Plano de Gestão de Riscos de TIC

UNIFESSPA | Centro de Tecnologia da Informação e Comunicação

Histórico de Revisão

Versão	Data	Autor	Descrição
1.0	15/04/2020	Ralfh Alan Gomes Machado e Edney Almeida do Nascimento (CGTIC)	Construção do Plano de Gestão de Riscos de TIC
1.1	07/07/2020	Vitor Castro	Revisão e sugestões
1.2	13/07/2020	Ralfh Alan Gomes Machado e Edney Almeida do Nascimento (CGTIC)	Consolidação
1.3	13/07/2020	Vitor Castro	Revisão e sugestões finais
1.4	16/07/2020	Ralfh Alan Gomes Machado e Edney Almeida do Nascimento (CGTIC)	Consolidação Final
1.4	13/10/2020	CGD	Aprovação na 12ª Reunião do CGD
1.5	24/06/2021	Gestores do CTIC	Revisão dos controles

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Quadros

Apresentação

A ação e interação dos objetivos organizacionais junto com as incertezas dão origem ao risco, que se apresentam no dia a dia de todas as formas em quaisquer atividades desenvolvidas. Muitas vezes, o risco não se apresenta visível, sendo necessárias determinadas ações para identificá-lo; em outras situações o risco é proveniente de ações repentinas que fogem do controle humano, como no caso de eventos de causas naturais.

O gerenciamento de riscos permite ações contínuas de planejamento, organização e controle dos recursos relacionados aos riscos que possam comprometer o sucesso da contratação, execução e da gestão contratual. Este plano tem por objetivo apresentar os principais ativos de tecnologia da informação e comunicação do Centro de Tecnologia da Informação e Comunicação (CTIC), assim como detalhar suas ameaças, vulnerabilidades, controles e riscos.

Termos e definições

Os conceitos relacionados aos termos técnicos e definições mencionadas no decorrer deste documento, são apresentados no quadro abaixo:

Quadro 01 - Termos e definições

Termo e Definições	**Descrição**
CAU	Coordenadoria de Atendimento ao Usuário
CGD	Comitê de Governança Digital
CGTIC	Coordenadoria de Governança de Tecnologia da Informação e comunicação
CTIC	Centro de Tecnologia da Informação e comunicação
DICTI	Divisão de Contratações de Tecnologia da Informação
DISI	Divisão de Sistemas de Informação
DIRSI	Divisão de Redes e Serviços de Internet
PDI	Plano de Desenvolvimento Institucional
PDTIC	Plano Diretor de Tecnologia da informação e comunicação
PGO	Plano de Gestão Orçamentária
POSIC	Política de Segurança da Informação e Comunicação
Unifesspa	Universidade Federal do Sul e Sudeste do Pará

1. Conceitos fundamentais

Segurança da Informação é a proteção da informação de vários tipos de ameaças, visando garantir a continuidade do negócio, minimizar os riscos que possam comprometê-lo e maximizar o retorno sobre os investimentos e as oportunidades de negócio. É obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais, funções de hardware e software. Além disso, ela pode ser realizada com a implementação de controles que deverão ser monitorados, analisados e continuamente melhorados, com o intuito de atender aos objetivos do negócio, mitigando os riscos e garantindo os preceitos de segurança da organização: confidencialidade, integridade, disponibilidade e autenticidade (CIDA) (GUIA 73, 2009) (ISO 31000, 2018).

Ameaça é todo e qualquer evento que possa explorar vulnerabilidades, geralmente é um fator externo à organização, podendo ser também a causa potencial de um incidente indesejado, que pode resultar em dano para os sistemas, pessoas ou a própria organização. Classificam-se em: intencionais, ação da natureza, não intencionais. São exemplos de ameaças: erros humanos, falhas de hardware, falhas de software, ações da natureza, terrorismo, vandalismo, entre outras (GUIA 73, 2009) (ISO 31000, 2018).

Vulnerabilidade é qualquer fraqueza que possa ser explorada para comprometer a segurança de sistemas ou informações, além disso, pode ser uma fragilidade de um ativo ou grupo de ativos que venha a ser explorada por uma ou mais ameaças. Comparando-as, a ameaça é o evento ou incidente, enquanto a vulnerabilidade é a fragilidade que será explorada para que a ameaça se concretize. São exemplos de vulnerabilidades: falta de treinamento de funcionários, sistema aceitar qualquer valor nos seus campos, desatualização dos servidores de banco de dados, entre outras (GUIA 73, 2009) (ISO 31000, 2018).

Risco é a combinação da probabilidade (chance da ameaça se concretizar) de um evento indesejado ocorrer e de suas consequências para a organização, ou seja, é a incerteza resultante da combinação da probabilidade de ocorrência de um evento e suas consequências (GUIA 73, 2009) (ISO 31000, 2018).

Riscos de segurança da informação é a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, assim prejudicando a organização (GUIA 73, 2009) (ISO 31000, 2018).

Identificação de riscos é o processo para localizar, listar e caracterizar elementos de risco. Por menor que seja a probabilidade de ocorrência de um risco, pode ser que determinada incerteza ocorra e explore uma vulnerabilidade, concretizando uma ameaça. Para se preparar para isso é necessário conhecer os riscos de todo o ambiente, através da realização de um processo formalizado de identificação de riscos (GUIA 73, 2009) (ISO 31000, 2018).

Impacto é a mudança adversa no nível obtido dos objetivos de negócios, ou seja, a consequência avaliada dos resultados com a ocorrência de um evento em particular, em que determinada vulnerabilidade foi explorada, uma ameaça ocorreu e o risco se concretizou (GUIA 73, 2009) (ISO 31000, 2018).

Estimativa de riscos é o processo utilizado para atribuir valores à probabilidade e consequências de um risco, permitindo ainda quantificar ou descrever de forma qualitativa um risco, desse modo, às organizações podem priorizar os riscos de acordo com os critérios estabelecidos (GUIA 73, 2009) (ISO 31000, 2018).

Ações de modificação do risco são ações tomadas para reduzir a probabilidade e as consequências negativas, ou ambas, associadas a um risco (GUIA 73, 2009) (ISO 31000, 2018).

Comunicação do risco é a troca ou compartilhamento de informações sobre o risco entre o tomador de decisão e outras partes interessadas (GUIA 73, 2009) (ISO 31000, 2018).

Ação de evitar o risco é a decisão de não se envolver ou agir de forma a mitigar uma situação de risco (GUIA 73, 2009) (ISO 31000, 2018).

Retenção do risco é a aceitação do ônus da perda ou do benefício do ganho associado a um determinado risco (GUIA 73, 2009) (ISO 31000, 2018).

Compartilhamento do risco é o compartilhamento com outra entidade do ônus da perda ou do benefício do ganho associado a um risco (GUIA 73, 2009) (ISO 31000, 2018).

Norma ABNT NBR ISO/IEC 27001:2013: destinada à tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação – requisitos. Apresenta e descreve os requisitos que devem ser implementados no estabelecimento de um Sistema de Gestão de Segurança da Informação (SGSI).

Norma ABNT NBR ISO/IEC 27002:2013: destinada à tecnologia da informação – técnicas de segurança – código de prática para a gestão de segurança da informação. Apresenta as melhores práticas para uma gestão adequada da segurança da informação.

Norma ABNT NBR ISO 31000:2018 Gestão de Riscos – Princípios e diretrizes: norma que fornece os princípios e diretrizes genéricas para qualquer indústria ou setor.

Norma ABNT ISO GUIA 73:2009 Gestão de Riscos – Vocabulário: norma que apresenta as definições de termos genéricos relativos à gestão de riscos.

Norma ISO/IEC 31010:2012 Gestão de riscos – Técnicas de avaliação de riscos: norma que deve ser trabalhada em apoio à norma "ABNT NBR ISO 31000:2018 Gestão de Riscos – Princípios e diretrizes". Descreve as diversas técnicas e ferramentas de análise de risco (ainda não traduzida pela ABNT).

Norma ABNT NBR ISO/IEC 27005:2019: destinada à tecnologia da Informação – técnicas de segurança – gestão de riscos de segurança da informação. Apresenta as diretrizes para o gerenciamento dos riscos de segurança da informação, além de empregar os conceitos da norma ABNT NBR ISO 27001:2013.

2. Princípios da gestão de riscos

Os princípios da gestão de riscos são:

- Cria e protege valor;
- Parte integrante de todos os processos organizacionais;
- Parte da tomada de decisões;
- Aborda explicitamente a incerteza;
- Sistemática, estruturada e oportuna;
- Baseia-se nas melhores informações disponíveis;
- Feita sob medida;
- Considera fatores humanos e culturais;
- Transparente e inclusiva;
- Dinâmica, iterativa e capaz de reagir a mudanças; e
- Facilita a melhoria contínua da organização.

Para a gestão de riscos ser eficaz, convém que uma organização, em todos os níveis, atenda aos princípios descritos.

2.1 Visão geral da gestão de riscos

É necessária uma abordagem sistemática de gestão de riscos que muda de organização para organização, assim como o nível de risco aceitável de cada uma, sendo que risco aceitável é o grau de risco que a organização está disposta a aceitar para concretizar seus objetivos. Além disso, faz-se necessário aumentar a capacidade de gerir o risco e otimizar o retorno.

A abordagem da gestão de riscos deve ser:

- Contínua;
- Realizada no tempo apropriado;
- Repetitiva;
- Própria ao ambiente da organização;
- Ajustada ao processo de gestão de riscos corporativos;
- Alinhada com os requisitos de negócios; e
- Apoiada pela alta direção.

Resumindo, a gestão de riscos são atividades formalizadas e coordenadas para controlar e dirigir um conjunto de instalações e pessoas com relações e responsabilidades, entre si e externamente.

3. Metodologia

A metodologia utilizada para a construção deste documento foi a norma ABNT NBR ISO/IEC 27005, a Figura 1 apresenta uma visão do processo de gestão de riscos:

Figura 01 - Processo de gestão de riscos.

Fonte: Konzen (2020)

3.1 Definição do contexto

Dentro do processo, a definição do contexto é responsável pela definição do ambiente, escopo, critérios de avaliação, entre outras definições. Esta etapa é essencial para a equipe que

realiza a gestão de risco conhecer todas as informações sobre a organização.

3.2 Análise/Avaliação de riscos

A próxima iteração é de análise e avaliação de risco, que permitirá a identificação dos riscos e a determinação das ações necessárias para reduzir o risco a um nível aceitável.

3.3 Tratamento do risco

A partir dos resultados obtidos na análise e avaliação do risco são definidos os controles necessários para o tratamento do risco. A norma ABNT NBR ISO/IEC 27001 especifica os controles que deverão ser implementados.

3.4 Aceitação do risco

Assegura os riscos aceitos pela organização, ou seja, os riscos que por algum motivo não serão tratados ou serão tratados parcialmente, são os chamados riscos residuais, cujo enquadramento nesta categoria deverá ser justificado.

3.5 Comunicação do risco

Nesta etapa é feita a comunicação do risco e da forma como será tratado, para todas as áreas operacionais e seus gestores.

3.6 Monitoramento e análise crítica

São as atividades de acompanhamento dos resultados, implementação dos controles e de análise crítica para a melhoria contínua do processo de gestão de riscos.

4. Contexto

Ao iniciar as atividades para a elaboração do plano de gestão de riscos, a primeira tarefa a ser feita é conhecer o ambiente em que o trabalho será desenvolvido, as pessoas que de alguma forma interagirão, o que será desenvolvido; em resumo, “conhecer o terreno” para saber conduzir o andamento dos trabalhos.

