectados ao Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov.

3. METODOLOGIA DE ELABORAÇÃO DO PLANEJAMENTO ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO

A elaboração do Planejamento Estratégico de Tecnologia de Informação teve como premissa o alinhamento com o Planejamento Estratégico da EMGEA, de forma que os objetivos, as iniciativas e as ações de TI contribuam para a consecução dos objetivos previstos no Planejamento Estratégico da Empresa.

No Planejamento Estratégico de 2023 foram definidos os seguintes pilares estratégicos, conforme Nota Técnica nº 255/2023 ASSES #I:

Gestão de Ativos e Sustentabilidade Financeira	
Norteadores e Pilares Estratégicos 2023	
Finanças	1. VIABILIZAR O INGRESSO DE RECURSOS FINANCEIROS QUE PERMITAM A SUSTENTABILIDADE ECONÔMICA E FINANCEIRA.
Processos	2. REDESENHAR OS PROCESSOS VISANDO A EFICIÊNCIA OPERACIONAL
Clientes	3. PROMOVER AMBIENTE DE ATENDIMENTO QUE MAXIMIZE OS RESULTADOS DO RELACIONAMENTO COM OS CLIENTES
Pessoas	4. PROMOVER A AQUISIÇÃO DE COMPETÊNCIAS PARA ATUAÇÃO ADEQUADA AOS PROCESSOS

Observada a premissa de alinhamento com os objetivos estratégicos definidos para 2023, o trabalho de elaboração do Planejamento Estratégico de Tecnologia de Informação foi realizado em etapas sequenciais:

- análise do ambiente;
- inventário das necessidades;
- definição dos objetivos estratégicos de TI e respectivas iniciativas estratégicas.

Nessas etapas, foram utilizados como referenciais teóricos:

- **Balanced Scorecard - BSC:** ferramenta de gestão organizada em quatro perspectivas: Financeira, Cliente, Processos Internos e Aprendizagem e Crescimento.
- **Técnica SWOT:** ferramenta que permite realizar a análise do cenário externo e interno. A palavra SWOT é um acrônimo formado pelas palavras inglesas Strengths (forças), Weaknesses (fraquezas), Opportunities (oportunidades) e Threats (ameaças).
- **Matriz RECI:** ferramenta utilizada para definir papéis e responsabilidades em projetos e processos multifuncionais ou departamentais. O RECI é um acrônimo derivado das quatro principais responsabilidades mais comumente usadas: Responsável, Executor, Consultado e Informado.
- **5W2H:** técnica composta por perguntas que devem ser feitas e respondidas ao investigar e relatar um fato ou situação, sendo aplicável às mais variadas atividades profissionais. O termo é um acrônimo em inglês derivado de Who? (Quem?), What? (O quê?), Where? (Onde?), When? (Quando?), Why? (Por que?), How? (Como?) e How Much? (Quanto?).

- **Cobit 5.0:** framework focado no que é necessário para atingir um adequado controle e gerenciamento de TI, relacionando os objetivos de TI aos objetivos corporativos.
- **ITIL v4:** ITIL® (Information Technology Infrastructure Library) framework para gerenciamento de serviços de TI (ITSM) adotado mundialmente.
- **Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709, de 14.8.2018:** dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
- **Decreto nº 9637, de 26.12.2018, alterado pelo Decreto 10.641, de 2.3.2021:** institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação, abrangendo cibersegurança.
- **Norma ISO/IEC 27001:** estabelece um padrão para sistema de gestão da segurança da informação. A norma foi elaborada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).
- **Instrução Normativa GSI/PR Nº 1, de 27.5.2020:** dispõe sobre a Estrutura de Gestão da Segurança da Informação e estabelece as instruções para implementação da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) nos órgãos e nas entidades da Administração Pública Federal.
- **Resolução CGPAR nº 41, de 4.8.2022** - Estabelece diretrizes e parâmetros para implementação, desenvolvimento e aperfeiçoamento da Governança de Tecnologia da Informação e Comunicação nas empresas estatais federais.
- **Ofício nº 119-TCU de 14.3.2023** - Relatório Individual de Auto avaliação com os resultados dessa organização relativos ao acompanhamento dos controles críticos de segurança cibernética das organizações públicas federais.

4. ANÁLISE DE AMBIENTE

Para subsidiar a definição dos objetivos estratégicos de TI foi realizada uma análise dos fatores externos à EMGEA (ambiente externo), bem como uma análise de fatores existentes na própria Empresa (ambiente interno), que podem influenciar a execução das estratégias organizacionais.

