PROCESSO DE GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO DA REDE EBSERH

EBSERH
HOSPITAIS UNIVERSITÁRIOS FEDERAIS

Identificação geral

CNPJ	15.126.437/0001-43
Administração Central	Brasília-DF
Tipo de estatal	Empresa Pública
Acionista controlador	União
Tipo societário	Sociedade por Cotas de Responsabilidade Limitada – Empresa Pública
Tipo de capital	Fechado
Abrangência de atuação	Nacional
Setores de atuação	Educação e Saúde
Presidente	**Oswaldo de Jesus Ferreira** Telefone: (61) 3255-8921 E-mail: oswaldo.ferreira@ebserh.gov.br
Auditor Interno	**Adriano Augusto de Souza** Telefone: (61) 3255-8970 E-mail: souza.adriano@ebserh.gov.br
Auditores independentes atuais Empresa	**Russel Bedford Auditores Independentes S/S** Telefone: (61) 3041-9592 ou (61) 3041-9500
Membros da Diretoria Executiva	**Oswaldo de Jesus Ferreira** Cargo: Presidente CPF: ***.430.927-** **Eduardo Chaves Vieira** Cargo: Vice-Presidente CPF: ***.431.577-** **Giuseppe Cesare Gatto** Cargo: Diretor de Ensino, Pesquisa e Atenção à Saúde CPF: ***.214.558-** **Simone Henriqueta Cossetin Scholze** Cargo: Diretora de Tecnologia da Informação CPF: ***.824.541-** **Iara Ferreira Pinheiro** Cargo: Diretora de Orçamento e Finanças CPF: ***.894.661-** **Erlon Cesar Dengo** Cargo: Diretor de Administração e Infraestrutura CPF: ***.884.910-** **Rodrigo Augusto Barbosa** Cargo: Diretor de Gestão de Pessoas CPF: ***.368.831-**
Equipe de Elaboração	Victor Alex Begnini Eliane Cunha Marques André Gomes Alay Esteves Cláudia Brandão Gonçalves Silva Wesley Rodrigo Couto Lira Fabiano Francisco Noetzold Saldanha Gustavo Tibau Do Espirito Santo Alves Rodrigo Vaz dos Santos Rodrigo de Souza Rezende
Data da Divulgação	07/06/2022
Versão	1.0

Sumário

1. Introdução

A Empresa Brasileira de Serviços Hospitalares – Ebserh traz em sua missão institucional a busca contínua pelo aprimoramento da gestão hospitalar, da prestação dos serviços de saúde e de serviços de apoio ao ensino e à pesquisa. Diante do desafio de administrar uma rede de hospitais universitários federais distribuídos pelo país, o papel da tecnologia da informação tem se tornado cada vez mais importante no enriquecimento dos processos organizacionais e estratégico para o atingimento dos objetivos institucionais.

Atualmente a Ebserh é uma rede de hospitais com 40 unidades e tem na sua Diretoria de Tecnologia de Informação o órgão responsável por promover a transformação digital da rede de hospitais universitários federais (HUF). Além da gestão de ações centralizadas ou compartilhadas para a provisão da infraestrutura de TI, a DTI desenvolve, dissemina e dá sustentação a um conjunto de sistemas de informação, entre os quais se destaca o Aplicativo de Gestão para Hospitais Universitários - AGHU.

2. Processo de Gestão de Riscos de Tecnologia da Informação

O Processo de Gestão de Riscos de Tecnologia da Informação (PGRTI) é baseado nas práticas definidas pelas normas ABNT NBR ISO/IEC 27005:2019 e ABNT NBR ISO/IEC 31010:2018 e adaptadas para o ambiente organizacional da Ebserh, devendo, para isto, ter apoio total e irrestrito por parte da Diretoria de Tecnologia da Informação.

Para que tais diretrizes possam ser executadas, contudo, as áreas de TI contarão com o apoio institucional do Representante de TI da Sede e dos Hospitais Universitários Federais (HUF).

Assim como os demais Processos de gestão da Ebserh, o Processo de GRTI deve estar devidamente alinhado com o planejamento estratégico de TI da Ebserh e, também, deve ser executado continuamente, adotando um ciclo de melhoria contínua, através do Subprocesso Monitorar Riscos, descrito na Seção 2.7, e também, visando monitorar a entrega de valor gerada pelo Processo, para isso, foi estabelecido um conjunto de Fatores Críticos de Sucesso, cuja apuração está descrita na Seção 3.

Este Processo está estruturado de forma a ser utilizado continuamente e sistematicamente, com o propósito de assegurar a proteção adequada dos ativos de TI da organização, envolvendo pessoas, Processos de negócio, informações, dados, soluções e serviços.

Para que o Processo de Gestão de Riscos de TI gere resultados efetivos e eficazes, os seguintes elementos essenciais devem estar presentes:

1. Analisar o contexto, definir o escopo, papéis e responsabilidades, identificar e justificar as restrições;
2. Identificar riscos considerando suas ameaças, vulnerabilidades, causas, consequências e controles existentes;
3. Analisar riscos de acordo com a metodologia, definindo os níveis de risco, segundo critérios de probabilidade, impacto e controles existentes;
4. Avaliar os riscos detalhadamente e priorizá-los conforme critérios de aceitação dos riscos (apetite ao risco);
5. Determinar formas de tratamento de riscos;
6. Analisar e determinar a aceitação de riscos residuais;

7. Monitorar a implementação da forma de tratamento de riscos definida;

8. Comunicar aos envolvidos os resultados da execução do Processo.

Esses elementos são obtidos através da execução do Processo, cujo diagrama de Fluxo é apresentado na Figura 6.

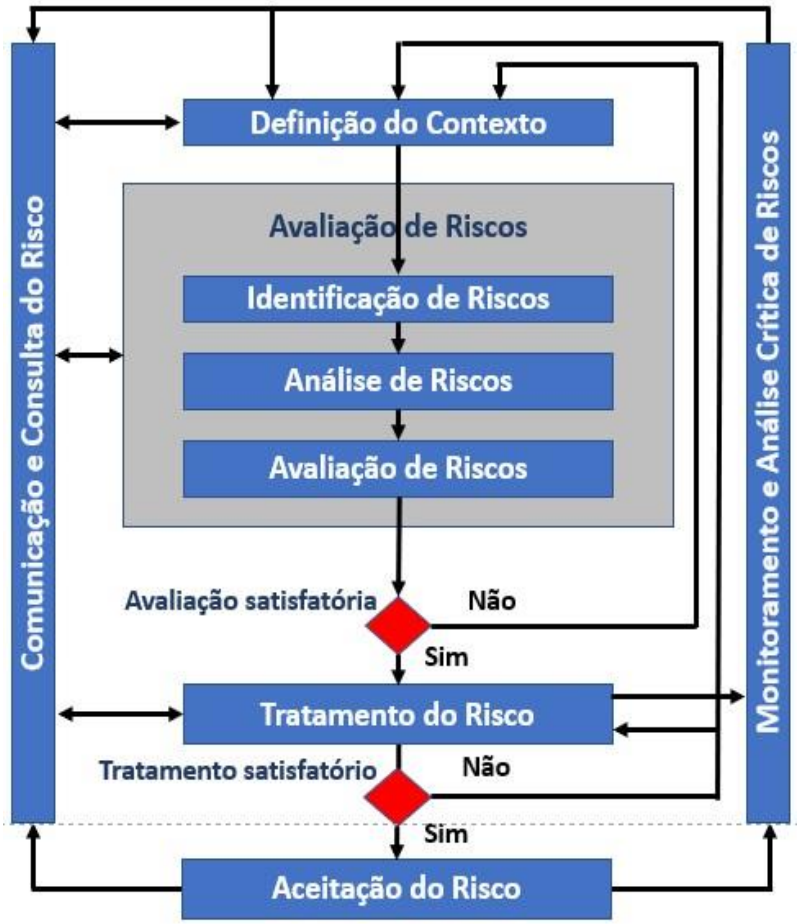

Figura 6 – Diagrama de Fluxo do Processo de Gestão de Riscos de Tecnologia da Informação – referência ABNT NBR ISO/IEC 27005:2019

Desta forma, o PGRTI está adaptado para atender as exigências legais aplicáveis, demais regramentos institucionais e alinhamento à PGRCI[1] da Ebserh, contendo subprocessos, que estruturam este documento através das seguintes seções, tendo o seu fluxo apresentado na Figura 2:

1. Definir o Contexto;
2. Identificar Riscos;
3. Analisar e Avaliar Riscos;
4. Tratar Risco;
5. Aceitar Risco;
6. Monitorar e Analisar Criticamente Riscos;
7. Comunicar e Consultar Riscos.