Nas atividades que envolvem gestão de riscos a definição do contexto é a parte inicial e tem como objetivo permitir o conhecimento do ambiente da organização. As informações listadas a seguir foram obtidas através de reuniões com a equipe de elaboração do plano de gestão de riscos instituída através da portaria nº 06/2019 CTIC/Unifesspa, de 16/07/2019:

4.1 Propósito principal da organização

A Universidade Federal do Sul e Sudeste do Pará (Unifesspa) tem por objetivo “produzir, sistematizar e difundir conhecimentos filosófico, científico, artístico, cultural e tecnológico, ampliando a formação e as competências do ser humano na perspectiva da construção de uma sociedade justa e democrática e no avanço da qualidade de vida”.

4.1.1 Negócio da organização

Promover o ensino, pesquisa e extensão com excelência.

4.1.2 Missão do CTIC

Prover soluções de tecnologia da informação e comunicação para a Unifesspa alcançar com excelência seus objetivos institucionais.

4.1.3 Seus valores

- Ética;
- Eficiência;
- Execução/planejamento dos projetos;
- Melhoria contínua;
- Melhoria de processos, serviços, normas, procedimentos;
- Gestão Participativa;
- Formação dos conselhos, colegiados, comissões;
- Profissionalismo;
- Qualificação e atualização profissional dos servidores;
- Postura colaborativa com as ações institucionais tais como: treinamentos, suportes, capacitações externas;
- Transparência;
- Redes sociais, dados abertos, portais, relatórios de gestão, indicadores de desempenho;
- Comprometimento;
- Promover e manter a missão do CTIC; e
- Avaliar o desempenho.

4.1.4 A estrutura da organização

A área de TIC na Unifesspa é representada pelo Centro de Tecnologia da Informação e Comunicação (CTIC), um órgão suplementar ligado a Reitoria (o organograma da Unifesspa pode ser visualizado no seguinte link: https://transparencia.unifesspa.edu.br/2-uncategorised/101-organograma-unifesspa.html). O Centro está organizado em 03 (três) divisões: Divisão de Sistemas de Informação (DISI), Divisão de Redes e Serviços de Internet (DIRSI), Divisão de Contratação em Tecnologia da Informação (DICTI).

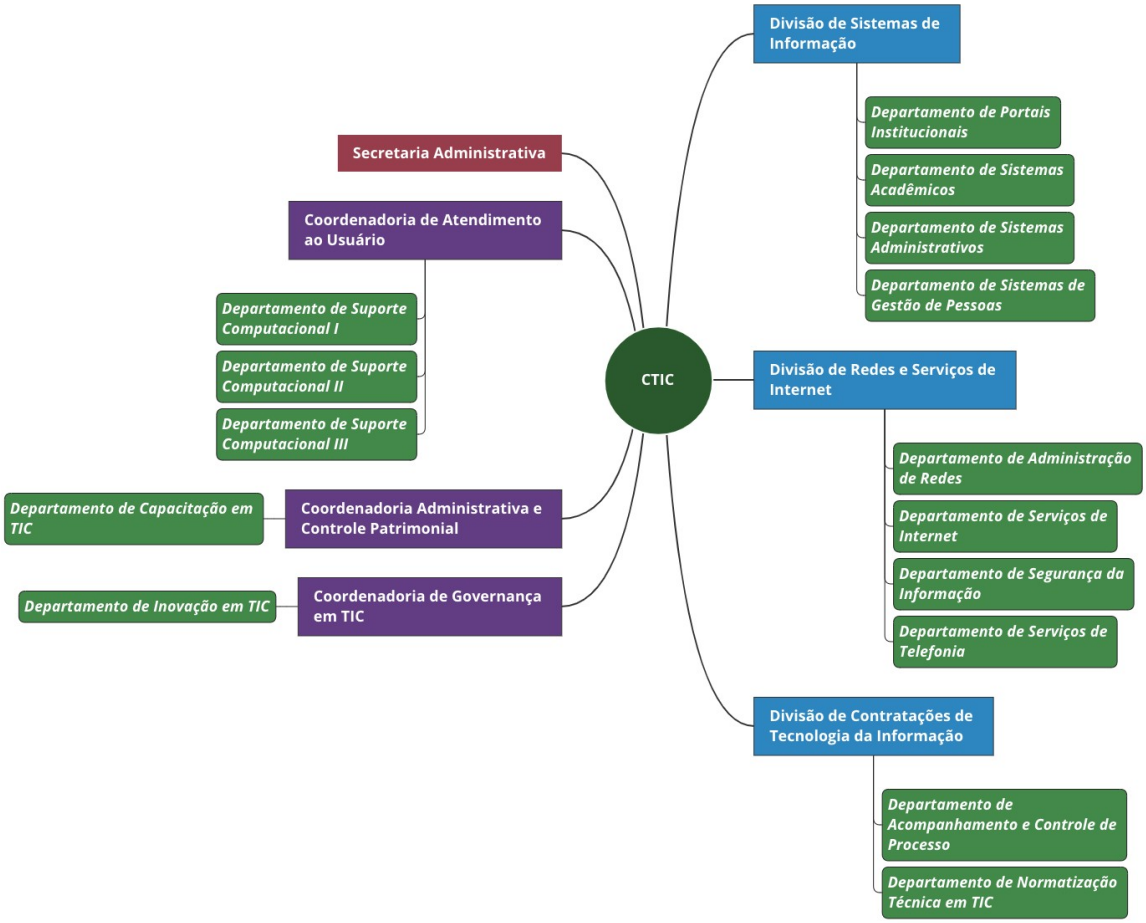
Respectivamente, essas divisões têm atribuições diretamente ligadas ao desenvolvimento, implantação e manutenção de sistemas, gerenciamento dos serviços de infraestrutura de TIC, e o apoio e planejamento às contratações de TIC.

O CTIC também conta com 03 (três) coordenadorias: Coordenadoria de Atendimento ao Usuário (CAU), Coordenadoria de Administração e Controle Patrimonial (CACP) e Coordenadoria de Governança em Tecnologia da Informação (CGTI), que possuem a função de prover apoio aos usuários dos serviços de TIC da Unifesspa, realizar o apoio administrativo, financeiro, patrimonial e auxiliar os processos finalísticos do CTIC, por meio do uso e implementação de práticas de Governança de TIC, respectivamente.

Como órgão executivo, o setor de TIC atua alinhado às estratégias direcionadas pelo Comitê de Governança Digital (CGD) que tem papel consultivo e deliberativo. O Comitê tem como competências: Promover a integração das estratégias da área de TIC e as estratégias organizacionais, apoiar a Administração Superior nos assuntos referentes às áreas finalísticas no âmbito de TIC da Unifesspa, propor e aprovar políticas e padrões relacionados às soluções de TIC, elaborar, aprovar e monitorar o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), implementar o gerenciamento do processo de contratação de bens e serviços de TIC, aderindo ao que determina à Instrução Normativa n° 04/2014 – STI/MPOG e sua posterior atualização através da IN 01/2019 do Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria de Governo Digital; propor plano de investimento para a área de TIC. A figura 2 exibe o organograma do CTIC.

A estrutura legal do CTIC pode ser obtida através do link abaixo:
https://sigrh.Unifesspa.edu.br/servicos/converterArquivoPdf?idArquivo=193450

Figura 02 – Organograma do CTIC



Fonte: PDTIC CTIC 2020-2021 - Unifesspa

4.1.5 Estratégias

O escopo estratégico adotado pela organização para a implantação, execução, monitoramento e revisão deste Plano de Gestão de Riscos de TIC, pode ser resumido em três pilares: uma equipe de tratamento de incidentes, que monitore as ameaças e apresente um relatório nas reuniões do CGD; uma Gestão da segurança da informação; e Normas, políticas e planos que apoiem e mantenham os objetivos alinhados para a conformidade entre os controles propostos e os respectivos resultados esperados aos tratamentos dos riscos.

4.1.6 Catálogo de serviços

Além de ter como objetivo principal ofertar serviços de TIC com excelência, o catálogo de serviços do CTIC que está em constante atualização pode ser obtido em https://governancadigital.unifesspa.edu.br/images/CatalogoAtualizado.pdf

4.1.7 Escopo legal e regulamentações externas

A gestão de riscos é um processo para identificar, avaliar, administrar, controlar e monitorar potenciais eventos ou situações capazes de afetar o desempenho da instituição, buscando estabelecer uma garantia razoável quanto ao cumprimento de seus objetivos. Para fins de aplicação do Plano de Gestão de Riscos de TIC, serão considerados, no que couber, os conceitos estabelecidos por Instruções Normativas dos Órgãos competentes como o Ministério de Planejamento Orçamento e Gestão (MPOG) e a Controladoria Geral da União (CGU), Processos de Gestão de Riscos padronizados internacionalmente, amplamente utilizados pelo mercado e adotados pelas organizações nacionais como ABNT NBR ISO/IEC. A lista com os principais escopos legais, padrões e regulamentações externas utilizadas neste Plano de Gestão de Riscos de TIC estão listados abaixo.

- Instrução Normativa Conjunta CGU/MP nº 1, de 10 de maio de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.
- Processo de Gestão de Riscos da Norma ABNT NBR ISO/IEC 31000:2018 Gestão de Riscos;
- Normas de gestão de segurança e de riscos: Norma ABNT NBR ISO/IEC 27001:2013;
- Norma ABNT NBR ISO/IEC 27002:2013; e
- Norma ABNT NBR ISO/IEC 27005:2019 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação.

4.1.8 Escopo e Políticas internas

O Plano de Gestão de Riscos de TIC deve estar em conformidade e alinhado aos requisitos e políticas internas que fazem parte do escopo interno da organização o qual ele está sujeito, tanto do CTIC quanto a própria Unifesspa. A lista das principais políticas internas e planos estão listadas abaixo com seus respectivos períodos de atualização.

- PDI (Plano de Desenvolvimento Institucional), quadrienal;
- PDTIC (Plano Diretor de Tecnologia da Informação e Comunicação), bienal;
- Política de Gestão de Riscos de TIC, bienal;
- POSIC (Política de Segurança da Informação e Comunicação), anual;
- Política de uso dos recursos computacionais, quadrienal;
- Plano de integridade, anual;

4.1.9 Processos de negócio da organização

Os principais processos de negócio da organização que serão mapeados estão listados abaixo:

- Gerência;
- Implantação;
- Aquisição;
- Manutenção e planejamento de serviços de TIC;

4.1.10 Principais fornecedores

Os principais fornecedores assim como os processos de compras para o CTIC, no papel vigente como organização desse Plano de Gestão de Riscos de TIC devem estar alinhados e ser realizadas em consonância com a IN 01, de 04 de abril de 2019, Ministério da Economia/Secretaria Especial de Desburocratização, Gestão e Governo Digital/Secretaria de

Governo Digital, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

4.1.11 Quadro pessoal e aperfeiçoamento

O CTIC em sua estrutura organizacional conta atualmente com um quadro pessoal de 30 (trinta) servidores ativos, os quais 02 (dois) se encontram em afastamento, 07 (sete) bolsistas que estão divididos em 01 (uma) direção, 03 (três) divisões, 01 (uma) secretaria administrativa, 03 (três) coordenadorias e 15 (quinze) departamentos.

Os aperfeiçoamentos e treinamentos podem ser o grande responsável por melhorar os resultados e manter os níveis de excelências dentro da organização, fazendo com que as entregas de valores sejam realizadas da melhor maneira possível para o público alvo. Se tratando de Gestão de Riscos de TIC a preocupação com a estrutura organizacional e a segurança de os ativos deve ser constantemente revisada e monitorada. Para manter a comunidade atendida pelo CTIC informada e atualizada sobre as ameaças e riscos envolvendo a segurança da informação o CTIC disponibiliza periodicamente boletins de segurança da informação, afinal assim como em qualquer organização a informação o conhecimento é a chave para uma boa gestão de riscos.