No quadro abaixo estão relacionados os fatores identificados no ambiente externo, que podem influenciar positivamente (“oportunidades”) e negativamente (“ameaças”); e no ambiente interno, que podem influenciar positivamente (“forças”) e negativamente (“fraquezas”).

Ambiente Externo

OPORTUNIDADES

- Utilização de serviços especializados de fornecedores.
- Utilização de tecnologias inovadoras emergentes.
- Utilização das melhores práticas de mercado em Tecnologia da Informação.

AMEAÇAS

- Instabilidade político-econômica.
- Descontinuidade de serviços por parte de fornecedores.
- Desastre natural, acidente, sabotagem ou vandalismo.
- Perda de colaboradores-chave.
- Rotatividade de colaboradores.

FORÇAS

- Patrocínio da alta administração.
- Comitês de TI atuantes.
- Política de Segurança da Informação documentada, divulgada na organização.
- Arquitetura da Informação implementada.
- Alto grau de integração dos sistemas corporativos.
- Utilização das melhores práticas em Governança de TI.
- Equipe multidisciplinar, com conhecimento sobre os produtos e serviços da empresa.

FRAQUEZAS

- Dificuldade de conclusão de todos os sistemas vinculados à gestão decorrente da internalização dos créditos.
- Dificuldade para atendimento célere de todas as solicitações de soluções de TI recebidas, face à quantidade de solicitações.
- Contingenciamento do orçamento de TI para capacitação e investimentos no parque tecnológico.
- Infraestrutura tecnológica defasada para suportar novos negócios.

Ambiente Interno

5. INVENTÁRIO DAS NECESSIDADES

Tendo como referencial os objetivos definidos no Planejamento Estratégico da EMGEA para 2023, e considerados os resultados da análise dos ambientes externo (oportunidades e ameaças) e interno (forças e fraquezas), foi realizado o levantamento das necessidades de tecnologia da informação para alcance dos objetivos estratégicos da Empresa.

Foram também utilizados como insumos para o levantamento das necessidades de TI:

- Demandas existentes para a manutenção e desenvolvimento de sistemas;
- Demandas para aquisição de *hardware* e *software*;
- Política de Segurança da Informação;
- Relatório do Mapeamento de Riscos e Controles de TI;
- Relatórios de Auditoria Interna e Externa.

Realizado o levantamento, foram identificadas as seguintes necessidades de TI:

Relação das Necessidades de TI	
N01	Melhoria na Gestão de Serviços, de Nível de Serviço e de Qualidade.
N02	Atualização e manutenção do parque tecnológico.
N03	Atualização da Política de Segurança da Informação.
N04	Aprimoramento do monitoramento e gerenciamento do ambiente de TI.
N05	Aprimoramento das soluções tecnológicas para sustentar o negócio.
N06	Aprimoramento da plataforma de negócios para viabilizar a integração com soluções de terceiros.
N07	Aprimoramento dos mecanismos de rastreamento de dados - Lei Geral de Proteção de Dados Pessoais (LGPD).
N08	Aprimoramento dos mecanismos de segurança cibernética (<i>Cibersegurança</i>).

6. OBJETIVOS ESTRATÉGICOS DE TECNOLOGIA DA INFORMAÇÃO E INICIATIVAS ESTRATÉGICAS

Levantadas as necessidades de tecnologia da informação para alcance dos objetivos estratégicos da EMGEA para 2023 foram mantidos os 3 (três) objetivos estratégicos de TI (OETI):

- **OETI 01:** Prover e disponibilizar soluções de TI para os negócios da Empresa e sustentabilidade financeira;
- **OETI 02:** Aprimorar a segurança da informação, com vistas a assegurar disponibilidade, integridade, confidencialidade e autenticidade das informações corporativas;
- **OETI 03:** Aprimorar a capacitação dos colaboradores para o desenvolvimento e utilização das soluções de TI.

Para cada objetivo estratégico de TI foram definidas iniciativas estratégicas, indicando as diretrizes para alcançar os objetivos.