[2] PGRCI - Política de Gestão de Riscos e Controles Internos (PGRCI), versão 1.0, 31/08/2018.

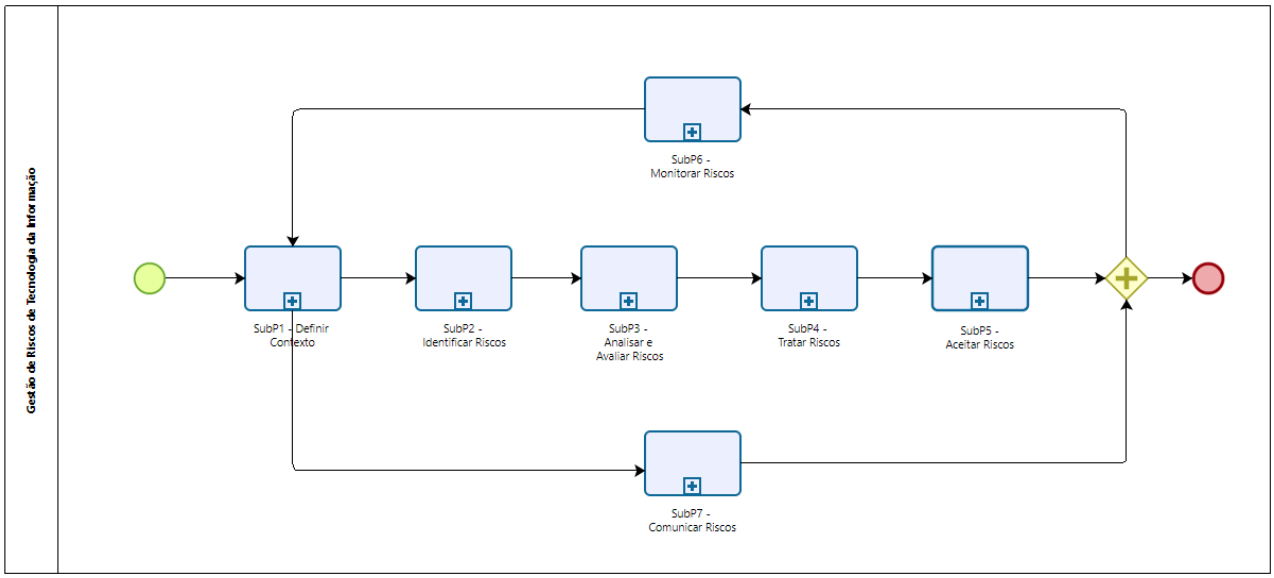

Figura 7 – Processo de Gestão de Riscos de Tecnologia da Informação - Ebserh

2.1. Subprocesso Definir Contexto

O subprocesso **Definir Contexto** define todos os critérios e definições que serão utilizados em todo o Processo de GRTI, conta com diretrizes e ações que permitem determinar o propósito do Plano de Riscos, levando em consideração os contextos externo e interno, envolvendo a definição dos *Critérios Básicos* necessários para a Gestão de Riscos, a definição do *Escopo e dos Limites* e o *Estabelecimento da Organização* apropriada para operar o Processo.

Tais informações devem ser consolidadas no Plano de Contexto, incluso no Apêndice 1 – *Template* do Plano de Riscos, e aprovado pelo Representante de TI, devendo ser comunicado às partes interessadas ao final da execução desse subprocesso, bem como sempre que houver alguma mudança em tal documento.

As atividades que compõem este subprocesso são apresentadas na Figura 8 e descritas nas seções seguintes.

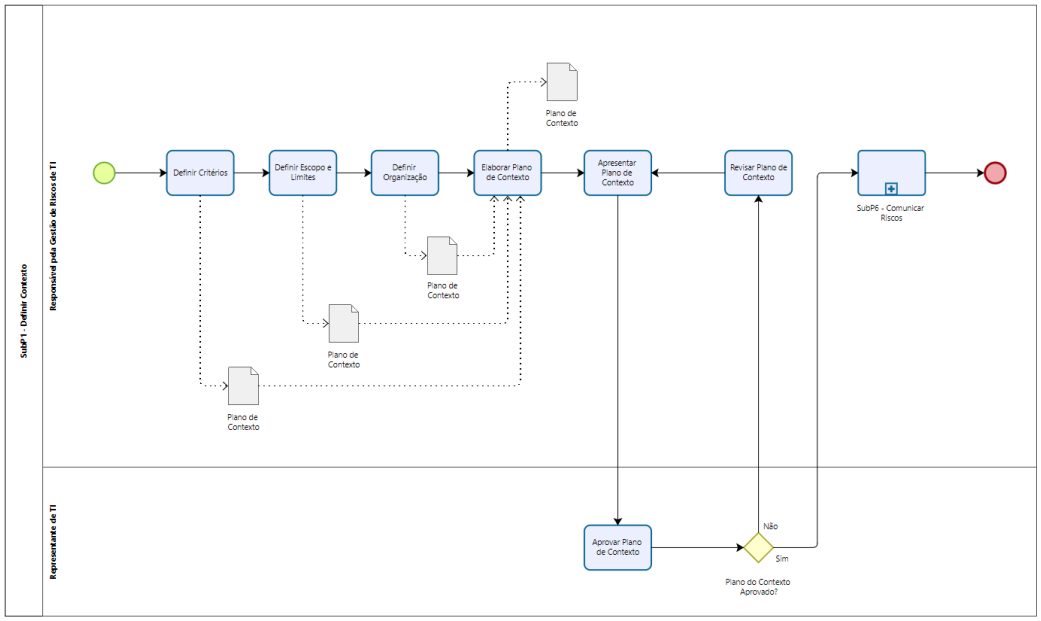

Figura 8 – Subprocesso 1 - Definir Contexto

2.1.1. Atividade Definir Critérios

Os *Critérios Básicos* para a GRTI devem ser utilizados ou atualizados conforme as necessidades organizacionais, pois eles apoiam a classificação dos riscos e a priorização do tratamento, para tanto suas identificações têm os seguintes critérios:

- O valor estratégico do processo que trata as informações de negócio;
- A criticidade dos ativos de informação envolvidos;
- A importância do ponto de vista operacional e dos negócios, da disponibilidade, da confidencialidade e da integridade, e
- As expectativas e percepções das partes interessadas e consequências negativas para o valor de mercado (a reputação).

Os critérios básicos são: Probabilidade, Impacto, Controle, Nível do Risco e Aceitação de Risco, sendo descritos nas seções seguintes, podendo ser adaptados conforme a orientação estratégica e necessidades específicas.

2.1.1.1. Critério de Probabilidade

Para estabelecer o Critério de Probabilidade, se considera a chance de algo acontecer, estimativa de frequência que um evento possa incorrer em um risco para a Ebserh, definida conforme apresentada na Tabela 2:

CRITÉRIOS DE PROBABILIDADE		
Nível	**Descrição**	**Valor**
Muito Alto	Praticamente certo;	5
	Deve ocorrer em algum momento.	
Alto	Provável; Em algum momento ocorrerá o evento; Aqui as circunstâncias apontam fortemente para essa possibilidade.	4
Médio	Possível; Poderá ocorrer; As circunstâncias apontam uma possibilidade moderada.	3
Baixo	Rara possibilidade de ocorrer.	2
Muito Baixo	Improvável; Pode ocorrer em circunstâncias excepcionais.	1

Tabela 2 - Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018) com adaptações

2.1.1.2. Critério de Impacto

Para estabelecer o Critério de Impacto, se considera os resultados ou efeitos de um evento, pontua-se o quão prejudicado será o negócio aos danos causados em relação à sua confidencialidade, integridade ou disponibilidade de um ativo da Ebserh, definidos conforme apresentados na Tabela 3:

CRITÉRIOS DE IMPACTO		
Nível	**Descrição**	**Valor**
Muito Alto	Tem grande visibilidade externa com repercussão em mais de uma mídia nacional; Prejuízos operacionais no HUF ou em toda a Ebserh; Eminente comprometimento na continuidade ou sustentabilidade da Ebserh de forma imediata; Não conformidade com requisitos legais.	5
Alto	Tem visibilidade externa com repercussão na mídia nacional; Prejuízos operacionais em uma ou mais diretoria(s) ou em uma ou mais gerência(s) do HUF; Comprometimento na continuidade ou sustentabilidade da Ebserh a curto prazo (ex.: definidos por SLA, RTO).	4
Médio	Visibilidade externa com repercussão em mídias locais; Prejuízos operacionais na DTI ou SEDISD; Comprometimento na continuidade ou sustentabilidade da Ebserh a médio prazo.	3
Baixo	Sem visibilidade externa; Prejuízo operacional apenas em uma coordenadoria ou a um grupo restrito de pessoas do HUF.	2
Muito Baixo	Afeta ativos que não estão vinculados à operação; Não afeta a operação da Ebserh.	1

Tabela 3 - Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018) com adaptações

2.1.1.3. Critério de Controle

Para estabelecer o Critério de Controle, se considera a identificação de controles existentes e suas efetividades, podendo desta forma inferir na relação ao nível risco identificado, definidos conforme apresentados na Tabela 4:

CRITÉRIOS DE CONTROLE		
Nível	**Descrição**	**Valor**
Forte	Controle mitiga o risco associado em todos os aspectos relevantes, podendo ser enquadrado num nível de "melhor prática".	0,2
Satisfatório	Controle normatizado e embora passível de aperfeiçoamento, está sustentado por ferramentas adequadas e mitiga o risco satisfatoriamente.	0,4
Mediano	Controle implementado mitiga aspectos do risco, mas não contempla todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Fraco	Controle depositado na esfera de conhecimento pessoal dos operadores do processo, em geral realizado de maneira manual, tendem a ser aplicados caso a caso, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Inexistente	Ausência completa de controle.	1

Tabela 4 - Fonte: Rede Nacional de Ensino e Pesquisa – RNP com adaptações

2.1.1.4. Nível do Risco

O Nível do Risco é o resultado do mapeamento dos riscos identificados em relação à análise da Probabilidade, Impacto e Controle, apresentando uma visão da criticidade e prioridade sobre o tratamento necessário, definidos conforme apresentado na Tabela 5:

CRITÉRIOS DE NÍVEL DO RISCO		
Nível	**Descrição**	**Valor**
Muito Alto	Nível de risco muito além do apetite a risco; Qualquer risco nesse nível deve ser comunicado à governança e alta administração e ter uma resposta de tratamento imediata; Postergação de medidas só com autorização do dirigente máximo.	5
Alto	Nível de risco além do apetite a risco; Qualquer risco nesse nível dever ser comunicado a alta administração e ter uma ação de tratamento, tomada em período determinado; Postergação de medidas só com autorização do dirigente de área.	4

Médio	Nível de risco dentro do apetite a risco; Requer atividades de tratamento e monitoramento específicas e atenção da gerência na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	3
Baixo	Nível de risco dentro do apetite a risco; Geralmente nenhuma medida especial é necessária, mas é possível que existam oportunidades de maior retorno que podem ser exploradas, assumindo-se mais riscos, avaliando a relação custos versus benefícios, como diminuir o nível de controles.	2
Muito Baixo	Nível de risco dentro do apetite a risco; Indica que o nível de risco está dentro da tolerância a risco.	1

Tabela 5 - Fonte: Gestão de Riscos – Avaliação da Maturidade (TCU, 2018), com adaptações

2.1.1.5. Aceitação do Risco

A Aceitação do Risco deve ser estabelecida conforme o apetite de risco da Ebserh, relacionando o risco identificado e avaliado, que pode ou não ser assumido pela Ebserh em busca de seus objetivos de negócio, definidos conforme apresentado na Tabela 6:

CRITÉRIOS DE ACEITAÇÃO DO RISCO			
Nível	**Aceitação**	**Definição**	**Alçada de Decisão**
Muito Alto	**Inaceitável**	Deve receber tratamento imediato, buscando sua eliminação ou redução de magnitude.	Tratado a nível de Conselho de Administração (CA).
Alto	**Inaceitável**	Deve prioritariamente receber tratamento, buscando sua eliminação ou redução de magnitude.	Tratado a nível de Diretoria Executiva (Direx) na Administração Central e Colegiado Executivo (Colex) no Hospital Universitário Federal – HUF.
Médio	**Tolerável**	Deve receber tratamento, mas pode ser aceito ou não após revisão e confirmação.	Tratado a nível de Diretoria de Tecnologia da Informação – DTI na Administração Central e Setor de Tecnologia da Informação e Saúde Digital – SETISD no Hospital Universitário Federal – HUF.
Baixo	**Aceitável**	Pode ser aceito através de meios formais, após revisão e confirmação do responsável pelo ativo ou processo.	Tratado a nível de Coordenadoria da DTI na Administração Central e Setor de Tecnologia da Informação e Saúde Digital – SETISD no Hospital Universitário Federal – HUF.

Muito Baixo	**Aceitável**	Pode ser aceito através de meios formais, após revisão e confirmação do responsável pelo ativo ou processo.	Tratado a nível de Coordenadoria da DTI na Administração Central e Setor de Tecnologia da Informação e Saúde Digital – SETISD no Hospital Universitário Federal – HUF.

Tabela 6- Fonte: Rede Nacional de Ensino e Pesquisa – RNP com adaptações

2.1.2. Atividade Definir Escopo e Limites

O propósito desta atividade é definir o objetivo, o escopo e limites da Gestão de Riscos de TI, assegurando que todos os ativos relevantes sejam considerados, identificando e justificando limites, para que seja possível reconhecer se os riscos possam transpor os parâmetros estabelecidos para o escopo.

O seguinte conjunto de informações pode ser considerado para a revisão desta atividade do subprocesso Definir Contexto:

- Cadeia de Valor;
- Objetivos estratégicos, políticas e estratégias da Ebserh;
- Processos de negócio;
- Funções e estrutura da Ebserh;
- Política de Segurança da Informação da Ebserh;
- Abordagem da Ebserh à Gestão de Riscos;
- Ativos de informação;
- Localidades em que a Ebserh se encontra e suas características geográficas;
- Restrições que afetam a Ebserh;
- Expectativas das partes interessadas;
- Ambiente sociocultural;
- Interfaces (ou seja, a troca de informação com o ambiente).

Ao definir as premissas do Processo de GRTI estabelece-se os limites e busca responder o que se pretende com a GRTI, até onde ela vai e quais suas limitações para isto (técnicas, operacionais, financeiras, etc.) deverão ser apontadas nesta tarefa, que incluem:

- Objetivo – Definir o objetivo da execução do Plano de Riscos para a Ebserh;
- Escopo – Definir o escopo e validar se está alinhado a cadeia de valor, objetivos de negócio e estratégicos;
- Restrições – Identificar e definir as restrições em conformidade com a Ebserh e o escopo do Plano de Riscos, considerando:
  - Restrições que afetam a Ebserh
    - De natureza política;
    - De natureza estratégica;
    - Territoriais;
    - Advindas do ambiente econômico e político;
    - Estruturais;
    - Funcionais;

- Relativas aos recursos humanos;
- Advindas da agenda da Ebserh;
- Relacionadas a métodos;
- Natureza cultural;
- Orçamentárias;

○ Restrições que afetam o escopo

- Derivadas de Processos preexistentes;
- Restrições técnicas;
- Financeiras;
- Ambientais;
- Temporais;
- Relacionadas a métodos;
- Legais;
- Organizacionais.

Deve-se explicar os motivos das exclusões das restrições de escopo, se houver, elencando-os como justificativas.

Para realizar esta atividade, sugere-se pré-identificar os normativos e documentos institucionais que estejam relacionados ao escopo da análise.

2.1.3. Atividade Definir Organização

Cada um dos papéis do processo de GRTI, bem como suas responsabilidades, devem ser elencados e consolidados à fim de que não restem dúvidas sobre o papel de cada um no processo. Papéis e Responsabilidades, neste contexto, deverão abranger não apenas aqueles relacionados à gestão do processo de GRTI, mas também aqueles responsáveis ou que em algum momento sejam demandados para operacionalizar alguma de suas atividades.