4.2 Análise das Restrições

A seguir são listadas a análise das restrições na qual o Centro está inserido:

- Advindas da agenda da organização:
  - Calendário institucionais (compras, acadêmico), PGO (Plano de Gestão Orçamentária), portarias de exercício.
- Advindas do ambiente econômico e político

- Alta administração é alterada a cada 04 anos;
- Orçamento da Organização já determinado com um ano de antecedência.

- De natureza cultural
  - Educação, experiência profissional, instrução, experiência fora do trabalho, filosofia, crença, opinião.
- De natureza estratégica
  - Indisponibilidade dos serviços do CTIC por no máximo 3 dias.
- De natureza política
  - Legislação limitante.
- Estruturais
  - Estrutura hierárquica e dificuldade de cooperação entre as unidades.
- Relativas aos recursos humanos
  - Recursos humanos abaixo do recomendado.
- Financeiras
  - Contingenciamento do governo, PGO, legislação.
- Organizacionais
  - Fornecimento de serviços terceirizados, planos contingenciais, soluções de incidentes, manutenções preventivas, qualificação para cargos de gestão.
- Temporais
  - Implementação dos controles de segurança em relação a capacidade estrutural e financeira da organização.

- Técnicas

  - Falta de capacitação, tecnologia legada, dificuldade na evolução dos sistemas e suas arquiteturas.

4.3 Análise do escopo

Serão mapeados os riscos dos principais macroprocessos e ativos do CTIC, o escopo envolve os ativos de TIC e os serviços disponibilizados pelo centro. Os departamentos envolvidos no mapeamento dos ativos foram: CAU, CGTIC, Direção do CTIC, DIRSI, DISI, DICTI.

Os processos envolvidos foram: processo de compra, os sistemas de informações gerenciais (SIG), sistemas internos e externos, processo de manutenção dos dados abertos, totalizando 42 pessoas envolvidas neste processo. Os limites do escopo foram os ativos e processos mais importantes a nível macro, além disso, não faz parte do escopo os ativos não relacionados a TIC.

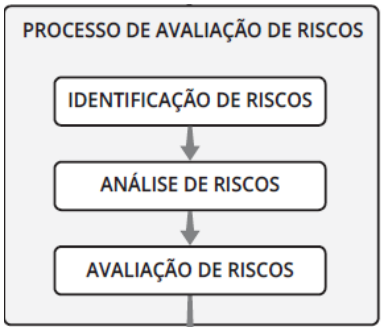
5. Processo de Análise e Avaliação de Riscos

Após a identificação do contexto e a definição do escopo, com o perfeito entendimento de todo ambiente, é iniciado o processo de análise e avaliação de riscos de segurança da informação. Segundo a norma ABNT NBR ISO/IEC 27005 essa fase do processo é subdividida em 03 (três) fases: identificação dos riscos, análise de riscos e avaliação de riscos.

Este processo é próxima iteração do processo de gestão de riscos de TIC, e consiste na análise e avaliação de risco, o que permitirá a identificação dos riscos e a determinação das ações necessárias para reduzir o risco a um nível aceitável. O processo de análise e avaliação de riscos identifica e valora ativos, ameaças e vulnerabilidade, abaixo podemos observar uma breve descrição sobre cada etapa dessa fase, assim como verificarmos a figura 03 que ilustra a ordem dessas etapas no processo de gestão de riscos.

- 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.

Figura 03 – Análise e Avaliação de Riscos



Fonte: Norma ABNT NBR ISO/IEC 27005, 2019

Cabe salientar que a avaliação e análise de riscos deve estar alinhada e em conformidade com o apetite a risco da organização, levando em consideração as necessidade de ações de controle e a percepção dos graus do riscos identificados, porém mais importante que o grau do risco é o nível de tolerância que a organização possui sobre aquele risco, se pode ser tolerável ou não, sempre utilizando o apetite a risco como limite de tolerância ao tratamento e aceitação dos riscos. Dessa forma, tanto os riscos inerentes (o risco antes da implementação de controles e ações pela organização), quanto os riscos residuais (os riscos que permanecem mesmo depois da implementação de controles e ações pela organização) precisam ser analisados e avaliados (Silva, 2015).

5.1 Identificação de riscos

No processo de análise e avaliação de riscos de TIC, a primeira etapa é a identificação de riscos. A identificação de riscos é realizada para que se possa conhecer e determinar os possíveis eventos com potencial de causar perdas, e fazer o levantamento de como isso pode

acontecer identificando os ativos.

5.1.1 Identificação os ativos

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. O quadro 02 apresenta os principais ativos identificados pelo CTIC:

Quadro 02 - Principais ativos priorizados pelo CTIC

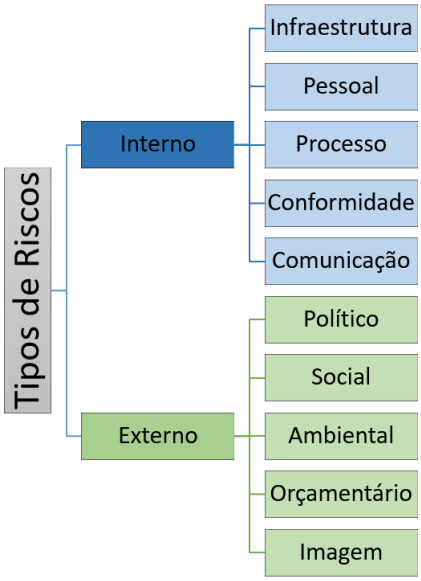
Id	Ativos	Justificativa	Responsável
AT1	Processo de contratação de TIC	Processo impacta a organização no atendimento dos seus objetivos	Gestor DICTI
AT2	Processo de seleção de bolsista de TIC	Processo impacta a organização no atendimento dos seus objetivos	Gestor CACP
AT3	Processo de desenvolvimento de software	Processo impacta a organização no atendimento dos seus objetivos	Gestor DISI
AT4	Suporte aos usuários de TIC	Processo impacta a organização no atendimento dos seus objetivos	Gestor CAU
AT5	Processo de Monitoramento dos recursos de TIC	Informação estratégica para organização	Gestor DIRSI
AT6	Equipe Técnica do CTIC	Imprescindível para o funcionamento da organização	Gestor CTIC
AT7	Estrutura física do Data Center	Todas as informações institucionais estão armazenadas nessa estrutura	Gestor DIRSI
AT8	Prédio do CTIC	Local de trabalho da equipe técnica de TIC	Gestor CTIC
AT9	Sistema Gerador de Energia do Data Center	Atender aos requisitos de segurança física e de acesso à	SINFRA

		informação	
AT10	Gestores do CTIC	Execução das atividades de gestão de risco e controle dos ativos institucionais	Gestor CTIC
AT11	Processo de gestão de contratos de TIC	Medida de disponibilidade	Gestor CTIC
AT12	Bancos de dados dos ambientes de produção	Armazena os dados primários da organização e dos usuários. Configura-se como primordial pois os dados contidos neles devem ser armazenados por longos períodos.	Gestor DIRSI
AT13	Softwares mantidos pela Unifesspa	Medida de disponibilidade para o Data Center	Gestor DISI
AT14	Softwares não mantidos pela Unifesspa	Medida de disponibilidade para o Data Center	Gestor DISI
AT15	Estações de trabalho da equipe de TIC	Medida de disponibilidade para o Data Center	Gestores da CACP e CAU
AT16	Serviço de Internet	Medida de disponibilidade para o Data Center	Gestor DIRSI
AT17	Serviço de telefonia	Medida de disponibilidade para o Data Center	Gestor DIRSI
AT18	Serviço de e-mail	Medida de disponibilidade para o Data Center	Gestor DIRSI
AT19	Processo de atualização dos dados abertos	Atender a Lei de Acesso a Informação	Gestor CGTI
AT20	Gestão de Conhecimento	Manter o compartilhamento e a continuidade das operações dos principais ativos	Gestor CTIC

5.1.2 Identificando as ameaças

A etapa de identificação de ameaças implica na realização de ações para levantamento e identificação, dentro do escopo estabelecido, as ameaças existentes na organização. Além da identificação nessa etapa também é feito a classificação quanto ao tipo da ameaça, ou seja, sua categoria de riscos que segundo Silva (Silva, 2015) corresponde a basicamente dois tipos: interna e externa. Na figura 04 podemos observar os tipos e suas categorias correspondentes.

Figura 04 – Tipos de ameaças/riscos



Fonte: Adaptada de (Silva, 2015)

O conceito de ameaça é definido como qualquer evento que explore vulnerabilidades, como visto no capítulo 1 – conceitos fundamentais, geralmente é um fator externo à organização na qual não se têm controle ou não se pode prever. Exemplos: erros humanos, falhas de hardware, falhas de software, ações da natureza, terrorismo, vandalismo. O quadro 03 apresenta as principais ameaças identificadas relacionadas aos ativos mapeados no quadro 01:

Quadro 03 - Principais ameaças identificadas.

Ativos	Ameaças	Tipo
AT1	Indisponibilidade da equipe de planejamento da contratação	Interna e externa
	Alteração na legislação	Externa
	Exequibilidade do tempo para execução do processo de contratação	Externa
	Interferência de empresa no processo de contratação a fim de direcionar ou restringir a competitividade	Externa
	Interposição de pedidos impugnações de editais	Externa
	Falta de competência técnica da equipe de planejamento da contratação	Interna
	Licitação fracassada ou deserta	Externa
	Indisponibilidade de recursos	Externa

AT2	Pouca demanda de candidatos	Externa
	Candidatos com perfil/experiência incompatível	Externa
AT3	Alta demanda de desenvolvimento de software	Externa
	Número insuficiente de pessoas na equipe para execução do processo	Interna e externa
AT4	Volume excessivo de chamados	Interna e externa
	Crescimento da instituição	Interna e externa
AT5	Ausência de ferramentas eficientes para monitoramento	Interna
	Expansão dos recursos de TIC	Externa
	Diminuição dos incentivos para qualificação	Externa
AT6	Fuga de talentos	Interna e externa
	Evolução tecnológica	Externa
AT7	Absenteísmo	Externa
	Inadequação do espaço físico	Interna
	Desastres naturais	Interna
AT8	Furto/Roubo de equipamentos	Interna
	Desastres naturais	Externa
AT9	Acesso indevido ao espaço físico	Externa
	Desastres naturais	Externa
AT10	Restrições orçamentárias	Externa
	Falta de alinhamento com a administração superior	Externa
	Contingenciamento de orçamento	Externa
AT11	Não entrega do objeto contratado	Externa
	Inadimplência do fornecedor	Externa
	Falência da empresa contratada	Externa
	Manuseio indevido de informação sigilosa por parte da contratada	Externa
AT12	Quebra da integridade dos arquivos do banco de dados	Interna e externa
	Indisponibilidade além do nível de acordo de serviços (SLA) das aplicações que dependem do banco de dados	Interna
AT13	Falha no ambiente de execução	Interna
	Indisponibilidade do sistema por erro introduzido durante o processo de desenvolvimento de software	Interna
AT14	Falha no ambiente de execução	Interna
	Falta de suporte/atualização pelo desenvolvedor	Externa
AT15	Falha de hardware fora do prazo de garantia	Externa
	Falha de hardware dentro do período da garantia	Externa
AT16	Indisponibilidade do provedor	Externa
	Falha de hardware	Interna e externa

AT17	Desastres naturais	Externa
	Indisponibilidade do provedor	Externa
	Falha de hardware	Interna e externa
	Desastres naturais	Externa
AT18	Indisponibilidade do serviço por ataque cibernético	Externa
	Falha de hardware	Interna e externa
	Falha de Software	Interna e externa
AT19	Alteração do software	Interna
	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	Interna
	Falha humana	Interna e externa
AT20	Indisponibilidade do técnico	Interna
	Perda de dados	Interna

5.1.3 Identificando os controles

Controle é qualquer mecanismo administrativo, físico ou operacional capaz de tratar os riscos da ocorrência de um incidente de segurança. Exemplos: políticas, procedimentos, estruturas organizacionais, antivírus, *patches*, fechaduras, extintor e backups. O quadro 04 apresenta os principais controles identificados relacionadas as ameaças mapeadas no quadro 03.