<i>OETI 01 – Prover e disponibilizar soluções de TI para os negócios da Empresa e sustentabilidade financeira.</i>	
<i>Iniciativas Estratégicas</i>	
Iniciativa 1.1	Promover a melhoria contínua dos serviços de TI.
Iniciativa 1.2	Manter e desenvolver (ou adquirir) novas aplicações para atendimento às necessidades da EMGEA.
<i>OETI 02 – Aprimorar a segurança da informação, com vistas a assegurar disponibilidade, integridade, confidencialidade e autenticidade das informações corporativas.</i>	
<i>Iniciativas Estratégicas</i>	
Iniciativa 2.1	Promover a melhoria contínua dos mecanismos de segurança da informação.
<i>OETI 03 – Aprimorar a capacitação dos colaboradores para o desenvolvimento e utilização das soluções de TI.</i>	
<i>Iniciativas Estratégicas</i>	
Iniciativa 3.1	Aprimorar a capacitação dos colaboradores da área de TI.
Iniciativa 3.2	Aprimorar a capacitação dos colaboradores da EMGEA para uso das soluções de TI.

7. ANÁLISE DE RISCOS

Utilizando a metodologia¹ de gestão de riscos adotada pela EMGEA e a Matriz de Riscos² relativa ao processo “Gestão de Tecnologia da Informação”, foram mapeados os eventos de risco que podem comprometer a execução do Planejamento Estratégico de Tecnologia da Informação, com os respectivos graus de exposição³, nas situações inerente (risco existente na ausência de qualquer medida de controle) e residual (risco que remanesce após a adoção de medidas de controle). Esses eventos estão relacionados no Anexo I.

8. MONITORAMENTO: METAS E INDICADORES DE DESEMPENHO

O cumprimento dos Objetivos Estratégicos de TI definidos no PDTIC será monitorado com a definição das seguintes metas e indicadores de desempenho para o exercício de 2023.

Trimestralmente, será reportado ao CGTI o relatório de acompanhamento dos indicadores do PDTIC elaborado pela SUTEC.

¹ Metodologia de mapeamento de riscos baseada na ISO 31000 e no COSO - Gerenciamento de Riscos Corporativos Integrado com Estratégia e Performance.

² Matriz de Riscos: modelo matemático por meio do qual, a partir das atividades relacionadas a cada processo e dos respectivos eventos e fatores de risco levantados, são apurados os níveis dos riscos incidentes, graduando-os em uma escala com graus de exposição (extremo, alto, médio ou baixo), considerando os níveis de probabilidade (possibilidade de ocorrência de um determinado evento de risco) e de impacto (efeito da ocorrência do evento de risco).

³ Grau de Exposição: medida utilizada para expressar o resultado da combinação da probabilidade e do impacto da ocorrência de um risco.

OETI 01 – Prover e disponibilizar soluções de TI para os negócios da Empresa e sustentabilidade financeira.

Indicador	O que mede	Periodicidade	Meta
Índice de execução das ações previstas no PDTIC, relacionadas ao OETI 01	Mostra o percentual de execução das ações previstas no PDTIC, relacionadas ao OETI 01.	Anual	85%

OETI 02 – Aprimorar a segurança da informação, com vistas a assegurar disponibilidade, integridade, confidencialidade e autenticidade das informações corporativas.

Indicador	O que mede	Periodicidade	Meta
Índice de execução das ações previstas no PDTIC, relacionadas ao OETI 02	Mostra o percentual de execução das ações previstas no PDTIC, relacionadas ao OETI 02.	Anual	66%

OETI 03 – Aprimorar a capacitação dos colaboradores para o desenvolvimento e utilização das soluções de TI.

Indicador	O que mede	Periodicidade	Meta
Índice de execução das ações previstas no PDTIC, relacionadas ao OETI 03	Mostra o percentual de execução das ações previstas no PDTIC, relacionadas ao OETI 03.	Anual	75%

PDTIC – Plano Diretor de Tecnologia da Informação e Comunicação

Indicador	O que mede	Periodicidade	Meta
Índice de execução das ações previstas no PDTIC 2023	Mostra o percentual de execução das ações previstas no PDTIC 2023.	Anual	80%