A estruturação da Gestão de Risco de TI da Administração Central e HUFs está caracterizada conforme apresentada na Figura 9:

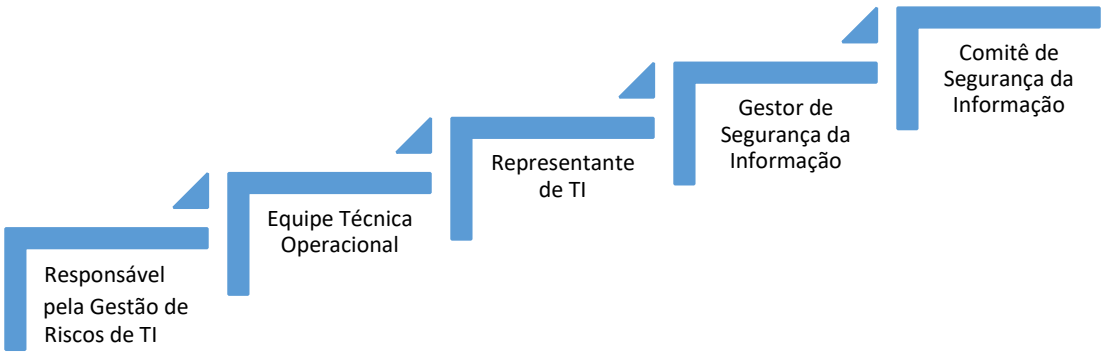

Figura 9 – Organização de Gestão de Riscos de TI da Administração Central e HUFs da Ebserh

Os Papéis e Responsabilidades da Ebserh são detalhados abaixo:

- Responsável pela Gestão de Riscos de TI

- Receber e executar a demanda de Gestão de Riscos de TI;
- Identificar e elencar Equipe Técnica Operacional;
- Elaborar e apresentar ao Representante de TI o Plano de Contexto, com apoio da Equipe Técnica Operacional, contendo a definição dos critérios, escopo, objetivos, limites, papéis e responsabilidades do Plano de Riscos;
- Elaborar o Plano de Riscos com apoio da Equipe Técnica Operacional;
- Elaborar e apresentar ao Representante de TI o Plano de Tratamento de Riscos, com apoio da Equipe Técnica Operacional, contendo os riscos identificados, analisados e avaliados e o detalhamento do tratamento de cada risco identificado;
- Realizar a gestão do Plano de Tratamento de Riscos, com apoio da Equipe Técnica Operacional;
- Elaborar e executar o Plano de Comunicação do Plano de Riscos;
- Elaborar e encaminhar aos gestores responsáveis o Termo de Aceite de Riscos;
- Gerir e propor melhorias ao Processo de GRTI;
- Gerir e apresentar ao Representante de TI os Fatores Críticos de Sucesso do Processo de Gestão de Riscos de TI.

- Equipe Técnica Operacional
  - Assessorar o Responsável pela Gestão de Riscos de TI na identificação de ativos, ameaças, vulnerabilidades, consequências e controles existentes atrelados aos riscos de TI, bem como na definição e implementação de novos controles, de acordo com o Plano de Tratamento de Riscos;
  - Propor melhorias ao Processo de GRTI.
- Representante de TI
  - Aprovar o Plano de Contexto contendo a definição dos critérios, escopo, objetivos, limites, papéis e responsabilidades da GRI;
  - Aprovar o Plano de Tratamento de Riscos contendo os riscos identificados, analisados e avaliados e o detalhamento do tratamento de cada risco identificado;
  - Aprovar e apresentar ao Gestor de Segurança da Informação os Fatores Críticos de Sucesso do Processo de Gestão de Riscos de TI;
  - Propor melhorias ao Processo de GRTI.
- Gestor de Segurança da Informação
  - Analisar e apresentar ao Comitê de Segurança da Informação os Fatores Críticos de Sucesso do Processo de Gestão de Riscos de TI, que envolvam a Segurança da Informação;
  - Propor melhorias ao Processo de GRTI.
- Comitê de Segurança da Informação
  - Analisar os Fatores Críticos de Sucesso do Processo de Gestão de Riscos de TI, que envolvam Segurança da Informação;
  - Propor melhorias ao Processo de GRTI.

2.1.4. Atividade Elaborar Plano de Contexto

As atividades anteriores geraram informações que precisam ser consolidadas em um documento único, sucinto e de fácil leitura e entendimento. Este documento, o Plano de Contexto, orienta a execução da GRTI e deve ser revisado periodicamente, sempre que alguma das informações sofrer alterações, como mudança e ampliação do escopo, aumento ou alteração de limites, revisão de critérios etc.

Entrada: Conjunto de informações descritos do subprocesso Definir Contexto.

Saída: Preencher o Plano de Contexto, utilizando a planilha Plano de Contexto, do Plano de Riscos de TI da Ebserh.

2.1.5. Atividade Apresentar Plano de Contexto

A apresentação do Plano de Contexto deve ser realizada em reunião, com o Representante de TI, para que este possa tomar conhecimento e deliberar sobre o conteúdo de tal documento.

Entrada: Planilha Plano de Contexto do Plano de Riscos de TI da Ebserh.

Saída: Plano de Contexto apresentado.

2.1.6. Atividade Aprovar Plano de Contexto

Avaliar e aprovar o Plano de Contexto é atividade fundamental a ser executada no Processo de GRTI e deve ser realizada pelo Representante de TI. Esta aprovação deve ser formal e realizada em reunião, demonstrando o comprometimento com a GRTI.

Como evidência da aprovação deve ser gerada uma Ata e certificá-la através do Sistema Eletrônico de Informações (SEI).

Entrada: Planilha Plano de Contexto do Plano de Riscos de TI da Ebserh.

Saída: Aprovação do Plano de Contexto pelo Representante de TI.

2.1.7. Atividade Revisar Plano de Contexto

Caso necessário, o Plano de Contexto deve ser revisado considerando os apontamentos realizados pelo Representante de TI, alinhando as expectativas da Ebserh quanto o Plano de Contexto, e após revisado, deverá passar por nova avaliação do Representante de TI para revisão.

Entrada: Planilha Plano de Contexto do Plano de Riscos de TI da Ebserh.

Saída: Planilha Plano de Contexto do Plano de Riscos de TI da Ebserh, revisada.

2.2. Subprocesso Identificar Riscos

O subprocesso **Identificar Riscos** tem como propósito identificar, reconhecer e descrever riscos que possam ajudar ou impedir a Ebserh de alcançar seus objetivos. Para tanto, todos os elementos relacionados à materialização dos riscos são identificados.

Risco - efeito da incerteza nos objetivos. Um efeito é um desvio em relação ao esperado. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças (ISO 31000:2018)

Para a execução desta atividade, é fundamental contar com apoio especializado de equipes técnicas e de negócio das mais diversas áreas da Ebserh alinhadas ao escopo do Plano de Contexto, formando assim uma Equipe Técnica Operacional responsável pela análise, sendo que sem o apoio desta, torna-se difícil obter resultados consistentes.

Nesta atividade, são detalhados os ativos, as ameaças, as vulnerabilidades, as consequências e os controles existentes para cada risco, e esta ação apoia a avaliação e o tratamento dos riscos nas atividades posteriores.

A identificação pode ser realizada através de:

- Executar oficinas com Equipe Técnica Operacional conforme escopo do Plano de Contexto;
- Realizar o levantamento de ativos de TI com apoio da Equipe Técnica Operacional relacionado ao escopo do Plano de Contexto;
- Realizar a Identificação de Riscos baseado nos ativos de TI com apoio da Equipe Técnica Operacional, utilizando técnica de brainstorming e questionários (checklist) de apoio;
- Realizar a Identificação dos riscos frente os impactos ao negócio.

Recomenda-se utilizar questionários (checklist) para auxiliar a identificação dos riscos, conforme referência do documento de apoio: “Apêndice 2 - Checklist Identificação de Riscos”.