Quadro 04 – Principais controles identificados

Ativos	Ameaças	Controles
AT1	Indisponibilidade da equipe de planejamento da contratação	Formalizar a gestão colaborativa da contratação Indicação de suplente para cada membro da equipe
	Alteração na legislação	Orçamento destinado para capacitação
	Exequibilidade do tempo para execução do processo de contratação	Realocar força de trabalho Planejar lista de possíveis projetos Manter atas de registros de preços vigentes sempre que possível
	Interferência de empresa no processo de contratação a fim de direcionar ou restringir a competitividade	Priorização de pesquisa de mercado via painel de preços e contratações de outros entes públicos
	Interposição de pedidos impugnações de editais	Revisões de artefatos por servidor técnico com experiência na área
	Falta de competência técnica da equipe de planejamento da contratação	Orçamento destinado para capacitação
	Licitação fracassada ou deserta	Avaliação de soluções disponíveis no mercado e elaboração de matriz de fornecedor
AT2	Indisponibilidade de recursos	Manter edital de bolsistas voluntários
	Pouca demanda de candidatos	Divulgação do edital e prorrogação de inscrição
	Candidatos com perfil/experiência incompatível	Realizar capacitações de acordo com a área específica
AT3	Alta demanda de desenvolvimento de software	Aplicação do plano de desenvolvimento de software e verificação de alinhamento ao PDTIC
AT4	Número insuficiente de pessoas na equipe para execução do processo	Realocar força de trabalho Redimensionar a demanda
	Volume excessivo de chamados	Capacitação dos usuários Aplicação da política de incidentes
AT5	Crescimento da instituição	Orçamento destinado para capacitação
	Ausência de ferramentas eficientes para monitoramento	Painel de monitoramento dos chamados
	Expansão dos recursos de TIC	Monitoração através do Zabbix

AT6	Diminuição dos incentivos para qualificação	Criação e aplicação do plano de qualificação
	Fuga de talentos	Política de qualificação do CTIC
	Evolução tecnológica	Orçamento destinado para capacitação em inovação tecnológica
	Absenteísmo	Política de capacitação e gestão de pessoal técnico
AT7	Inadequação do espaço físico	Orçamento destinado para adequação
	Desastres naturais	Plano de contingência
AT8	Furto/Roubo de equipamentos	Sistema de videomonitoramento Vigilância armada
AT9	Desastres naturais	Manutenções periódicas Orçamento para melhorias e adequações Plano de contingência
	Acesso indevido ao espaço físico	Controle da chave de acesso
	Desastres naturais	Manutenções periódicas Orçamento para melhorias e adequações Plano de contingência
AT10	Restrições orçamentárias	Orçamento destinado para capacitação
	Falta de alinhamento com a administração superior	Vinculação das ações aos instrumentos de planejamento
	Contingenciamento de orçamento	Captação de recursos externos
AT11	Não entrega do objeto contratado	Exigência de atestados de capacidade técnica e verificação de saúde financeira no momento de seleção do fornecedor Verificação de cadastro de empresas inidôneas
	Inadimplência do fornecedor	Verificação de saúde financeira no momento de seleção do fornecedor, verificação de cadastro de empresas inidôneas
	Falência da empresa contratada	Verificação de saúde financeira no momento de seleção do fornecedor, verificação de cadastro de empresas inidôneas
	Manuseio indevido de informação sigilosa por parte da contratada	Assinar termos de compromisso de sigilo
	Quebra da integridade dos arquivos do banco de dados	Aplicação da política de backup
	Indisponibilidade além do nível de acordo de serviços (SLA) das aplicações	Manter ambiente redundante

AT12	que dependem do banco de dados	
AT13	Falha no ambiente de execução	Manter ambiente redundante
	Indisponibilidade do sistema por erro introduzido durante o processo de desenvolvimento de software	Controle de versionamento Aplicação do plano de desenvolvimento de software
AT14	Falha no ambiente de execução	Manter ambiente redundante
	Falta de suporte/atualização pelo desenvolvedor	Realizar a gestão patrimonial efetiva
AT15	Falha de hardware fora do prazo de garantia	Aplicação do plano de atualização do parque computacional da Unifesspa
	Falha de hardware dentro do período da garantia	Acionar a garantia
AT16	Indisponibilidade do provedor	Manter ambiente redundante
	Falha de hardware	Substituição de equipamentos Plano de contingência
	Desastres naturais	Manutenções periódicas Orçamento para melhorias e adequações Plano de contingência
AT17	Indisponibilidade do provedor	Manter ambiente redundante
	Falha de hardware	Substituição de equipamentos Plano de contingência
	Desastres naturais	Manutenções periódicas Orçamento para melhorias e adequações Plano de contingência
AT18	Indisponibilidade do serviço por ataque cibernético	Plano de contingência
	Falha de hardware	Substituição de equipamentos Plano de contingência
	Falha de Software	Atualizações periódicas Acionar suporte
AT19	Alteração do software	Aplicação das correções através da execução do plano de desenvolvimento de software
	Violação das condições de uso do sistema de informação que possibilitam sua	Norma de controle de propriedade e leis de direitos

	manutenção	autorais
	Falha humana	Capacitação dos usuários
AT20	Indisponibilidade do técnico	Realizar documentação dos processos
	Perda de dados	Manter ambiente redundante

5.1.4 Identificando as vulnerabilidades

Vulnerabilidade é qualquer fraqueza que possa ser explorada para comprometer a segurança de sistemas ou informações. Além disso, determina uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças, geralmente se apresenta no ambiente interno. O quadro 05 apresenta as principais vulnerabilidades identificados relacionadas as ameaças mapeadas no quadro 03:

Quadro 05 - Principais vulnerabilidades identificadas

Ativos	Vulnerabilidades	Tipo
AT1	Muitos processos concorrentes	Interna
	Ausência de capacitação do servidor	Interna e externa
	Ausência da definição do processo de contratação	Interna
AT2	Bolsista não capacitado	Interna
	Ausência de critérios objetivos para definição do perfil do candidato	Externa
	Ausência de mecanismos de avaliação	Interna
AT3	Não execução das atividades de acordo com o processo estabelecido	Interna
	Ausência de planejamento institucional	Externa
	Inexistência de processo de desenvolvimento de software	Interna
AT4	Ausência de políticas de gestão de problemas	Interna
	Ausência de conhecimento do catálogo de serviços de TIC do CTIC	Interna e externa
	Baixa experiência técnica	Interna
	Falta de informação para os usuários	Interna e externa
AT5	Ausência de conhecimento técnico no uso de ferramentas de monitoramento	Interna
	Efetiva execução do processo de monitoramento e melhoria contínua	Interna
	Ausência de ações proativas face a identificação de incidentes por meio do monitoramento	Interna
	Ausência do processo de monitoramento	Interna
AT6	Inexistência de políticas de capacitação de RH	Interna e externa
	Ausência de engajamento da equipe técnica	Interna e externa
	Ausência de capacitação profissional	Interna
AT7	Inexistência de controle de acesso físico	Interna
	Ausência de orçamento interno para manter a segurança física	Interna
	Acesso indevido ao espaço físico do Data Center	Interna e externa
	Ausência de mecanismos de controle para monitoramento das estruturas	Interna e externa
	Ausência de controle e ferramentas adequadas para o monitoramento da	Interna

	estrutura física	
AT8	Ausência de controle e ferramentas adequadas para manutenção das estruturas físicas	Interna
	Espaço sem monitoramento/segurança adequada	Interna
	Acesso indevido ao espaço físico	Interna e externa
	Ausência de orçamento interno para manter a estrutura do prédio	Interna
AT9	Ausência de controle e ferramentas adequadas para manutenção das estruturas físicas	Interna
	Falta de manutenção regular nos equipamentos/espaço	Interna e externa
	Ausência de mecanismos de controle para monitoramento do gerador	Interna
	Falta de limpeza do ambiente interno e externo	Interna
AT10	Falta de cursos de formação na área de gestão de pessoas	Interna
	Indisponibilidade dos gestores em participar de capacitação	Interna
	Ausência de formação em gestão de pessoas	Externa
AT11	Ausência de capacitação profissional	Interna
	Ausência de controle e ferramentas adequadas para gestão do contrato	Interna e externa
	Ausência de conhecimento do gestor do contrato sobre o objeto contratado	Interna
AT12	Manipulação direta de arquivos no servidor de gerenciamento de banco de dados	Interna e externa
	Desligamento não programado do serviço de gerenciamento de banco de dados	Interna
	Falta de atualização dos softwares de gestão das bases de dados	Interna e externa
AT13	Ambiente computacional de desenvolvimento do software e de operação inadequado	Interna
	Não seguir o processo de desenvolvimento de software	Interna
	Ausência de treinamentos para os usuários sobre o software desenvolvido	Externa
AT14	Ambiente computacional do software e de operação inadequado	Interna
	Não garantia de suporte de longo prazo para o software	Externa
	Ausência de treinamentos para os usuários sobre o software desenvolvido	Interna
AT15	Mau uso	Interna e externa
	Obsolescência	Interna
	Ausência de especificação do perfil de uso	Interna
AT16	Falta de atualização periódica dos ativos de rede	Interna
	Falta de plano de manutenção da infraestrutura de rede	Interna
	Ausência de orçamento interno para manter os serviços de internet	Interna
AT17	Falta de garantia de suporte a longo prazo para a solução	Externa
	Falta de atualização da agenda telefônica	Interna e externa
	Ausência de orçamento interno para manter os serviços de telefonia	Interna e externa
	Falta de atualização de software periódica da solução	Interna
	Falta de monitoramento e aplicação da política de uso de e-mail	Interna e

AT18		externa
	Falta de atualização das ferramentas de segurança do e-mail institucional	Interna e externa
AT19	Inexistência de um controle eficaz de mudança	Interna e externa
	Rotatividade dos responsáveis pelos dados	Interna
	Falta de padronização de entrada dos dados	Interna e externa
AT20	Falta de ferramenta adequada para gestão da informação	Interna
	Ausência de política de propriedade intelectual	Interna
	Falta de documentação dos procedimentos do setor	Interna
	Falta de processo estabelecidos	Interna

5.1.5 Identificando as consequências

Entende-se por consequência o resultado de um incidente ou evento que pode ter um impacto nos objetivos da organização. Na análise de riscos uma consequência pode ser por exemplo: a perda da eficácia no funcionamento operacional dos sistemas, instabilidade no funcionamento de sistemas, perda de oportunidade de negócios, entre outros.

Esta atividade visa identificar as consequências ou prejuízos para a organização que podem decorrer de um cenário de incidentes, fruto das vulnerabilidades identificadas. Ressalta-se que um cenário a descrição de uma ameaça explorando uma ou mais vulnerabilidades em um incidente. O quadro 06 apresenta as principais consequências identificadas relacionadas as ameaças mapeadas no quadro 03.

