

**PETI**

**2022**

**Planejamento  
Estratégico de  
Tecnologia da  
Informação**



## HISTÓRICO DE REVISÃO

<b>Data</b>	<b>Versão</b>	<b>Descrição</b>	<b>Documento Autorizativo</b>
07/12/2021	1.0	Versão original	Nota Técnica nº 309/2021 - SUTEC aprovada pelo Conselho de Administração em 14.12.2021 (Ata nº 260/2021)

Brasília, 7 de dezembro de 2021



## SUMÁRIO

<b>1. APRESENTAÇÃO.....</b>	<b>4</b>
1.1. ESCOPO DO PLANEJAMENTO ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO - PETI.....	4
1.2. VIGÊNCIA DO PETI.....	4
1.3. ELABORAÇÃO E APROVAÇÃO.....	4
<b>2. O MODELO DE GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO DA EMGEA .....</b>	<b>4</b>
<b>3. METODOLOGIA DE ELABORAÇÃO DO PETI .....</b>	<b>5</b>
<b>4. ANÁLISE DE AMBIENTE .....</b>	<b>7</b>
<b>5. INVENTÁRIO DAS NECESSIDADES .....</b>	<b>9</b>
<b>6. OBJETIVOS ESTRATÉGICOS DE TECNOLOGIA DA INFORMAÇÃO E INICIATIVAS ESTRATÉGICAS .....</b>	<b>9</b>
<b>7. ANÁLISE DE RISCOS .....</b>	<b>11</b>
<b>8. MONITORAMENTO: METAS E INDICADORES DE DESEMPENHO.....</b>	<b>11</b>



## **1. APRESENTAÇÃO**

### **1.1. Escopo do Planejamento Estratégico de Tecnologia da Informação - PETI**

O Planejamento Estratégico de Tecnologia da Informação (PETI) é o documento que define diretrizes para o fornecimento de recursos e de ferramentas de tecnologia da informação necessários para o alcance dos objetivos estratégicos da Empresa, conforme determina a Resolução CGPAR nº 11, de 10.5.2016.

Como tal, o PETI é um documento de natureza estratégica, correlacionado e alinhado com o Planejamento Estratégico da EMGEA.

Os objetivos estratégicos de TI definidos no PETI norteiam a elaboração anual do Plano Diretor de Tecnologia da Informação (PDTI), no qual são elencadas as ações previstas no período de vigência do PETI.

### **1.2. Vigência do PETI**

Este PETI tem validade para o 1º semestre do ano de 2022, alinhado com o Planejamento Estratégico da Empresa para o mesmo período, uma vez que em 25/08/2021 foi publicada a Resolução CPPI nº 200, na qual foram aprovadas as modalidades operacionais de desestatização da EMGEA e o prazo máximo para iniciar o processo de dissolução da Empresa (30/06/2022). Essa resolução foi chancelada em 19/11/2021, pelo Decreto nº 10.863, que ratificou o marco temporal para início do processo de desestatização da EMGEA.

De acordo com o cronograma elaborado pelo BNDES, a alienação dos ativos da EMGEA deve ocorrer até 30.6.2022. Caso, eventualmente, alterações no cronograma posterguem a alienação das carteiras para além do previsto, uma nova revisão do PETI deverá ser efetuada, em linha com o novo Planejamento Estratégico da Empresa.

### **1.3. Elaboração e aprovação**

O PETI é elaborado pela Superintendência de Tecnologia (SUTEC), com assessoria do Gabinete de Governança (GABIN), no que tange aos temas relacionados a riscos e controles internos. É 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.