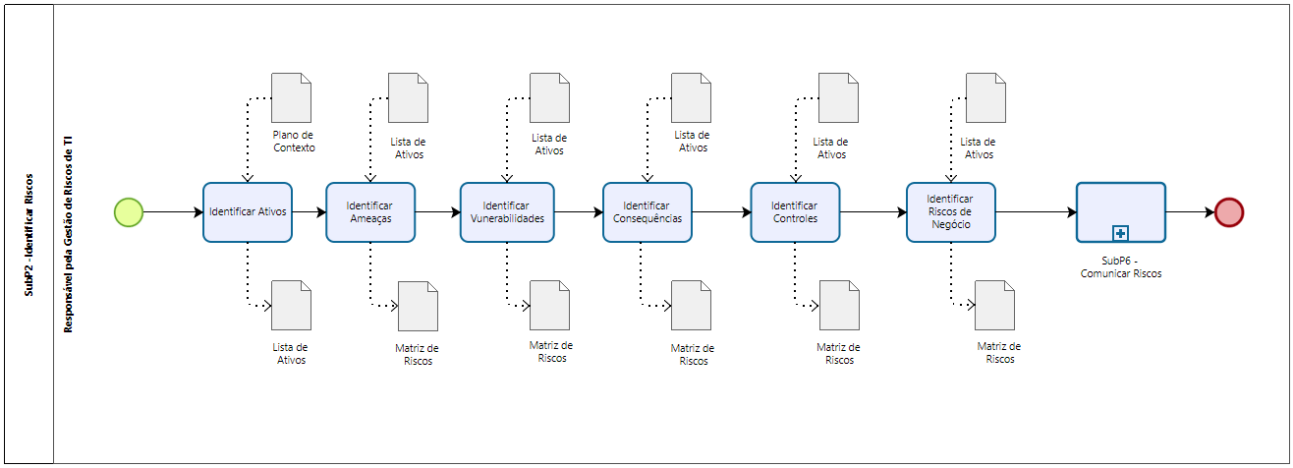

Figura 10 – Subprocesso 2 - Identificar Riscos

2.2.1. Atividade Identificar Ativos

Ativo - aquilo que tem valor – tangível ou intangível - para a organização, tais como informação, software, equipamentos, instalações, serviços, pessoas e imagem institucional (Dicionário de Referência de TI).

Identificar e catalogar os ativos relacionados ao Plano de Contexto apoia a Equipe Técnica Operacional na identificação de possíveis riscos relacionados ao escopo da análise, na identificação dos responsáveis e em questões técnicas relacionadas a identificação dos riscos, análise, avaliação e no tratamento dos riscos.

Entrada: Planilha Plano de Contexto do Plano de Riscos da de TI da Ebserh.

Saída: Planilha Lista de Ativos do Plano de Riscos de TI da Ebserh.

2.2.2. Atividade Identificar Ameaças

Ameaças são eventos ou circunstâncias, com potencialidade de causar perdas ou danos a um ativo da Ebserh, podendo também definida como a intenção ou capacidade de um agente empreender ações nocivas ou danosas aos interesses da Ebserh.

Identificar e detalhar as ameaças apoia o entendimento dos riscos, análise, avaliação e no tratamento dos riscos.

Entrada: Planilha Lista de Ativos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.2.3. Atividade Identificar Vulnerabilidades

Vulnerabilidade é qualquer fraqueza que possa ser explorada por uma ameaça, e que cause perda ou danos a um ativo da Ebserh.

Identificar e detalhar as vulnerabilidades apoia o entendimento dos riscos, análise, avaliação e no tratamento dos riscos.

Entrada: Planilha Lista de Ativos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.2.4. Atividade Identificar Causas

Elencar possíveis fontes ou causas dos riscos identificados.

Identificar e detalhar as vulnerabilidades apoia o entendimento dos riscos, análise, avaliação e no tratamento dos riscos.

Entrada: Planilha Lista de Ativos **do Plano de Riscos de TI da Ebserh**.

Saída: Planilha Matriz de Riscos **do Plano de Riscos de TI da Ebserh**.

2.2.5. Atividade Identificar Consequências

Consequências são todos os resultados de dano ou perda concretizados a um ativo da TI da Ebserh.

Consequência - resultado de um evento que afeta os objetivos.

Uma consequência pode ser certa ou incerta e pode ter efeitos positivos ou negativos, diretos ou indiretos, nos objetivos (ISO 31000:2018).

Identificar e detalhar as consequências apoia o entendimento dos riscos, análise, avaliação e no tratamento dos riscos.

Entrada: Planilha Lista de Ativos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.2.6. Atividade Identificar Controles

Controle é a medida que mantém e/ou modifica o risco. Controles incluem, mas não estão limitados a qualquer processo, política, dispositivo, prática ou outras condições e/ou ações que mantêm e/ou modificam o risco (ISO 31000:2018).

Controles existentes na Ebserh para cada Risco Identificado e suas eventuais efetividades podem interferir na relação ao Nível Risco Identificado.

Identificar e detalhar os Controles Existentes apoia o entendimento dos riscos, análise, avaliação e no tratamento dos riscos.

Entrada: Planilha Lista de Ativos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.2.7. Atividade Identificar Riscos de Negócio

Identificar Riscos de Negócio é descrever como um risco está relacionado aos objetivos de negócio, detalhando como será o real dano para a Ebserh e não ao ativo, caso o risco se materialize.

Identificar os Riscos de Negócio apoia na análise, avaliação e no tratamento dos riscos e habilita aos gestores a tomada de decisão ao simplificar a visão sobre os riscos alinhados ao negócio.

Entrada: Planilha Lista de Ativos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.3. Subprocesso Analisar e Avaliar Riscos

O subprocesso **Analisar e Avaliar Riscos** tem como propósito, compreender a natureza dos riscos e suas características, incluindo o nível de cada risco, e realizar uma avaliação crítica se os riscos estão alinhados com o Plano de Contexto e se foram definidos corretamente.

A primeira atividade deste subprocesso consiste em realizar uma análise de cada risco, esta análise pode ser qualitativa ou quantitativa ou uma combinação de ambos, e deve ser coerente com os critérios desenvolvidos como parte da Definição de Contexto. Nesta atividade do subprocesso são definidos os Níveis de Probabilidade, Impacto e dos Controles Existentes para cada risco identificado.

Devido ao grau de maturidade da Ebserh neste momento, foi definido que inicialmente seria utilizado a análise qualitativa, e sempre que possível dados quantitativos, pois serão elaborados indicadores e históricos de referências para futuras análises quantitativas a partir desse Processo.

A Análise de Riscos, pode ser baseada através de:

- Executar oficinas para analisar e definir a Probabilidade, Impacto e Controles Existentes com Equipe Técnica Operacional relacionada aos riscos identificados.

Após a execução da Análise de Riscos é necessário realizar a atividade de Avaliação de Riscos, baseando-se nas decisões que foram tomadas durante a Definição de Contexto. Convém que essas decisões e o contexto sejam revisados detalhadamente nesse estágio em que se conhece mais sobre os riscos identificados, avaliando se os critérios estão adequados e se os riscos identificados fazem parte do escopo definido no Plano de Contexto.

Convém que a Probabilidade, Impacto e Controles de cada risco seja avaliada e priorizada, pois a agregação de vários riscos de nível baixo ou médio podem resultar em um risco total significativo e convém que seja tratado adequadamente.

A Avaliação de Riscos, pode ser baseada em:

- Revisitar detalhadamente os riscos e critérios definidos conforme o Plano de Contexto;
- Priorizar os riscos conforme Critérios de Aceitação.

A Análise e Avaliação de Riscos deverão ser conduzidas conforme o subprocesso apresentado na Figura 11.

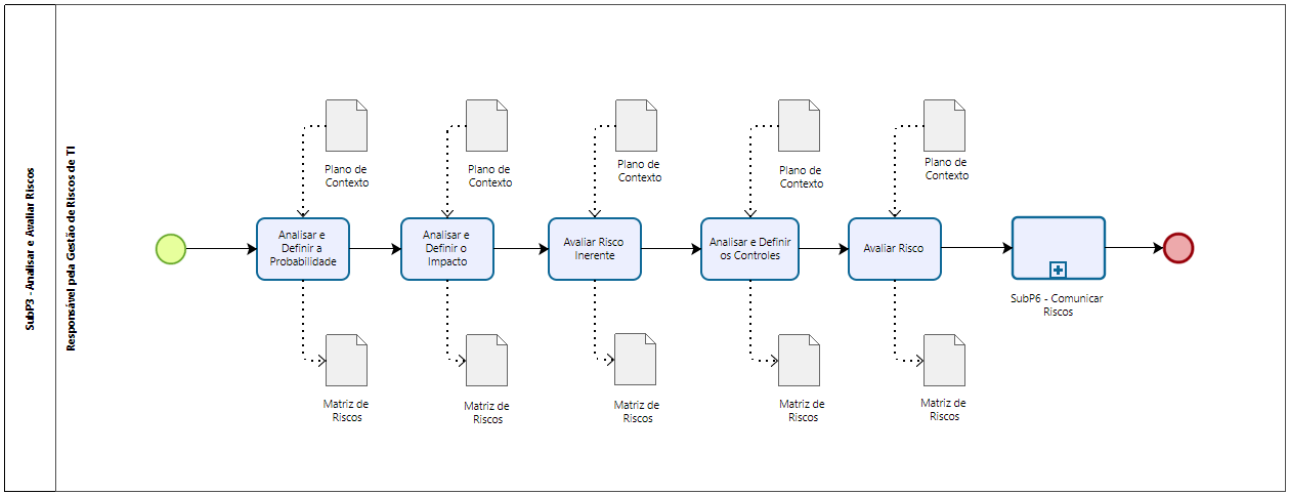

Figura 11 – Subprocesso 3 - Analisar e Avaliar Riscos

2.3.1. Atividade Analisar e Definir a Probabilidade

Nesta atividade do subprocesso, é necessário analisar e definir com o apoio da Equipe Técnica Operacional, a Probabilidade de ocorrência de cada risco identificado.