Quadro 06 - Principais consequências identificadas

Ativos	Ameaças	Consequências
AT1	Indisponibilidade da equipe de planejamento da contratação	Perda de oportunidade de negócios
	Alteração na legislação	Violação de obrigações regulatórias
	Exequibilidade do tempo para execução do processo de contratação	Prejuízo financeiro
	Interferência de empresa no processo de contratação a fim de direcionar ou restringir a competitividade	Perda de competitividade
	Interposição de pedidos impugnações de editais	Perda de oportunidade de negócios
	Falta de competência técnica da equipe de planejamento da contratação	Perda da integridade
	Licitação fracassada ou deserta	Perda da disponibilidade
AT2	Indisponibilidade de recursos	Perda de oportunidade de negócios
	Pouca demanda de candidatos	Prejuízo financeiro por retrabalho
	Candidatos com perfil/experiência incompatível	Condições adversas de operação
AT3	Alta demanda de desenvolvimento de software	Perda da eficácia no funcionamento operacional dos sistemas
	Número insuficiente de pessoas na equipe para execução do processo	Violação de obrigações regulatórias
AT4	Volume excessivo de chamados	Condições adversas de operação
	Crescimento da instituição	Condições adversas de operação
AT5	Ausência de ferramentas eficientes para monitoramento	Perda da eficácia no funcionamento operacional dos sistemas
	Expansão dos recursos de TIC	Condições adversas de operação
AT6	Diminuição dos incentivos para qualificação	Perda de competitividade
	Fuga de talentos	Condições adversas de operação
	Evolução tecnológica	Perda de competitividade
	Absenteísmo	Perda de oportunidade de negócios
AT7	Inadequação do espaço físico	Condições adversas de operação
	Desastres naturais	Perda de dados e informações
	Furto/Roubo de equipamentos	Perda da disponibilidade

AT8	Desastres naturais	Perda da disponibilidade
	Acesso indevido ao espaço físico	Violação de obrigações regulatórias
AT9	Desastres naturais	Perda da disponibilidade
	Restrições orçamentárias	Prejuízo financeiro
AT10	Falta de alinhamento com a administração superior	Perda de oportunidade de negócios
	Contingenciamento de orçamento	Prejuízo financeiro
	Não entrega do objeto contratado	Violação de obrigações regulatórias
	Inadimplência do fornecedor	Condições adversas de operação
AT11	Falência da empresa contratada	Condições adversas de operação
	Manuseio indevido de informação sigilosa por parte da contratada	Perda da confidencialidade
	Quebra da integridade dos arquivos do banco de dados	Perda da integridade
AT12	Indisponibilidade além do nível de acordo de serviços (SLA) das aplicações que dependem do banco de dados	Perda da disponibilidade
	Falha no ambiente de execução	Perda da disponibilidade
AT13	Indisponibilidade do sistema por erro introduzido durante o processo de desenvolvimento de software	Condições adversas de operação
	Falha no ambiente de execução	Perda da disponibilidade
AT14	Falta de suporte/atualização pelo desenvolvedor	Condições adversas de operação
	Falha de hardware fora do prazo de garantia	Violação de obrigações regulatórias
AT15	Falha de hardware dentro do período da garantia	Condições adversas de operação
	Indisponibilidade do provedor	Condições adversas de operação
AT16	Falha de hardware	Perda da disponibilidade
	Desastres naturais	Perda da disponibilidade
	Indisponibilidade do provedor	Condições adversas de operação
	Falha de hardware	Perda da disponibilidade
AT17	Desastres naturais	Perda da disponibilidade
	Indisponibilidade do serviço por ataque cibernético	Perda da disponibilidade
	Falha de hardware	Perda da disponibilidade

AT18	Falha de Software	Perda da disponibilidade
	Alteração do software	Condições adversas de operação
AT19	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	Perda da disponibilidade
	Falha humana	Perda da disponibilidade
AT20	Indisponibilidade do técnico	Condições adversas de operação
	Perda de dados	Perda da disponibilidade

5.2 Análise de riscos: avaliação da probabilidade e nível do risco

A partir da verificação dos resultados das fases anteriores, parte-se para a análise e avaliação dos riscos. Esta fase tem como objetivo principal descobrir as causas dos eventos de riscos, entender como será analisada a probabilidade de ocorrência deste evento e a consequência para a organização, utilizando como norteador limiar o apetite a risco da organização em todos essas variáveis.

Segundo o Orange Book (Orange Book, 2004), podemos considerar duas variáveis principais para a avaliação de riscos: a probabilidade desse risco ocorrer, e o impacto, caso ele venha a se materializar. A categorização adotada pelo CTIC para probabilidade, impacto, relevância e riscos neste Plano de Gestão de Riscos de TIC foram baseadas numa matriz 5x5 (cinco por cinco) e serão descritas abaixo, o produto resultante contendo o nível do risco foi classificado nas seguintes categorias: “Irrelevante”, “Baixo”, “Médio”, “Alto” e “Extremo”. Silva (Silva, 2015) cita em seu trabalho que as normal como Orange Book ou ABNT NBR ISO/IEC 27005 não possuem um padrão absoluto para a escala da matriz de riscos ou de classificações dos riscos, e que pode-se usar uma matriz e classificações que melhor se adeque a organização em estudo na presente avaliação dos riscos.

Sobre o critério de probabilidade, esse foi o direcionador para a avaliação da chance de ocorrência do evento, as causas que levam a esse evento e as consequências caso este evento se materialize. A partir destas definições é possível iniciar a fase de avaliação dos riscos, em que são analisadas a probabilidade e seu impacto. É importante frisar que a metodologia empregada neste Plano de Gestão de Riscos de TIC seguiu aspectos qualitativos e quantitativos, em que as percepções dos envolvidos no processo serão convertidos em valores ordinais de 1 (um) a 5 (cinco) tanto para a probabilidade quanto para o impacto. A partir disto serão realizadas operações algébricas simples como forma de avaliar o nível de risco do evento e o risco residual gerado após a implementação de controles.

Para o contexto do CTIC foi escolhida uma escala de cinco pontos para avaliação da probabilidade, em que cada uma possui uma chance de ocorrência e uma descrição diferenciada, conforme exposto na Tabela 01.

Tabela 01 – Critérios de probabilidade

Nível	Descrição	Valor
Improvável	Nunca ocorreu	1
Remoto	Ocorre somente 1 vez ao ano	2
Ocasional	Ocorre de 2 a 3 vez ao ano	3
Provável	Ocorre de 4 a 6 vezes ao ano	4
Frequente	Tem ocorrido mais de 6 vezes ao ano	5

Fonte: Próprio autor

Com relação ao critério de impacto definiu-se também uma escala de cinco alternativas, em que a base da avaliação é o atendimento dos objetivos estratégicos da organização, conforme a tabela 02. É importante perceber que a adaptação e/ou modificação destas métricas só pode ser realizada pelo Comitê de Riscos, e aprovada pelo CGD devido a necessidade de uniformização dos procedimentos de Gestão de Riscos de TIC em conformidade com o alinhamento estratégico (PDI, PDTIC, etc.) da organização, no caso a Unifesspa.

Tabela 02 – Critérios de impacto

Nível	Descrição	Valor
Desprezível	Sem danos ou com danos insignificantes aos equipamentos e/ou instalações e aos serviços.	1
Baixo	Danos leves aos equipamentos ou instalações, controláveis e/ou de baixo custo de reparo. Os sistemas ficaram fora de operação por até 30 minutos.	2
Significativo	Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	3
Importante	Provoca lesões moderadas em uma ou mais pessoas (na força de trabalho e/ou em pessoas externas). Danos reparáveis a equipamentos ou instalações (reparação lenta). Perda de dados. Clientes com atendimento parcial.	4
Desastre	Provoca morte ou lesões graves em uma ou mais pessoas (na força d e trabalho e/ou em pessoas externas). Danos irreparáveis a equipamentos ou instalações (reparação lenta ou impossível). Perda de dados e informações. Clientes sem atendimento total.	5

Fonte: Próprio autor

A partir destas duas definições: probabilidade e impacto, pode-se calcular o Risco Inerente (RI), ou apenas risco, do evento a partir da multiplicação das pontuações da probabilidade e do impacto, conforme representado na Equação 1. Nas seções abaixo até a conclusão desse plano iremos nos referir ao termo risco inerente apenas como risco, o que não se aplica para o termo de riscos residuais os quais continuarão a serem referidos como tal.

(1) RI (risco) = Probabilidade x Impacto

Esta multiplicação gera um valor numérico que varia de 01 (um) a 25 (vinte e cinco) e que representa o nível de risco do evento. No contexto da Unifesspa, o CTIC convencionou a partir do Comitê de Riscos, e dos princípios de governança e controles os limiares de classificação dos riscos apresentados na Tabela 03 e complementada de forma visual pela figura 05.

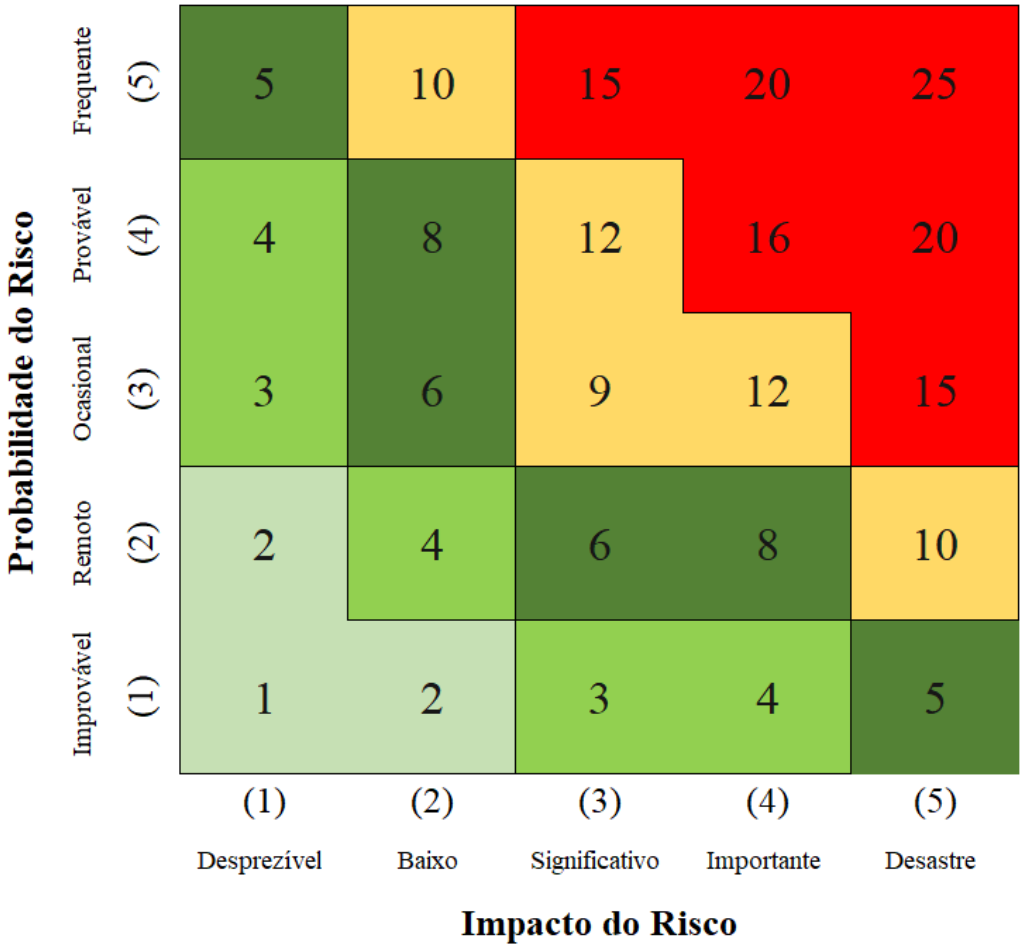
Tabela 03 – Classificação dos riscos

Risco	Descrição	Valor
Irrelevante	A organização interrompe totalmente seus serviços por mais de 1 hora, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.	≤ 2 entre 1 e 2
Baixo	A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.	> 2 e ≤ 4 entre 3 e 4
Médio	A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.	> 4 e ≤ 8 entre 5 e 8
Alto	A organização interrompe totalmente seus serviços por mais de 24 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.	> 8 e ≤ 14 entre 9 e 14
Extremo	A organização interrompe totalmente seus serviços por mais de 48 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.	> 14 e ≤ 25 entre 15 e 25

Fonte: Próprio autor

O cálculo necessário para definir o nível/grau de risco será realizado automaticamente, conforme a equação 1, necessitando que os gestores se preocupem apenas em definir a probabilidade e o impacto dos eventos identificados de acordo com as tabelas 01 e 02. Os eventos de riscos categorizados deverão passar por mecanismos de controle para que as ações como modificar (mitigar), reter (aceitar), evitar e compartilhar os riscos sejam devidamente implementadas.