Anexo I - Eventos de Riscos

Risco	Eventos de riscos	Grau de exposição		Ações de mitigação
		Inerente	Residual	
Risco de compras e contratações	Aquisição de bens inadequados ou de baixa qualidade.	MÉDIO	BAIXO	<ul style="list-style-type: none">▪ Rotina de elaboração, revisão e aprovação de projetos básicos e termos de referência para aquisição de bens ou contratação de serviços de TI.▪ Normatização de compras e contratações - Regulamento de Licitações e Contratos Administrativos (LG.NOR.008).▪ Fiscalização de contratos para monitoramento da qualidade dos serviços prestados e/ou dos produtos fornecidos.
	Contratação de serviços inadequados ou de baixa qualidade.	MÉDIO	BAIXO	
	Suspensão ou cancelamento de procedimentos licitatórios.	MÉDIO	BAIXO	
Risco de conformidade	Inobservância de normas externas.	ALTO	BAIXO	<ul style="list-style-type: none">▪ Treinamento.▪ Repasse de conhecimento para os demais colaboradores.▪ Atualização de políticas e normas internas.▪ Monitoramento do ambiente regulatório.
	Inobservância de normas internas.	ALTO	BAIXO	
	Falha humana.	ALTO	BAIXO	
	Divulgação de informações incorretas ou incompletas ao público interno.	MÉDIO	BAIXO	
	Inadequação da quantidade de licenças de software.	ALTO	MÉDIO	
Risco de governança	Desalinhamento de planejamento estratégico de tecnologia da informação com o planejamento estratégico institucional.	ALTO	BAIXO	<ul style="list-style-type: none">▪ Reorganização e reprogramação das ações do PDTIC em caso de alteração do Planejamento Estratégico da EMGEA.▪ Divulgação do PDTIC.▪ Aprovação feito por comitês de TI.
	Falhas nas etapas de identificação, avaliação, resposta, controle, reporte e monitoramento dos riscos.	ALTO	MÉDIO	
Risco de infraestrutura	Falta de espaço para armazenamento de dados, informações e documentos.	ALTO	BAIXO	<ul style="list-style-type: none">▪ Manutenções periódicas dos equipamentos de infraestrutura do Centro de Processamento de Dados – CPD.▪ Sistema de combate a incêndio.▪ Monitoramento do ambiente de infraestrutura.▪ Análise periódica do ciclo de vida dos equipamentos de TI.▪ Atualização periódica dos equipamentos de infraestrutura de TI.
	Inadequação do parque tecnológico.	ALTO	MÉDIO	
	Não atendimento de demandas de suporte técnico ou atendimento intempestivo e/ou com baixa qualidade.	ALTO	BAIXO	
	Falha nos equipamentos de infraestrutura de TI	ALTO	MÉDIO	



Risco	Eventos de riscos	Grau de exposição		Ações de mitigação
		Inerente	Residual	
				<ul style="list-style-type: none"> ▪ Contratação de empresas especializadas na manutenção preventiva e corretiva dos equipamentos de infraestrutura de TI. ▪ Pesquisas de satisfação.
Risco de integridade	Furto/roubo de bens ou valores.	ALTO	MÉDIO	<ul style="list-style-type: none"> ▪ Código de Ética, Integridade e Conduta. ▪ Programa de Integridade. ▪ Controles de acesso às dependências. ▪ Definição de níveis de acesso lógico. ▪ Monitoramento CFTV. ▪ Trilhas de auditoria nos sistemas automatizados. ▪ Inventário físico. ▪ Plantonistas. ▪ Termos de Proteção de Dados, Sigilo e Responsabilidade. ▪ Fiscais de contratos.
	Uso indevido da informação.	ALTO	BAIXO	
	Corrupção.	MÉDIO	BAIXO	
	Fraude nas operações internas.	MÉDIO	BAIXO	
Risco de reputação	Divulgação de informações incorretas ou incompletas ao público externo	ALTO	BAIXO	<ul style="list-style-type: none"> ▪ Código de Ética, Integridade e Conduta. ▪ Programa de Integridade. ▪ Atualização de políticas e normas internas.
Risco de pessoal	Falta de qualificação profissional	MÉDIO	MÉDIO	<ul style="list-style-type: none"> ▪ Repasse de conhecimento para os demais colaboradores. ▪ Formação de sucessores. ▪ Treinamento.
	Perda de colaboradores-chave	ALTO	ALTO	
Risco de segurança da informação	Ataques cibernéticos	ALTO	MÉDIO	<ul style="list-style-type: none"> ▪ Teste de restauração periódico das mídias magnéticas de backup. ▪ Aplicação de contingência dos principais recursos de TI. ▪ Elaboração e implantação de um BIA (<i>Business Impact Analysis</i>) e definição de procedimentos de contingência para processos e aplicações mais críticas de TI. ▪ Elaboração de um Plano de Continuidade da TI. ▪ Controles de acesso às dependências. ▪ Definição de níveis de acesso lógico. ▪ Monitoramento CFTV.
	Ataques de engenharia social	MÉDIO	MÉDIO	
	Inconsistência de dados ou informações	MÉDIO	BAIXO	
	Inserção, alteração ou exclusão de dados / informações	ALTO	BAIXO	
	Perda de documentos e registros	MÉDIO	BAIXO	
	Vazamento de informações estratégicas ou sigilosas	ALTO	MÉDIO	