## **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 (GERIN) e Gerência de Redes e Suporte Técnico (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 PETI**

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 2022 foram definidos os seguintes pilares estratégicos, conforme Nota Técnica nº 282/2021:



1	Dissolução Societária	2	Alienação de Ativos	3	Sustentabilidade Financeira
<b>Norteadores</b>					
Finanças	VIABILIZAR O INGRESSO DE RECURSOS FINANCEIROS QUE PERMITAM HONRAR OS COMPROMISSOS DA EMPRESA E QUE MANTENHAM A SUSTENTABILIDADE FINANCEIRA.				
Processos	EQUACIONAR AS PENDÊNCIAS OPERACIONAIS, FINANCEIRAS E CONTÁBEIS QUE CONTRIBUAM PARA A ALIENAÇÃO DE ATIVOS DAS CARTEIRAS E A DISSOLUÇÃO SOCIETÁRIA DA EMPRESA.				
Clientes	ATUAR NO SENTIDO DE MINIMIZAR EVENTUAIS IMPACTOS NEGATIVOS AOS CLIENTES, DECORRENTES DO PROCESSO DE ALIENAÇÃO DE ATIVOS DAS CARTEIRAS.				
Pessoas	DESENVOLVER UM PLANO DE DESMOBILIZAÇÃO HUMANIZADO, QUE VALORIZE AS PESSOAS E ENCAMINHE A TRANSIÇÃO DE SUAS CARREIRAS.				

Observada a premissa de alinhamento com os objetivos estratégicos definidos para 2022, o trabalho de elaboração do PETI 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.

#### 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.
- Incertezas inerentes ao processo de desestatização.

### 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.
- Infraestrutura tecnológica preparada para suportar novos negócios.
- Utilização das melhores práticas em Governança de TI.
- Utilização de tecnologias modernas e inovadoras para suportar o negócio.
- 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 até 30.6.2022.
- 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, face o cenário de desestatização.

## Ambiente Interno



## 5. INVENTÁRIO DAS NECESSIDADES

Tendo como referencial os objetivos definidos no Planejamento Estratégico da EMGEA para 2022, 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.
- Relatório de avaliação de conformidade, metodologia e plano de ação para adequação da EMGEA à LGPD.

A segurança da informação abordada neste PETI abrange (Art. 2º, do Decreto nº 9.637/2018):

- Segurança cibernética;
- Defesa cibernética;
- Segurança física e a proteção de dados organizacionais; e
- Ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

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

Relação das Necessidades de TI	
<b>N01</b>	Melhoria na Gestão de Serviços, de Nível de Serviço e de Qualidade
<b>N02</b>	Atualização e manutenção do parque tecnológico
<b>N03</b>	Atualização da Política de Segurança da Informação
<b>N04</b>	Aprimoramento do monitoramento e gerenciamento do ambiente de TI
<b>N05</b>	Aprimoramento das soluções tecnológicas para sustentar o negócio
<b>N06</b>	Aprimoramento da plataforma de negócios para viabilizar a integração com soluções de terceiros.
<b>N07</b>	Aprimoramento dos mecanismos de rastreamento de dados - Lei Geral de Proteção de Dados Pessoais (LGPD).
<b>N08</b>	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 2022 foram definidos os 3 (três) objetivos estratégicos de TI (OETI):

- **OETI 01:** Prover e disponibilizar soluções de TI para os negócios da Empresa e para viabilizar o processo de alienação de ativos e dissolução societária
- **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.

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



## 7. ANÁLISE DE RISCOS

Utilizando a metodologia<sup>1</sup> de gestão de riscos adotada pela EMGEA e a Matriz de Riscos<sup>2</sup> relativa ao processo “Gestão de Tecnologia da Informação”, foram mapeados os eventos de risco que podem comprometer a execução do PETI, com os respectivos graus de exposição<sup>3</sup>, 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 PETI será monitorado com a definição das seguintes metas e indicadores de desempenho.