Figura 05 – Matriz de risco



Fonte: Próprio autor

Conforme pode ser verificado na matriz de risco apresentada na figura 05, as margens da matriz apresentam os valores qualitativos e quantitativos dos critérios de probabilidade e impactos dos eventos. A adoção desta metodologia foi dada pela dificuldade de criação e aferição de indicadores que representem de maneira confiável as probabilidades de os eventos ocorrerem assim como o real impacto dos diversas eventos de caráter subjetivo, principalmente aqueles relacionados aos objetivos estratégicos.

O risco irrelevante é retratado pelo tom mais claro da cor verde. O evento receberá sempre essa classificação de risco quando o produto decorrente da multiplicação entre sua probabilidade e o seu impacto for menor ou igual a 2. O risco baixo é ilustrado pela cor verde padrão. O evento receberá sempre essa classificação de risco quando o produto decorrente da multiplicação entre sua probabilidade e o seu impacto for maior que 2 e menor ou igual a 4.

O risco médio é exibido pela cor verde escuro. O evento receberá sempre essa classificação de risco quando o produto decorrente da multiplicação entre sua probabilidade e o seu impacto for maior que 4 e menor ou igual a 8. O risco alto é representado pela cor amarela. O evento receberá sempre essa classificação de risco quando o produto decorrente da multiplicação entre sua probabilidade e o seu impacto for maior que 8 e menor ou igual a 14. Por fim o risco extremo é exibido pela cor vermelha. O evento receberá sempre essa classificação de risco quando o produto decorrente da multiplicação entre sua probabilidade e o seu impacto for maior que 14 e menor ou igual a 25.

Nesta etapa da análise de risco, que faz parte do processo de análise de risco, são tratadas as atividades de identificação das probabilidades de ocorrência e a determinação do nível de risco. Estas duas atividades irão compor a conclusão do processo de análise de risco.

Após a identificação dos cenários de incidentes e da avaliação das consequências, é necessário realizar a avaliação da probabilidade de riscos em cada cenário e dos impactos correspondentes. Nesta atividade é importantíssimo o uso do histórico de ocorrências de incidentes de segurança.

A determinação do nível de risco é uma atividade na qual a equipe de análise vai mensurar o nível de risco com o uso dos resultados obtidos nas etapas anteriores. Nesta atividade serão dados valores para a probabilidade e consequências do risco. O quadro 07 apresenta a avaliação de probabilidade, impacto e relevância dos ativos identificados no quadro 03:

Quadro 07 – Probabilidade, nível do risco identificados

Ativos	Consequências	Probabilidade	Impacto	Relevância
AT1	Perda de oportunidade de negócios	Provável: ocorre de 4 a 6 vezes ao ano	Significativo: lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Significante: interrompe parcialmente o acesso aos serviços
	Violação de obrigações regulatórias	Provável: ocorre de 4 a 6 vezes ao ano	Significativo: lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Significante: interrompe parcialmente o acesso aos serviços
	Prejuízo financeiro	Provável: ocorre de 4 a 6 vezes ao ano	Importante: provoca lesões moderadas em uma ou mais pessoas (na força de trabalho e/ou em pessoas externas). Danos reparáveis a equipamentos ou instalações (reparação lenta). Perda de dados. Clientes com atendimento parcial.	Significante: interrompe parcialmente o acesso aos serviços
	Perda de competitividade	Remoto: ocorre somente 1 vez ao ano	Importante: provoca lesões moderadas em uma ou mais pessoas (na força de trabalho e/ou em pessoas externas). Danos reparáveis a equipamentos ou instalações (reparação lenta). Perda de dados. Clientes com atendimento parcial.	Significante: interrompe parcialmente o acesso aos serviços
	Perda de oportunidade de negócios	Frequente: tem ocorrido mais de 6 vezes ao ano	Importante: provoca lesões moderadas em uma ou mais pessoas (na força de trabalho e/ou em pessoas externas). Danos reparáveis a equipamentos ou instalações (reparação lenta). Perda de dados. Clientes com atendimento parcial.	Importante: interrompe plenamente o acesso aos serviços e influência menos de que 50% dos ativos
	Perda da integridade	Remoto: ocorre somente 1 vez ao ano	Importante: provoca lesões moderadas em uma ou mais pessoas (na força de trabalho e/ou em pessoas externas). Danos reparáveis a equipamentos ou instalações (reparação lenta). Perda de dados.	Importante: interrompe plenamente o acesso aos serviços e influência menos de que 50% dos ativos

			Clientes com atendimento parcial.	
	Perda da disponibilidade	Remoto: ocorre somente 1 vez ao ano	Baixo: danos leves aos equipamentos ou instalações, controláveis e/ou de baixo custo de reparo. Os sistemas ficaram fora de operação por até 30 minutos.	Baixo: interrompe um pouco o acesso aos serviços
AT2	Perda de oportunidade de negócios	Provável: ocorre de 4 a 6 vezes ao ano	Significativo: lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
	Prejuízo financeiro por retrabalho	Ocasional: ocorre de 2 a 3 vezes ao ano	Significativo: lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Baixo: interrompe um pouco o acesso aos serviços
	Condições adversas de operação	Provável: ocorre de 4 a 6 vezes ao ano	Significativo: lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Baixo: interrompe um pouco o acesso aos serviços
AT3	Perda da eficácia no funcionamento operacional dos sistemas	Frequente: tem ocorrido mais de 6 vezes ao ano	Importante: provoca lesões moderadas em uma ou mais pessoas (na força de trabalho e/ou em pessoas externas). Danos reparáveis a equipamentos ou instalações (reparação lenta). Perda de dados. Clientes com atendimento parcial.	Significante: interrompe parcialmente o acesso aos serviços
	Violação de obrigações regulatórias	Provável: ocorre de 4 a 6 vezes ao ano	Importante: provoca lesões moderadas em uma ou mais pessoas (na força de trabalho e/ou em pessoas externas). Danos reparáveis a equipamentos ou instalações (reparação lenta). Perda de dados. Clientes com atendimento parcial.	Importante: interrompe plenamente o acesso aos serviços e influência menos de que 50% dos ativos
AT4	Condições adversas de operação	Frequente: tem ocorrido mais	Significativo: lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os	Significante: interrompe parcialmente o acesso aos serviços

		de 6 vezes ao ano	sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	
	Condições adversas de operação	Ocasional: Ocorre de 2 a 3 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Significante: Interrompe parcialmente o acesso aos serviços
AT5	Perda da eficácia no funcionamento operacional dos sistemas	Remoto: Ocorre somente 1 vez ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
	Condições adversas de operação	Remoto: Ocorre somente 1 vez ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Significante: Interrompe parcialmente o acesso aos serviços
	Perda de competitividade	Provável: Ocorre de 4 a 6 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Baixo: Interrompe um pouco o acesso aos serviços
AT6	Condições adversas de operação	Provável: Ocorre de 4 a 6 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Significante: Interrompe parcialmente o acesso aos serviços
	Perda de competitividade	Frequente: Tem ocorrido mais de 6 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Significante: Interrompe parcialmente o acesso aos serviços
	Perda de oportunidade de negócios	Provável: Ocorre de 4 a 6 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de	Significante: Interrompe parcialmente o acesso aos serviços

			30 minutos. Necessidade de recuperar backup.	
AT7	Condições adversas de operação	Frequente: Tem ocorrido mais de 6 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
AT8	Perda de dados e informações	Improvável: Nunca ocorreu	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
	Perda da disponibilidade	Improvável: Nunca ocorreu	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
AT9	Perda da disponibilidade	Improvável: Nunca ocorreu	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Significante: Interrompe parcialmente o acesso aos serviços
	Violação de obrigações regulatórias	Improvável: Nunca ocorreu	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
AT10	Perda da disponibilidade	Improvável: Nunca ocorreu	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
	Prejuízo financeiro	Provável: Ocorre de 4 a 6 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Significante: Interrompe parcialmente o acesso aos serviços

	Perda de oportunidade de negócios	Remoto: Ocorre somente 1 vez ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Significante: Interrompe parcialmente o acesso aos serviços
	Prejuízo financeiro	Ocasional: Ocorre de 2 a 3 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Importante: Interrompe plenamente o acesso aos serviços e influência menos de que 50% dos ativos
AT11	Violação de obrigações regulatórias	Ocasional: Ocorre de 2 a 3 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
	Condições adversas de operação	Remoto: Ocorre somente 1 vez ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
	Condições adversas de operação	Remoto: Ocorre somente 1 vez ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
	Perda da confidencialidade	Improvável: Nunca ocorreu	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Importante: Interrompe plenamente o acesso aos serviços e influência menos de que 50% dos ativos
AT12	Perda da integridade	Remoto: Ocorre somente 1 vez ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
	Perda da disponibilidade	Remoto:	Significativo: Lesões leves em pessoas. Danos	Crítico: Interrompe plenamente o

		Ocorre somente 1 vez ao ano	severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	acesso aos serviços e influência mais de 50% dos ativos
AT13	Perda da disponibilidade	Frequente: Tem ocorrido mais de 6 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Importante: Interrompe plenamente o acesso aos serviços e influência menos de que 50% dos ativos
	Condições adversas de operação	Frequente: Tem ocorrido mais de 6 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Significante: Interrompe parcialmente o acesso aos serviços
AT14	Perda da disponibilidade	Ocasional: Ocorre de 2 a 3 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
	Condições adversas de operação	Frequente: Tem ocorrido mais de 6 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Significante: Interrompe parcialmente o acesso aos serviços
AT15	Violação de obrigações regulatórias	Ocasional: Ocorre de 2 a 3 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Significante: Interrompe parcialmente o acesso aos serviços
	Condições adversas de operação	Remoto: Ocorre somente 1 vez ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Baixo: Interrompe um pouco o acesso aos serviços
	Condições adversas de operação	Ocasional: Ocorre de 2 a 3	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os	Crítico: Interrompe plenamente o acesso aos serviços e influência mais

		vezes ao ano	sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	de 50% dos ativos
AT16	Perda da disponibilidade	Improvável: Nunca ocorreu	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
	Perda da disponibilidade	Improvável: Nunca ocorreu	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
	Condições adversas de operação	Frequente: Tem ocorrido mais de 6 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
AT17	Perda da disponibilidade	Frequente: Tem ocorrido mais de 6 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
	Perda da disponibilidade	Improvável: Nunca ocorreu	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
	Perda da disponibilidade	Ocasional: Ocorre de 2 a 3 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos
AT18	Perda da disponibilidade	Improvável: Nunca ocorreu	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de	Crítico: Interrompe plenamente o acesso aos serviços e influência mais de 50% dos ativos