Essa análise deve ser baseada nos Critérios de Probabilidade definidos no Plano de Contexto.

Entrada: Planilha Plano de Contexto do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.3.2. Atividade Analisar e Definir o Impacto

Nesta atividade do subprocesso, é necessário analisar e definir com o apoio da Equipe Técnica Operacional, os Impactos de ocorrência de cada risco identificado.

Essa análise deve ser baseada nos Critérios de Impacto definidos no Plano de Contexto.

Entrada: Planilha Plano de Contexto do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.3.3. Atividade Avaliar Risco Inerente

Nesta atividade do subprocesso, é necessário revisar detalhadamente se as definições dos critérios de Probabilidade e Impacto estão adequadas ao risco identificado, consolidando assim o Nível de Risco Inerente.

Risco inerente é aquele que uma organização terá de enfrentar na falta de medidas que a administração possa adotar para alterar a probabilidade ou o impacto dos eventos. (COSO-2004)

Risco inerente é o resultado da Probabilidade X Impacto, de acordo com o Plano de Contexto.

Para tanto, essa avaliação necessita basear-se no Plano de Contexto definido, que também pode ser avaliado nesse estágio em que se conhece mais sobre os riscos identificados.

Entrada: Planilha Plano de Contexto do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.3.4. Atividade Analisar e Definir os Controles

Nesta atividade do subprocesso, é necessário analisar e definir com o apoio da Equipe Técnica Operacional, os Controles atuais existentes de cada risco identificado.

Essa análise deve ser baseada nos Critérios de Controles definidos no Plano de Contexto.

Entrada: Planilha Plano de Contexto do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.3.5. Atividade Avaliar Risco

Esta atividade do subprocesso, é a atividade mais abrangente da avaliação.

Deve-se revisar detalhadamente se as decisões do Plano de Contexto e dos critérios utilizados de Probabilidade, Impacto e Controles existentes de cada risco identificado estão adequadas, e se necessário adequá-las, resultando na correta definição do nível de cada risco.

Entrada: Planilha Plano de Contexto do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.4. Subprocesso Tratar Riscos

O subprocesso **Tratar Riscos** tem como objetivo definir e implementar opções apropriadas para abordar riscos identificados, executando tudo aquilo que for necessário, aplicável e que estiver ao alcance da Ebserh para reduzir os riscos ao negócio. Os riscos identificados devem ter sua execução planejada no Plano de Tratamento de Riscos, de forma a balancear os benefícios potenciais derivados em relação ao alcance dos objetivos, face aos custos, esforços ou desvantagens da implementação.

O tratamento dos riscos inicia-se em como a Ebserh pretende lidar com cada risco e os potenciais danos ou benefícios, definindo as opções de tratamento entre as opções: Modificar, Reter, Evitar e Compartilhar Riscos, seguido com um plano detalhado de ações visando a implementação de controles do ponto de vista técnico, operacional, financeiro e de recursos humanos para alcançar os objetivos.

O Subprocesso Tratar Riscos deverá ser conduzido conforme apresentado na Figura 12:

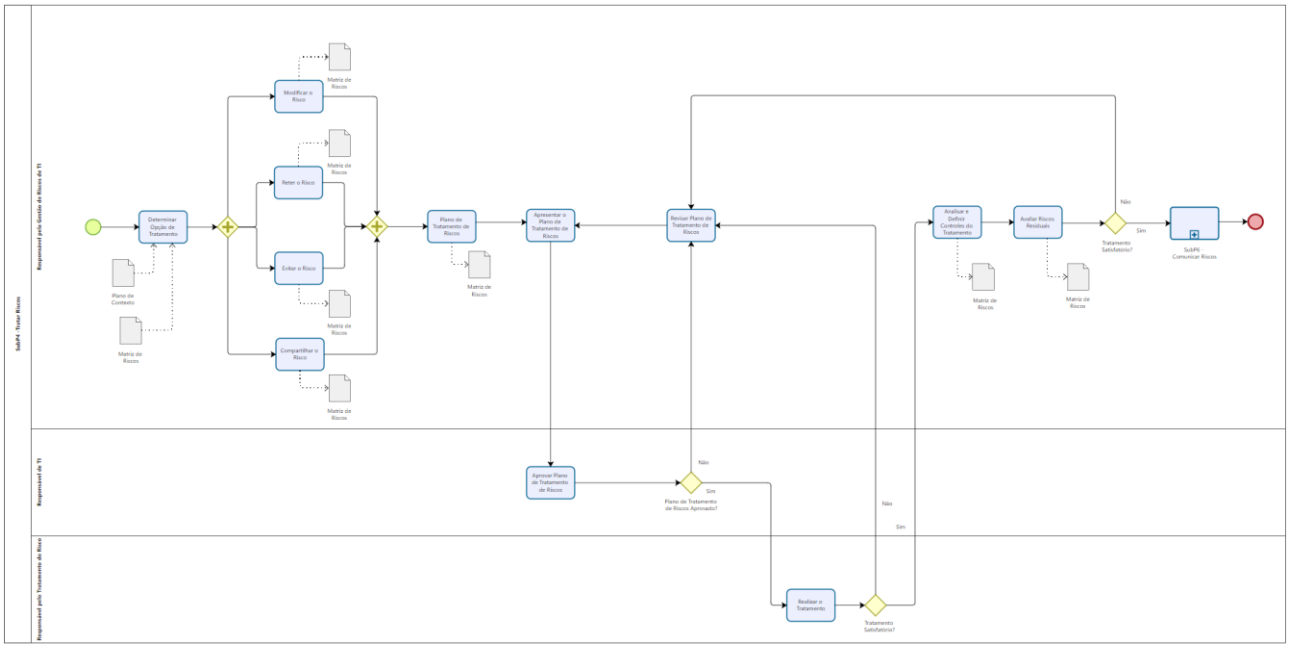

Figura 12 – Subprocesso 4 - Tratar Riscos

2.4.1. Atividade Determinar Opção de Tratamento

Nesta atividade do subprocesso é necessário realizar um trabalho analítico acerca das possibilidades de como a Ebserh irá tratar os riscos, levando em consideração o Plano de Contexto e a Matriz de Riscos para cada risco devidamente identificado, detalhado, analisado e avaliado.

Os riscos podem ser modificados, retidos, evitados ou compartilhados.

Entrada: Planilha Plano de Contexto e Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Seleção da Opção de Tratamento na Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.4.2. Atividade Modificar o Risco

Modificar o risco significa reduzir o seu nível, ou seja, a sua probabilidade ou o seu impacto, caso se materialize, mas não o mitigar por completo. A modificação como forma de tratamento de um risco deve ocorrer, entre outros motivos, devido a limitação de recursos.

Nesta situação apenas uma parte dos controles aplicáveis é implementada e seu risco residual deve ser aceito e monitorado, pois não deixa de existir como risco, apenas teve seu nível reduzido.

Entrada: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.4.3. Atividade Reter o Risco

Reter um risco não irá interferir em seu nível e nem em seu potencial impacto ou probabilidade.

O risco não deixa de existir da forma como é, apenas é aceito pela Ebserh, seja por conta da limitação de recursos para a implementação de controles ou pelo baixo nível que representa, onde os recursos alocados podem fazer com que se torne mais dispendioso tratá-lo do que conviver com ele, de forma controlada e monitorada.

Os Riscos retidos devem ser monitorados constantemente e formalmente aceitos.

Entrada: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.4.4. Atividade Evitar o Risco

Evitar um risco elimina-o por completo e não apenas altera o seu nível.