<b>OETI 01 – Prover e disponibilizar soluções de TI para os negócios da Empresa e para viabilizar o processo de alienação de ativos e dissolução societária.</b>			
<b>Indicador</b>	<b>O que mede</b>	<b>Periodicidade</b>	<b>Meta 2022</b>
Percentual de chamados de suporte técnico atendidos dentro do prazo.	Mostra o percentual de chamados cujo primeiro atendimento ocorreu sem atraso, dentro do prazo para início do atendimento. Não necessariamente o chamado deve ser concluído dentro deste prazo. Medido através da quantidade de chamados atendidos no ano versus a quantidade de chamados atendidos com atraso no ano.	Semestral	92%
Percentual de satisfação dos usuários internos em relação ao atendimento prestado durante o suporte técnico.	Mostra o percentual de satisfação dos usuários internos em relação ao atendimento prestado pelos técnicos de suporte. Medido através da pesquisa de encerramento de chamados. O chamado será considerado como satisfatório se o atendimento for classificado como “Ótimo” ou “Bom”.	Semestral	97%
Índice de execução das ações previstas no PDTI, relacionadas ao OETI 01	Mostra o percentual de execução das ações previstas no PDTI, relacionadas ao OETI 01.	Semestral	90%

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

<sup>2</sup> 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).

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



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

<b>Indicador</b>	<b>O que mede</b>	<b>Periodicidade</b>	<b>Meta 2022</b>
Percentual de disponibilidade dos links de Internet.	Mostra o percentual de disponibilidade dos links de Internet durante o horário de funcionamento da EMGEA.	Semestral	99,4%
Índice de execução das ações previstas no PDTI, relacionadas ao OETI 02	Mostra o percentual de execução das ações previstas no PDTI, relacionadas ao OETI 02.	Semestral	85%

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

<b>Indicador</b>	<b>O que mede</b>	<b>Periodicidade</b>	<b>Meta 2022</b>
Percentual de gestores que participaram de eventos ou cursos gerenciais.	Mostra o percentual dos gestores da SUTEC que participaram de eventos e/ou cursos técnicos para o desenvolvimento de competências gerenciais.	Semestral	50%
Percentual de colaboradores que participaram de eventos ou cursos técnicos.	Mostra o percentual dos colaboradores da SUTEC que participaram de eventos e/ou cursos técnicos para o desenvolvimento de competências técnicas.	Semestral	50%
Quantidade de eventos ou cursos.	Mostra a quantidade de eventos (workshop, fóruns, conferências, etc.) e cursos que tiveram a participação de um ou mais colaboradores da SUTEC.	Semestral	4
Índice de execução das ações previstas no PDTI, relacionadas ao OETI 03	Mostra o percentual de execução das ações previstas no PDTI, relacionadas ao OETI 03.	Semestral	95%

## 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	ALTO	BAIXO	<ul style="list-style-type: none"> <li>▪ Rotina de elaboração, revisão e aprovação de projetos básicos e termos de referência para aquisição de bens ou contratação de serviços de TI</li> <li>▪ Normatização de compras e contratações - Regulamento de Licitações e Contratos Administrativos (LG.NOR.008)</li> <li>▪ Fiscalização de contratos para monitoramento da qualidade dos serviços prestados e/ou dos produtos fornecidos</li> </ul>
Risco de conformidade	Inobservância de normas externas	ALTO	MÉDIO	<ul style="list-style-type: none"> <li>▪ Treinamento</li> <li>▪ Repasse de conhecimento para os demais colaboradores</li> <li>▪ Atualização de políticas e normas internas</li> <li>▪ Monitoramento do ambiente regulatório</li> </ul>
	Inobservância de normas internas	ALTO	MÉDIO	
	Falha humana	ALTO	BAIXO	
	Divulgação de informações incorretas ou incompletas ao público interno	MÉDIO	BAIXO	
Risco de governança	Desalinhamento de planejamento estratégico de tecnologia da informação com o planejamento estratégico institucional	ALTO	BAIXO	<ul style="list-style-type: none"> <li>▪ Reorganização e reprogramação das ações do PETI em caso de alteração do Planejamento Estratégico da EMGEA</li> <li>▪ Divulgação do PETI e do PDTI</li> <li>▪ Aprovação feito por comitês de TI</li> </ul>
Risco de infraestrutura	Falta de espaço para armazenamento de dados, informações e documentos	ALTO	BAIXO	<ul style="list-style-type: none"> <li>▪ Manutenções periódicas dos equipamentos de infraestrutura do Centro de Processamento de Dados - CPD</li> <li>▪ Sistema de combate a incêndio</li> <li>▪ Monitoramento do ambiente de infraestrutura</li> <li>▪ Análise periódica do ciclo de vida dos equipamentos de TI</li> <li>▪ Atualização periódica dos equipamentos de infraestrutura de TI</li> <li>▪ Contratação de empresas especializadas na manutenção preventiva e corretiva dos equipamentos de infraestrutura de TI</li> <li>▪ Pesquisas de satisfação</li> </ul>
	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 de integridade	Furto/roubo de bens ou valores	ALTO	BAIXO	<ul style="list-style-type: none"> <li>▪ Código de Ética, Integridade e Conduta</li> <li>▪ Programa de Integridade</li> <li>▪ Controles de acesso às dependências</li> <li>▪ Definição de níveis de acesso lógico</li> <li>▪ Monitoramento CFTV</li> <li>▪ Trilhas de auditoria nos sistemas automatizados</li> <li>▪ Inventário físico</li> </ul>
	Uso indevido da informação	ALTO	MÉDIO	
	Corrupção	MÉDIO	BAIXO	