			30 minutos. Necessidade de recuperar backup.	
	Perda da disponibilidade	Improvável: Nunca ocorreu	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Importante: Interrompe plenamente o acesso aos serviços e influência menos de que 50% dos ativos
	Condições adversas de operação	Improvável: Nunca ocorreu	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Significante: Interrompe parcialmente o acesso aos serviços
AT19	Perda da disponibilidade	Remoto: Ocorre somente 1 vez ao ano	Baixo: Danos leves aos equipamentos ou instalações, controláveis e/ou de baixo custo de reparo. Os sistemas ficaram fora de operação por até 30 minutos.	Baixo: Interrompe um pouco o acesso aos serviços
	Perda da disponibilidade	Remoto: Ocorre somente 1 vez ao ano	Baixo: Danos leves aos equipamentos ou instalações, controláveis e/ou de baixo custo de reparo. Os sistemas ficaram fora de operação por até 30 minutos.	Baixo: Interrompe um pouco o acesso aos serviços
AT20	Condições adversas de operação	Frequente: Tem ocorrido mais de 6 vezes ao ano	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Baixo: Interrompe um pouco o acesso aos serviços
	Perda da disponibilidade	Improvável: Nunca ocorreu	Significativo: Lesões leves em pessoas. Danos severos a equipamentos e/ou instalações. Os sistemas de TI ficaram fora de operação acima de 30 minutos. Necessidade de recuperar backup.	Importante: Interrompe plenamente o acesso aos serviços e influência menos de que 50% dos ativos

5.3 Análise de riscos: 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 as equipes 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. O quadro 08 apresenta a avaliação de severidade e critério de risco identificados nas ameaças mapeadas no quadro 03:

Quadro 08 – Severidade e critério de risco mapeados

Ativos	Ameaças	Severidade	Critério de risco
AT1	Indisponibilidade da equipe de planejamento da contratação	Baixa: Integridade não é afetada e pode haver indisponibilidade de até 2 dias	Extremo: A organização interrompe totalmente seus serviços por mais de 48 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Alteração na legislação	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Alto: A organização interrompe totalmente seus serviços por mais de 24 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Exequibilidade do tempo para execução do processo de contratação	Baixa: Integridade não é afetada e pode haver indisponibilidade de até 2 dias	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Interferência de empresa no processo de contratação a fim de direcionar ou restringir a competitividade	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Interposição de pedidos impugnações de editais	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Falta de competência técnica da equipe de planejamento da contratação	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Licitação fracassada ou deserta	Baixa: Integridade não é afetada e pode haver indisponibilidade de até 2 dias	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT2	Indisponibilidade de recursos	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Pouca demanda de	Média: Integridade não é afetada e pode	Médio: A organização interrompe totalmente seus serviços por

	candidatos	haver indisponibilidade de até 5 horas	mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Candidatos com perfil/experiência incompatível	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT3	Alta demanda de desenvolvimento de software	Alta: Integridade corrompida dos dados do SIG e indisponibilidade dos serviços de até 1 hora com algum controle	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Número insuficiente de pessoas na equipe para execução do processo	Alta: Integridade corrompida dos dados do SIG e indisponibilidade dos serviços de até 1 hora com algum controle	Alto: A organização interrompe totalmente seus serviços por mais de 24 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT4	Volume excessivo de chamados	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Crescimento da instituição	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT5	Ausência de ferramentas eficientes para monitoramento	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Expansão dos recursos de TIC	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Diminuição dos incentivos para qualificação	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT6	Fuga de talentos	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.

	Evolução tecnológica	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Absenteísmo	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT7	Inadequação do espaço físico	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Alto: A organização interrompe totalmente seus serviços por mais de 24 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Desastres naturais	Alta: Integridade corrompida dos dados do SIG e indisponibilidade dos serviços de até 1 hora com algum controle	Extremo: A organização interrompe totalmente seus serviços por mais de 48 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT8	Furto/Roubo de equipamentos	Alta: Integridade corrompida dos dados do SIG e indisponibilidade dos serviços de até 1 hora com algum controle	Extremo: A organização interrompe totalmente seus serviços por mais de 48 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Desastres naturais	Alta: Integridade corrompida dos dados do SIG e indisponibilidade dos serviços de até 1 hora com algum controle	Extremo: A organização interrompe totalmente seus serviços por mais de 48 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT9	Acesso indevido ao espaço físico	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Desastres naturais	Alta: Integridade corrompida dos dados do SIG e indisponibilidade dos serviços de até 1 hora com algum controle	Extremo: A organização interrompe totalmente seus serviços por mais de 48 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT10	Restrições orçamentárias	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Falta de alinhamento com a administração superior	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Alto: A organização interrompe totalmente seus serviços por mais de 24 horas, impedindo de executar serviços e produzir,

			afetando sua imagem pública de forma significativa.
AT11	Contingenciamento de orçamento	Alta: Integridade corrompida dos dados do SIG e indisponibilidade dos serviços de até 1 hora com algum controle	Alto: A organização interrompe totalmente seus serviços por mais de 24 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Não entrega do objeto contratado	Alta: Integridade corrompida dos dados do SIG e indisponibilidade dos serviços de até 1 hora com algum controle	Alto: A organização interrompe totalmente seus serviços por mais de 24 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Inadimplência do fornecedor	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Extremo: A organização interrompe totalmente seus serviços por mais de 48 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Falência da empresa contratada	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Extremo: A organização interrompe totalmente seus serviços por mais de 48 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Manuseio indevido de informação sigilosa por parte da contratada	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT12	Quebra da integridade dos arquivos do banco de dados	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Extremo: A organização interrompe totalmente seus serviços por mais de 48 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Indisponibilidade além do nível de acordo de serviços (SLA) das aplicações que dependem do banco de dados	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT13	Falha no ambiente de execução	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Indisponibilidade do sistema por erro introduzido durante	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir,

	o processo de desenvolvimento de software		afetando sua imagem pública de forma significativa.
AT14	Falha no ambiente de execução	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Falta de suporte/atualização pelo desenvolvedor	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT15	Falha de hardware fora do prazo de garantia	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Alto: A organização interrompe totalmente seus serviços por mais de 24 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Falha de hardware dentro do período da garantia	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT16	Indisponibilidade do provedor	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Alto: A organização interrompe totalmente seus serviços por mais de 24 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Falha de hardware	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Alto: A organização interrompe totalmente seus serviços por mais de 24 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Desastres naturais	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Extremo: A organização interrompe totalmente seus serviços por mais de 48 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Indisponibilidade do provedor	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Extremo: A organização interrompe totalmente seus serviços por mais de 48 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT17	Falha de hardware	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Extremo: A organização interrompe totalmente seus serviços por mais de 48 horas, impedindo de executar serviços e produzir,

			afetando sua imagem pública de forma significativa.
	Desastres naturais	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Extremo: A organização interrompe totalmente seus serviços por mais de 48 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT18	Indisponibilidade do serviço por ataque cibernético	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Falha de hardware	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Alto: A organização interrompe totalmente seus serviços por mais de 24 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Falha de Software	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT19	Alteração do software	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	Baixa: Integridade não é afetada e pode haver indisponibilidade de até 2 dias	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Falha humana	Baixa: Integridade não é afetada e pode haver indisponibilidade de até 2 dias	Baixo: A organização interrompe totalmente seus serviços por mais de 10 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
AT20	Indisponibilidade do técnico	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Médio: A organização interrompe totalmente seus serviços por mais de 12 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.
	Perda de dados	Média: Integridade não é afetada e pode haver indisponibilidade de até 5 horas	Alto: A organização interrompe totalmente seus serviços por mais de 24 horas, impedindo de executar serviços e produzir, afetando sua imagem pública de forma significativa.

6. Tratamento e aceitação de riscos

A fase de tratamento de risco é realizada após as fases de definição do contexto, análise de riscos e avaliação de riscos. Ao final destas três fases, a equipe faz uma análise crítica dos resultados e verifica a situação dos trabalhos desenvolvidos.

O tratamento de risco é utilizado para responder aos riscos identificados. As escolhas e decisões tomadas devem levar em conta: a avaliação do tratamento de risco proposto já realizado, viabilidade técnica e financeira, eficácia dos controles, eficiência do tratamento, decisão se os níveis de risco residual são toleráveis e as características do negócio da organização.

Essa fase possui quatro opções, que não são mutuamente exclusivas:

- Modificar é a ação de implementar controles para reduzir os riscos a um nível aceitável: correção, eliminação, prevenção, minimização do impacto, dissuasão, detecção, recuperação, monitoramento, conscientização.
- Reter: significa a aceitação do risco de uma perda, ou seja, “correr o risco”, incluindo ainda os riscos que não tenham sido identificados"
- Evitar: eliminação da atividade ou processo gerador do risco através de mudanças na forma de sua ocorrência.
- Compartilhar: envolve a transferência ou compartilhamento dos riscos com uma entidade externa. Uma forma de compartilhamento do risco é o uso de seguros que cubram as consequências da ocorrência de um incidente.

Além disso, riscos residuais são aqueles que restam após a implantação de controles para evitar, transferir ou mitigar riscos. Após a implementação de um controle, pode ser que o risco não tenha sido mitigado, esta diferença é o risco residual que devem ser tratados através da implementação de controles. Caso o risco esteja acima do nível de aceitação de riscos estabelecido pela organização, pode ser necessária nova iteração. Entre os riscos residuais incluem-se também os riscos sem importância. O quadro 09 apresenta os principais tratamentos aos riscos identificadas relacionadas aos ativos mapeados no quadro 01:

Quadro 09 - Principais ameaças identificadas

Ativos	Ameaças	Prioridade	Risco (P X I)*	Tratamento
AT1	Indisponibilidade da equipe de planejamento da contratação	4	Alto	Modificar
	Alteração na legislação	5	Alto	Modificar
	Exequibilidade do tempo para execução do processo de contratação	4	Alto	Modificar
	Interferência de empresa no processo de contratação a fim de direcionar ou restringir a competitividade	3	Médio	Modificar
	Interposição de pedidos impugnações de editais	4	Alto	Modificar
	Falta de competência técnica da equipe de planejamento da contratação	4	Médio	Modificar
	Licitação fracassada ou deserta	3	Baixo	Reter
AT2	Indisponibilidade de recursos	1	Alto	Modificar
	Pouca demanda de candidatos	2	Alto	Modificar
	Candidatos com perfil/experiência incompatível	4	Alto	Modificar
AT3	Alta demanda de desenvolvimento de software	4	Alto	Modificar
	Número insuficiente de pessoas na equipe para execução do processo	4	Alto	Modificar
AT4	Volume excessivo de chamados	4	Alto	Modificar
	Crescimento da instituição	2	Alto	Modificar
AT5	Ausência de ferramentas eficientes para monitoramento	1	Alto	Modificar
	Expansão dos recursos de TIC	2	Alto	Modificar
AT6	Diminuição dos incentivos para qualificação	3	Alto	Modificar
	Fuga de talentos	2	Alto	Modificar
	Evolução tecnológica	4	Alto	Modificar
	Absenteísmo	4	Alto	Reter