Risco	Eventos de riscos	Grau de exposição		Ações de mitigação
		Inerente	Residual	
				<ul style="list-style-type: none">▪ Backup de mídias em ambiente externo à Empresa.▪ Divulgação periódica de boas práticas de segurança da informação.▪ Normas e procedimento sobre o uso de informações.▪ Norma de sigilo aplicável a empregados, prestadores de serviços, fornecedores, fornecedores em pré-venda, parceiros e clientes.▪ Utilização de Firewall.▪ Utilização de Antivírus.
Risco de sistemas	Falha na configuração de sistemas.	MÉDIO	BAIXO	<ul style="list-style-type: none">▪ Fiscais de contratos.▪ Validação de bases de dados.▪ Janela de processamento e manutenção.▪ Políticas, normas e procedimentos sobre gestão e desenvolvimento de sistemas.▪ Trilhas de auditoria nos sistemas automatizados.▪ Metodologia para gerenciamento ágil de projetos de software, denominada SCRUM.▪ Documentação de intervenções realizadas em sistemas de terceiros.▪ Ambiente de teste e homologação de sistemas.▪ Formalização de demandas relacionadas à tecnologia.
	Falha no processamento e importação de dados.	MÉDIO	BAIXO	
	Falha na definição de requisitos em sistemas informatizados.	MÉDIO	MÉDIO	
	Falha na transmissão de informações/dados.	MÉDIO	MÉDIO	
	Incompatibilidade de software e hardware.	ALTO	MÉDIO	
	Falha na geração de boletos.	BAIXO	BAIXO	
	Inadequação da estrutura de sistemas.	ALTO	ALTO	
Risco de terceiro	Descontinuidade de prestação de serviços.	MÉDIO	BAIXO	<ul style="list-style-type: none">▪ Instrumentos contratuais.▪ Fiscalização de contrato.▪ Termo de Referência.▪ Edital.
	Falha na prestação de serviços.	MÉDIO	BAIXO	
	Interrupção temporária de prestação de serviços.	BAIXO	BAIXO	
	Falha no tratamento de dados pessoais pelo prestador de serviços.	ALTO	MÉDIO	
	Entrega de bens em desacordo com o contratado.	MÉDIO	BAIXO	
	Prestação de serviço em desacordo com o contratado.	MÉDIO	BAIXO	
Risco orçamentário	Insuficiência de recursos orçamentários	MÉDIO	BAIXO	<ul style="list-style-type: none">▪ Programação orçamentária com base no desdobramento do Planejamento Estratégico organizacional para a TI e na evolução tecnológica.



Risco	Eventos de riscos	Grau de exposição		Ações de mitigação
		Inerente	Residual	
Risco de privacidade	Falha no tratamento de dados pessoais	ALTO	MÉDIO	<ul style="list-style-type: none">▪ Termo de Consentimento; Capacitação de colaboradores da EMGEA▪ Política de Privacidade; Proteção de Dados Pessoais, Sigilo e Responsabilidade;▪ Comitê de Segurança da Informação, Proteção de Dados Pessoais e Privacidade (CSI);▪ Termo de Consentimento; Contratos; Acordos; Convênios; Registros (logs) em sistemas e softwares; SLA para atendimento das demandas via SISADE; Políticas, normas e procedimentos internos.▪ Backup Corporativo; Capacitação de colaboradores da EMGEA▪ Processo administrativo; Programa de Desenvolvimento de Competências
	Não atendimento de demandas dos titulares de dados pessoais ou atendimento intempestivo e/ou com baixa qualidade	ALTO	BAIXO	
	Não comunicação de incidentes de segurança da informação e privacidade ou comunicação intempestiva	MÉDIO	BAIXO	
	Perda ou alteração de dados pessoais	MÉDIO	BAIXO	
	Remoção não autorizada de dados pessoais	ALTO	MÉDIO	
	Tratamento sem consentimento do titular dos dados pessoais	ALTO	BAIXO	
Riscos de Tesouraria	Atraso no pagamento das obrigações	MÉDIO	BAIXO	<ul style="list-style-type: none">▪ Contrato Administrativo; Sistema de Apoio ao Processo de Aquisição de Bens e Serviços - SISPAQ; Fiscal do Contrato