Sempre que possível os riscos devem ser evitados, porém deve-se considerar as condições para que isto possa ocorrer de forma que a Ebserh não seja penalizada por ter alocado recursos além dos necessários, balanceando os benefícios versus eventuais prejuízos.

Entrada: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.4.5. Atividade Compartilhar o Risco

Compartilhar um risco é uma forma de tratá-lo transferindo a outrem a responsabilidade no caso de sua concretização, por exemplo, a cobertura através de seguros permite transferir um risco.

Compartilhar o risco com terceiros transfere para estes a responsabilidade pelo seu gerenciamento, mas não a responsabilidade legal pela sua eventual materialização.

Entrada: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.4.6. Atividade Plano de Tratamento de Riscos

O Plano de Tratamento dos Riscos é um consolidado geral com a definição de tratamento para cada risco, contendo, assim, um detalhamento do plano com informações sobre os responsáveis pela implementação dos controles, área corresponsável pelo tratamento, o período de implementação, e o status de tais atividades para um ideal monitoramento da implantação de tal plano.

O Plano de Tratamento de Riscos não é imutável, devendo ser reavaliado periodicamente, inclusive como forma de análise de eficácia de controles e para identificar uma possível mudança de cenário que altere os riscos ou os próprios controles a serem implementados.

Entrada: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.4.7. Atividade Apresentar o Plano de Tratamento de Riscos

A apresentação do Plano de Tratamento dos Riscos deve ser realizada em reunião com o Representante de TI, para que este possa tomar conhecimento e deliberar sobre o conteúdo de tal documento.

O Representante de TI deve ser comunicado com antecedência sobre o conteúdo do Plano de Tratamento dos Riscos para que a reunião sirva para aprová-lo ou rejeitá-lo.

Entrada: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Plano de Tratamento de Riscos apresentado.

2.4.8. Atividade Aprovar o Plano de Tratamento de Riscos

Avaliar e aprovar o Plano de Tratamento dos Riscos é atividade fundamental a ser executada no Processo de GRTI e deve ser realizada pelo Representante de TI.

Como evidência da aprovação deve ser gerada uma Ata e certificá-la através do Sistema Eletrônico de Informações (SEI).

Entrada: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Aprovação do Plano de Tratamento de Risco pelo Representante de TI.

2.4.9. Atividade Revisar o Plano de Tratamento de Riscos

Caso necessário, o Plano de Tratamento dos Riscos deve ser revisado considerando os apontamentos realizados pelo Representante de TI ou Responsável pelo Tratamento do Risco, alinhando as expectativas da Ebserh e a efetividade quanto aos controles sugeridos para tratamento dos riscos, e após revisado, deve passar por nova avaliação do Representante de TI para deliberação.

Entrada: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh, revisada.

2.4.10. Atividade Realizar o Tratamento

Após o Plano de Tratamento dos Riscos ser aprovado pelo Representante de TI (atividade 2.4.8 – Atividade Aprovar Plano de Tratamento de Riscos), o responsável pelo tratamento de cada risco deve iniciar a execução do tratamento conforme o plano aprovado, pois ele é o responsável por tratar os riscos com o propósito de atingir o objetivo definido no planejamento.

Durante a atividade do tratamento, caso o responsável identifique que o tratamento não está satisfatório conforme os critérios de Aceitação de Riscos estabelecidos no Plano de Contexto, ele deve encaminhar ao Responsável pela Gestão de Riscos de TI a revisão do Plano de Tratamento, conforme a atividade 2.4.9 – Revisar o Plano de Tratamento dos Riscos, deste subprocesso.

Entrada: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.4.11. Atividade Analisar e Definir Controles do Tratamento

Após a realização do tratamento dos riscos, o Representante de TI é o responsável por avaliar os novos controles implementados com o apoio da Equipe Técnica Operacional, com o objetivo de analisar a efetividade dos novos controles implementados.

Entrada: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.4.12. Atividade Avaliar Riscos Residuais

Avaliar os Riscos Residuais é a atividade onde é comparado o Nível do Risco antes do tratamento e após os controles implementados, conforme o Plano de Riscos de TI da Ebserh.

O objetivo dessa atividade é entender se o tratamento realizado foi satisfatório conforme o planejamento, e caso não seja, será necessário revisar o Plano de Tratamento de Riscos, conforme a atividade 2.4.9 – Revisar o Plano de Tratamento de Riscos, até que ele seja considerado satisfatório, conforme os critérios de Aceitação de Riscos estabelecidos no Plano de Contexto.

Entrada: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

2.5. Subprocesso Aceitar Riscos

O subprocesso **Aceitar Riscos** tem como objetivo apoiar os gestores responsáveis pelas alçadas de decisão, estabelecidas no Plano de Contexto realizarem uma análise crítica e aprovarem os riscos residuais resultantes.

Os riscos residuais são todos os riscos que conforme ao apetite de risco da Ebserh podem ser aceitos, baseando-se nos critérios de Aceitação de Riscos estabelecido no Plano de Contexto ou nos objetivos estratégicos da Ebserh. Em geral, são riscos que os custos de implementação de controles ou objetivos estratégicos ultrapassam o benefício que possa ser gerado.

O Subprocesso Aceitar Riscos deve ser conduzido conforme apresentado na Figura 13.

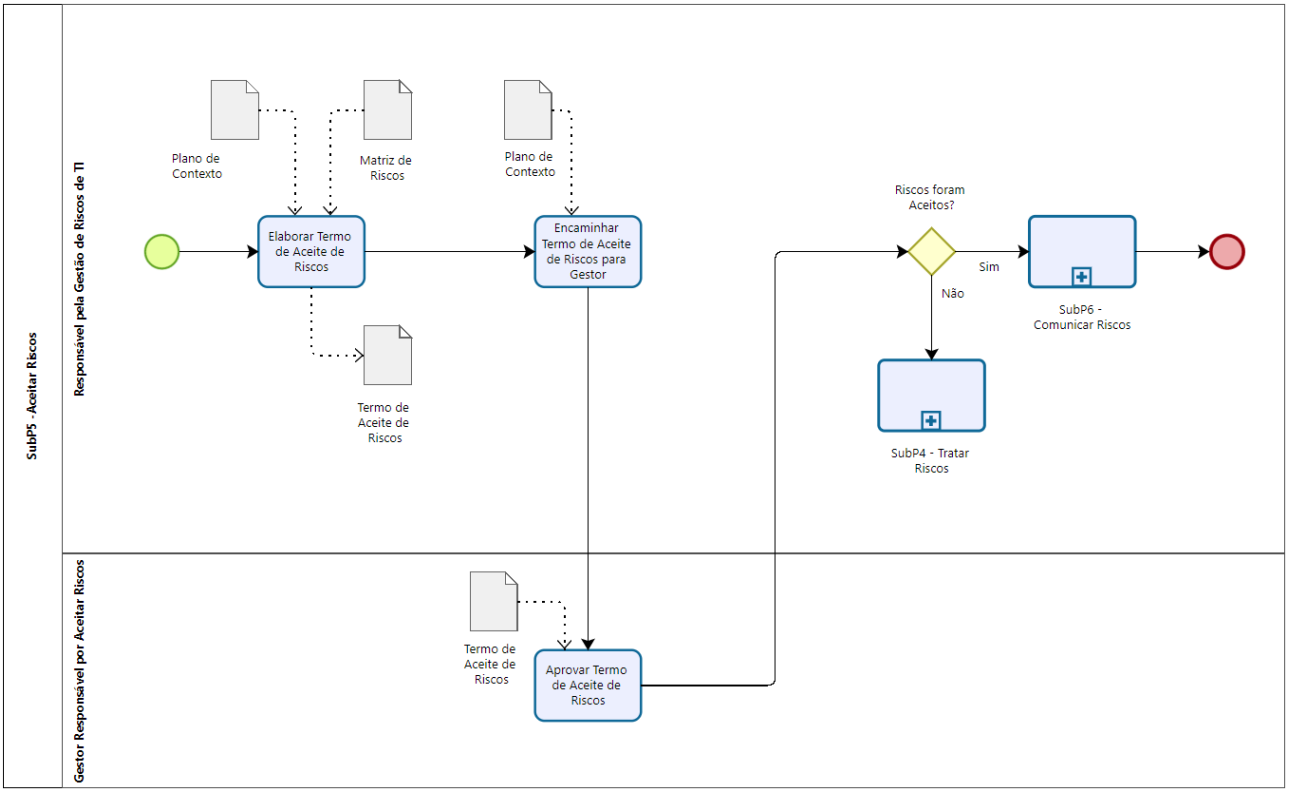

Figura 13 – Subprocesso 5 - Aceitar Riscos

2.5.1. Atividade Elaborar Termo de Aceite de Riscos

Nesta atividade, após a avaliação dos riscos residuais, é necessário que o Representante de TI avalie quais riscos residuais da Matriz de Riscos atendem os critérios de Aceitação de Riscos estabelecidos no Plano de Contexto, e elabore o Termo de Aceite de Riscos que deve ser encaminhado para o Gestor Responsável para formalização do aceite.