Risco	Eventos de riscos	Grau de exposição		Ações de mitigação
		Inerente	Residual	
	Fraude nas operações internas	MÉDIO	BAIXO	<ul style="list-style-type: none"> <li>▪ Plantonistas</li> <li>▪ Termos de Proteção de Dados, Sigilo e Responsabilidade</li> <li>▪ Fiscais de contratos</li> </ul>
Risco de reputação	Divulgação de informações incorretas ou incompletas ao público externo	ALTO	MÉDIO	<ul style="list-style-type: none"> <li>▪ Código de Ética, Integridade e Conduta</li> <li>▪ Programa de Integridade</li> <li>▪ Atualização de políticas e normas internas</li> </ul>
Risco de pessoal	Falta de qualificação profissional	MÉDIO	MÉDIO	<ul style="list-style-type: none"> <li>▪ Repasse de conhecimento para os demais colaboradores</li> <li>▪ Formação de sucessores</li> <li>▪ Treinamento</li> </ul>
	Perda de colaboradores-chave	ALTO	MÉDIO	
Risco de segurança da informação	Ataques cibernéticos	ALTO	MÉDIO	<ul style="list-style-type: none"> <li>▪ Teste de restauração periódico das mídias magnéticas de backup</li> <li>▪ Aplicação de contingência dos principais recursos de TI</li> <li>▪ 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</li> <li>▪ Elaboração de um Plano de Continuidade da TI</li> <li>▪ Controles de acesso às dependências</li> <li>▪ Definição de níveis de acesso lógico</li> <li>▪ Monitoramento CFTV</li> <li>▪ Backup de mídias em ambiente externo à Empresa</li> <li>▪ Divulgação periódica de boas práticas de segurança da informação</li> <li>▪ Normas e procedimento sobre o uso de informações</li> <li>▪ Norma de sigilo aplicável a empregados, prestadores de serviços, fornecedores, fornecedores em pré-venda, parceiros e clientes</li> <li>▪ Utilização de Firewall</li> <li>▪ Utilização de Antivírus</li> </ul>
	Ataques de engenharia social	MÉDIO	BAIXO	
	Inconsistência de dados ou informações	MÉDIO	BAIXO	
	Inserção, alteração ou exclusão de dados / informações	ALTO	MÉDIO	
	Perda de conhecimento	ALTO	MÉDIO	
	Perda de documentos e registros	MÉDIO	BAIXO	
	Vazamento de informações estratégicas ou sigilosas	ALTO	MÉDIO	
Risco de sistemas	Falha na configuração de sistemas	ALTO	BAIXO	<ul style="list-style-type: none"> <li>▪ Fiscais de contratos</li> <li>▪ Monitoramento</li> <li>▪ Validação de bases de dados</li> <li>▪ Janela de processamento e manutenção</li> <li>▪ Políticas, normas e procedimentos sobre gestão e desenvolvimento de sistemas</li> <li>▪ Trilhas de auditoria nos sistemas automatizados</li> </ul>
	Falha no processamento e importação de dados	ALTO	BAIXO	
	Falha na definição de requisitos em sistemas informatizados	MÉDIO	BAIXO	