	Inadequação do espaço físico	3	Alto	Modificar
AT7	Desastres naturais	1	Alto	Reter
	Furto/Roubo de equipamentos	1	Alto	Reter
AT8	Desastres naturais	3	Alto	Modificar
	Acesso indevido ao espaço físico	5	Alto	Modificar
AT9	Desastres naturais	1	Alto	Reter
	Restrições orçamentárias	2	Alto	Modificar
AT10	Falta de alinhamento com a administração superior	1	Alto	Modificar
	Contingenciamento de orçamento	3	Alto	Modificar
	Não entrega do objeto contratado	5	Alto	Modificar
AT11	Inadimplência do fornecedor	4	Alto	Modificar
	Falência da empresa contratada	2	Alto	Reter
	Manuseio indevido de informação sigilosa por parte da contratada	1	Alto	Evitar
	Quebra da integridade dos arquivos do banco de dados	3	Alto	Modificar
AT12	Indisponibilidade além do nível de acordo de serviços (SLA) das aplicações que dependem do banco de dados	5	Alto	Modificar
AT13	Falha no ambiente de execução	4	Alto	Modificar
	Indisponibilidade do sistema por erro introduzido durante o processo de desenvolvimento de software	5	Alto	Modificar
AT14	Falha no ambiente de execução	4	Alto	Modificar
	Falta de suporte/atualização pelo desenvolvedor	4	Alto	Modificar
AT15	Falha de hardware fora do prazo de garantia	5	Alto	Modificar
	Falha de hardware dentro do período da garantia	5	Alto	Compartilhar
	Indisponibilidade do provedor	3	Alto	Compartilhar
AT16	Falha de hardware	3	Alto	Compartilhar

	Desastres naturais	2	Alto	Reter
	Indisponibilidade do provedor	1	Alto	Compartilhar
	Falha de hardware	2	Alto	Compartilhar
AT17	Desastres naturais	3	Alto	Reter
	Indisponibilidade do serviço por ataque cibernético	1	Alto	Modificar
	Falha de hardware	5	Alto	Compartilhar
AT18	Falha de Software	1	Alto	Compartilhar
	Alteração do software	2	Alto	Modificar
AT19	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	4	Alto	Modificar
	Falha humana	3	Baixo	Modificar
	Indisponibilidade do técnico	5	Alto	Modificar
AT20	Perda de dados	3	Alto	Modificar

* Risco (P x I): Probabilidade x Impacto

7. Comunicação e monitoramento dos riscos

Durante a análise de riscos, existem duas fases que se desenvolvem simultaneamente às demais fases: a comunicação e o monitoramento dos riscos. Comunicação do risco é uma troca interativa de informações, conhecimentos e percepções sobre como os riscos devem ser gerenciados, documentados formalmente e de forma contínua, sendo também realizada entre a equipe envolvida e as partes interessadas nas decisões do processo de análise de riscos, sendo uma atividade crítica para o sucesso.

O monitoramento é definido como a observação contínua e registro regular das atividades e ações da gestão de riscos, é um processo contínuo de coleta de informações em todos os seus aspectos. Monitorar é verificar e acompanhar o progresso das atividades, ou seja, uma observação sistemática, regular e com propósito de verificar o desenvolvimento de todo o processo.

A análise crítica é uma avaliação geral e criteriosa sobre os resultados e ações da gestão de riscos com relação a requisitos preestabelecidos, com o objetivo de fazer o levantamento e a identificação de problemas e pontos de melhoria, para com isso solucionar os problemas e aprimorar continuamente.

A comunicação e atualização deste plano de riscos se realizará através de publicações no site: https://governancadigital.unifesspa.edu.br/. O monitoramento e melhorias no processo ficarão a cargo do CTIC junto com a CGTI, desse modo, poderão se formar novas comissões de elaboração e monitoria para gerenciar o processo da gestão de riscos. Além disso, este documento deverá ser revisado anualmente pelo Comitê de Governança Digital (CGD), de modo a atualizar suas diretrizes e alinhamentos estratégicos.

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 Unifesspa através do CTIC, 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.

1ª revisão do plano de riscos de TIC

Tendo em vista que o gerenciamento de riscos de TIC é um mecanismo dinâmico e ativo dentro das instituições, foi elaborada a primeira revisão do plano visando principalmente adequar os controles, suas ameças e vulnerabilidades.

Nessa revisão foram ajustados os principais controles, analisando principalmente seu escopo e viabilidade desde a aprovação no CGD em 2020, além disso, também foi analisada a proposta de implementação dessas ações e seus status. O quadro 10 lista as mudanças ocorridas nesta revisão.

Quadro 10 – Atualização dos controles e seus status de implementação

Ativo	Gestor do Ativo	Ameaças Prioritárias	Controles Definidos	Situação (26/03)	Proposta de implementação (09/05/2021)
Sistema Gerador de Energia do Data Center	Gestor do DIRSI	Acesso indevido ao espaço físico	Criação de formulário de quem acessa as salas	Não implementado	Não implementado
			Listagem de quem pode acessar a edícula	-	-
Processo de Contratação de TIC	Gestor de DICTI	Alteração na legislação	Capacitação e acompanhamento no portal de compras do governo	Implementado	Implementado
		Indisponibilidade da equipe de Planejamento da contratação	Indicação de Suplentes	Implementado	Implementado
		Falta de competência técnica da equipe de planejamento da contratação	Cursos de capacitação e composição de equipe de planejamento com membros de outros de unidades que possam colaborar	Parcialmente Implementado	Parcialmente Implementado
		Exequibilidade do tempo para execução do processo de contratação	Monitorar o tempo de permanência do processo em cada Unidade envolvida	Não implementado	Parcialmente Implementado
Processo de Seleção de Bolsista de TI	Gestor da CACP	Candidatos com perfil/experiência incompatível	Participação do gestor da área/equipe de estágio no processo seletivo	Não implementado	Não implementado

		Pouca demanda de candidatos	Divulgação nas redes sociais e dentro das turmas	Implementado	Implementado
Estações de trabalho da equipe de TIC	Gestores da CACP e CAU	Falha de hardware fora do prazo de garantia.	Mapeamento dos ativos por tempo de garantia	Não implementado	Não implementado
		Falha de hardware dentro do período da garantia.	Acionar a garantia do equipamento / Renovar / Controle de incidente	Parcialmente Implementado	Parcialmente Implementado
Suporte aos usuário de TIC	Gestor da CAU	Volume excessivo de chamados	Identificar e tratar causas raízes	Parcialmente Implementado	Parcialmente Implementado
			Funil da implantação do Serviço	Parcialmente Implementado	Parcialmente Implementado
Equipe Técnica do CTIC	Gestor do CTIC	Absenteísmo	Criar indicador sobre os relatório de atividades	Não implementado	Parcialmente Implementado
		Evolução tecnológica	Promover cursos de formação e participação de eventos de tecnologia	Parcialmente Implementado	Parcialmente Implementado
Prédio do CTIC	Gestor do CTIC	Furto/Roubo de equipamentos	Implantar sistema de videomonitoramento e alarmes em locais de circulação no prédio | Fechaduras eletrônicas	Não implementado	Não implementado
Gestores do CTIC	Gestor do CTIC	Restrições orçamentárias	Definir prioridade e reserva de contingência (Criação de PI)	Parcialmente Implementado	Parcialmente Implementado
		Falta de alinhamento com a	Participação das reuniões de	Implementado	Implementado

		Administração Superior	conselhos, CAS e ter reunião periódicas		
Processo de gestão de contratos de TIC	Gestor do CTIC	Não entrega do objeto contratado	Indicação de fiscais qualificados	Parcialmente Implementado	Implementado
		Não entrega do objeto contratado	Promover capacitações sobre gestão do contrato	-	-
		Inadimplência do fornecedor	Promover penalidade para os fornecedores inadimplentes	Não implementado	Implementado
Gestão de Conhecimento	Gestor do CTIC	Indisponibilidade do técnico	Promover elaboração de processos internos pelas equipes	Parcialmente Implementado	Parcialmente Implementado
		Perda de dados	Promover e fiscalizar a execução da política de Backup	Parcialmente Implementado	Parcialmente Implementado
Processo de Desenvolvimento de Software	Gestor da DISI	Alto demanda de desenvolvimento de software	Avaliar viabilidade técnica e submeter análise ao CGD solicitando recursos adicionais quando for o caso.	Parcialmente Implementado	Parcialmente Implementado
			Definir critérios para priorização dos projetos	-	-
Softwares mantidos pela UNIFESSPA	Gestor da DISI	Indisponibilidade do sistema por erro introduzido durante o processo de desenvolvimento de software.	Priorizar a correção imediata	Parcialmente Implementado	Implementado
			Criação do Processo de Qualidade de Software	-	-
Softwares não mantidos	Gestor da DISI	Falha no ambiente de execução.	Acionar suporte do mantenedor.	Implementado	Implementado

pela UNIFESSPA		Falta de suporte/atualização pelo desenvolvedor.	Capacitar a equipe para assumir a manutenção ou avaliar alternativas de software.	Não implementado	Não implementado
Processo de Monitoramento dos recurso de TIC	Gestor da DIRSI	Expansão dos recursos de TIC	Rotina de atualização dos ativos monitorados nas ferramentas	Implementado	Implementado
Estrutura física do Data Center	Gestor da DIRSI	Inadequação do espaço físico	Realizar melhorias no espaço físico - Fechamento das janelas	Parcialmente Implementado	Parcialmente Implementado
Bancos de dados dos ambientes de produção	Gestor da DIRSI	Quebra da integridade dos arquivo de banco de dados.	Controle de acesso (permissão) aos DBs	Parcialmente Implementado	Implementado
		Indisponibilidade além do nível de acordo de serviços (SLA) das aplicações que dependem do banco de dados.	Monitorar e notificar os responsáveis pelo serviço para que o atendimento seja o mais breve possível	Parcialmente Implementado	Parcialmente Implementado
Serviço de Internet	Gestor da DIRSI	Indisponibilidade do provedor	Contratação de link redundante	Não implementado	Não implementado
		Falha de hardware	Aquisição de ativos de reserva	Parcialmente Implementado	Parcialmente Implementado
Serviço de telefonia	Gestor da DIRSI	Falha de hardware	Aquisição de ativos de reserva	Parcialmente Implementado	Parcialmente Implementado
Serviço de e-mail	Gestor da DIRSI	Indisponibilidade do serviço por ataque cibernético	Manter ambiente interno preparado para voltar a atuar como provedor de e-mail principal	Não implementado	Implementado

Processo de atualização dos dados abertos	Gestor do CGTI	Falha humana	Fomentar a capacitação das Unidades responsáveis pelos Dados	Parcialmente Implementado	Parcialmente Implementado

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31000: Gestão
de riscos - princípios e diretrizes, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31010: Gestão
de riscos - técnicas para o processo de avaliação de riscos, 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT ISO GUIA 73:Gestão de riscos – Vocabulário, 2009.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. Governança de tecnologia da informação: artefato gestão de riscos de TIC / Ministério do Planejamento, Desenvolvimento e Gestão, Secretaria de Coordenação e Governança das Empresas Estatais, Coordenação-Geral de Gestão da Informação de Estatais; Universidade de Brasília – Brasília: MP, 2018. 21p

SILVA, Bruno José Pereira. Proposta de modelo de gestão de riscos para uma IFES visando a realização de auditoria baseada em riscos. 2015. 191f. Dissertação (Mestrado Profissional em Gestão de Processos Institucionais) - Centro de Ciências Humanas, Letras e Artes, Universidade Federal do Rio Grande do Norte, Natal, 2015.

ORANGE BOOK, UK Treasury Orange. Management of Risk Principles and Concepts. HM Treasury, Crown, London, 2004.

TRIBUNAL DE CONTAS DA UNIÃO. Governança Pública - Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública e Ações Indutoras de Melhoria. Brasil, 2014.

KONZEN, Marcos Paulo et al. Gestão de Riscos de Segurança da Informação Baseada na Norma NBR ISO/IEC 27005. Usando Padrões de Segurança, 2013.