Risco	Eventos de riscos	Grau de exposição		Ações de mitigação
		Inerente	Residual	
	Falha na transmissão de informações/dados	MÉDIO	BAIXO	<ul style="list-style-type: none"> <li>Metodologia para gerenciamento ágil de projetos de software, denominada SCRUM</li> <li>Documentação de intervenções realizadas em sistemas de terceiros</li> <li>Ambiente de teste e homologação de sistemas</li> <li>Formalização de demandas relacionadas à tecnologia</li> </ul>
Risco de terceiro	Descontinuidade de prestação de serviços	ALTO	BAIXO	<ul style="list-style-type: none"> <li>Instrumentos contratuais</li> <li>Fiscais de contratos</li> <li>Banco de fornecedores</li> </ul>
	Falha na prestação de serviços	ALTO	BAIXO	
	Interrupção temporária de prestação de serviços	BAIXO	BAIXO	
Risco orçamentário	Insuficiência de recursos orçamentários	MÉDIO	BAIXO	<ul style="list-style-type: none"> <li>Programação orçamentária com base no desdobramento do Planejamento Estratégico organizacional para a TI e na evolução tecnológica</li> </ul>
Risco de privacidade	Coleção excessiva de dados pessoais	ALTO	MÉDIO	<ul style="list-style-type: none"> <li>Termo de Consentimento; Capacitação de colaboradores da EMGEA</li> <li>Política de Privacidade; Proteção de Dados Pessoais, Sigilo e Responsabilidade;</li> <li>Comitê de Segurança da Informação, Proteção de Dados Pessoais e Privacidade (CSI);</li> <li>Termo de Consentimento; Contratos; Acordos; Convênios; Registros (logs) em sistemas e softwares; SLA para atendimento das demandas via SISADE; Políticas, normas e procedimentos internos.</li> <li>Backup Corporativo; Backup Corporativo; Capacitação de colaboradores da EMGEA</li> <li>Processo administrativo; Programa de Desenvolvimento de Competências</li> </ul>
	Falha no tratamento de dados pessoais	ALTO	MÉDIO	
	Não atendimento de demandas dos titulares de dados pessoais ou atendimento intempestivo e/ou com baixa qualidade	ALTO	MÉDIO	
	Não comunicação de incidentes de segurança da informação e privacidade ou comunicação intempestiva	ALTO	MÉDIO	
	Perda ou alteração de dados pessoais	MÉDIO	MÉDIO	
	Remoção não autorizada de dados pessoais	MÉDIO	MÉDIO	
	Retenção prolongada de dados pessoais sem necessidade	MÉDIO	MÉDIO	
	Tratamento sem consentimento do titular dos dados pessoais	ALTO	MÉDIO	
Risco de conjuntura	Decisões políticas que possam comprometer o alcance dos objetivos e do propósito da EMGEA	ALTO	BAIXO	<ul style="list-style-type: none"> <li>Planejamento estratégico institucional; Monitoramento</li> <li>Ações direcionadas ao fortalecimento e proteção da imagem da empresa</li> <li>Alta Administração mantém tratativas permanentes acerca dos objetivos e do propósito da EMGEA com representantes do Ministério da Economia.</li> </ul>
	Mudanças legais que afetem as operações da EMGEA	MÉDIO	BAIXO	



emgea

empresa gestora de ativos