Entrada: Planilha do Plano de Contexto e Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Planilha Termo de Aceite de Riscos do Plano de Riscos de TI da Ebserh.

2.5.2. Atividade Encaminhar Termo de Aceite de Riscos para Gestor

Nesta atividade, o Representante de TI necessita avaliar, conforme alçada dos critérios Aceitação de Riscos estabelecida no Plano de Contexto, qual o Gestor Responsável por Aceitar os Riscos residuais e encaminhar o Termo de Aceite.

Entrada: Planilha do Plano de Contexto do Plano de Riscos de TI da Ebserh.

Saída: Planilha Termo de Aceite de Riscos do Plano de Riscos de TI da Ebserh, encaminhado.

2.5.3. Atividade Aprovar Termo de Aceite de Riscos

Nesta atividade, o Gestor Responsável por Aceitar os Riscos residuais deve avaliar se estes podem ser aceitos pela Ebserh.

Se forem aceitos, o Termo de Aceite de Riscos deve ser encaminhado para o Responsável pela Gestão de Riscos de TI. Se não forem aceitos, o Termo de Aceite de Riscos deve retornar para o Responsável pela Gestão de Riscos de TI com a justificativa do não aceite, devendo ser analisados os riscos através do Subprocesso 4 – Tratar Riscos, para um novo planejamento sobre o tratamento destes riscos.

Entrada: Termo de Aceite de Riscos.

Saída: Termo de Aceite de Riscos, avaliado.

2.6. Subprocesso Comunicar Riscos

O subprocesso **Comunicar Riscos** é transversal e tem como finalidade comunicar às partes interessadas a qualquer momento o status do Processo de GRTI.

A comunicação é uma atividade que apoia obter um consenso sobre como gerenciar os riscos, por meio da troca ou compartilhamento das informações sobre o risco entre os tomadores de decisão e as partes interessadas. A comunicação eficaz entre as partes interessadas é importante, uma vez que isso pode ter um impacto significativo sobre as decisões a serem tomadas.

O Subprocesso Comunicar Riscos deve ser conduzido conforme apresentado na Figura 14.

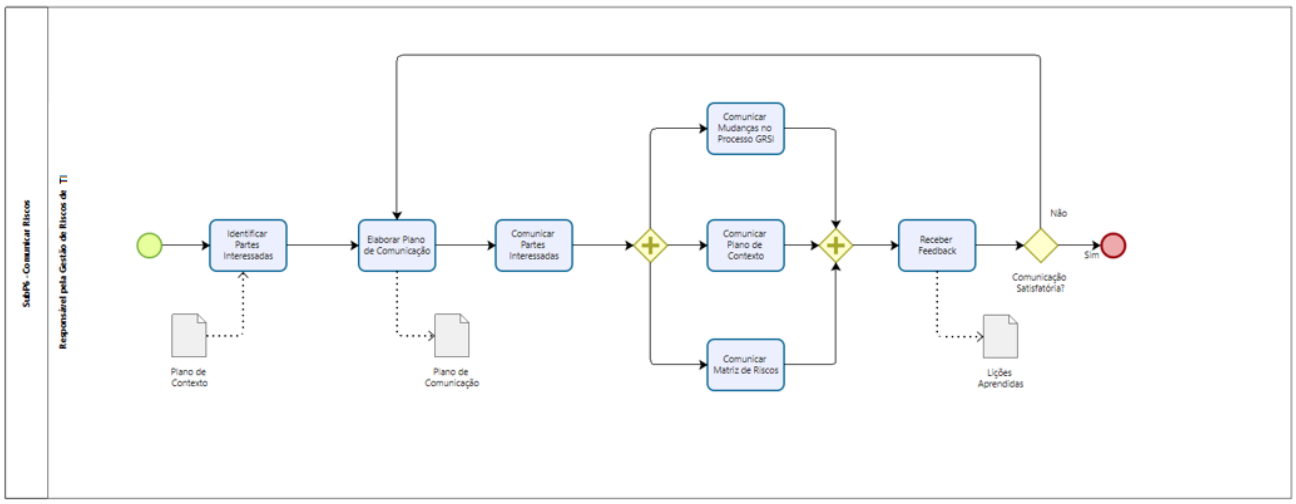

Figura 14 – Subprocesso 6 - Comunicar Riscos

2.6.1. Atividade Identificar Partes Interessadas

Nesta atividade, o Responsável pela Gestão de Riscos de TI necessita identificar quais são as partes interessadas que necessitam ser comunicadas sobre os resultados do Processo de GRTI.

A comunicação dentro do Processo de GRTI é elemento essencial e para que seja efetiva e eficaz deve ser realizada de forma organizada e direcionada apenas às partes interessadas identificadas.

Entrada: Planilha Plano de Contexto do Plano de Riscos de TI da Ebserh.

Saída: Partes Interessadas identificadas.

2.6.2. Atividade Elaborar o Plano de Comunicação

Nesta atividade, o Responsável pela Gestão de Riscos de TI, após identificar as partes interessadas, necessita reunir todos os elementos necessários para a comunicação, e elaborar o Plano de Comunicação de GRTI.

Entrada: Partes Interessadas identificadas.

Saída: Planilha Plano de Comunicação do Plano de Riscos de TI da Ebserh.

2.6.3. Atividade Comunicar Partes Interessadas

Elaborado o plano de comunicação, as partes interessadas devem ser comunicadas conforme o planejamento, respeitando o destinatário da comunicação, o prazo, seu conteúdo e a necessidade ou não da parte interessada dar um feedback sobre o conteúdo comunicado.

Entrada: Planilha Plano de Comunicação do Plano de Riscos de TI da Ebserh.

Saída: Partes Interessadas comunicadas.

2.6.4. Atividade Comunicar Mudanças no Processo de GRTI

Sempre que alguma mudança ocorrer ao Processo de GRTI, esta deve ser comunicada às partes interessadas. Como não se trata de comunicação sobre os resultados da GRTI, a Ebserh como um todo pode ser comunicada sobre o Processo, para conhecimento da estrutura em vigor do Processo.

Entrada: Planilha Plano de Comunicação do Plano de Riscos de TI da Ebserh.

Saída: Partes Interessadas comunicadas.

2.6.5. Atividade Comunicar Plano de Contexto

O Plano de Contexto é o documento que dá a direção de execução da GRTI na Ebserh.

Desta forma, a comunicação deve ocorrer sempre que este for elaborado ou alterado, para que todos os envolvidos tomem conhecimento, inclusive sobre seus próprios papéis e responsabilidades no escopo da GRTI, constantes no documento.

A comunicação do Plano de Contexto deve ocorrer sempre antes do início de qualquer nova análise ou quando algum de seus elementos sofrer alterações.

Entrada: Planilha Plano de Comunicação.

Saída: Partes Interessadas comunicadas.

2.6.6. Atividade Comunicar Matriz de Riscos

A Matriz de Riscos é base do Processo de GRTI.

Sempre que a Matriz de Riscos sofrer qualquer alteração deve ser comunicada para as Partes Interessadas.

Entrada: Planilha Plano de Comunicação do Plano de Riscos de TI da Ebserh.

Saída: Partes Interessadas comunicadas.

2.6.7. Atividade Receber Feedbacks

Eventualmente, as Partes Interessadas venham comunicar informações relevantes sobre o Processo de GRTI, o Plano de Contexto ou a Matriz de Riscos.

Essas informações devem ser formalizadas para o Representante de TI e registradas.

Entrada: Partes Interessadas.

Saída: Registro de feedbacks das Partes Interessadas.

2.7. Subprocesso Monitorar Riscos

O subprocesso **Monitorar Riscos** é transversal e tem como objetivo acompanhar cada atividade e cada resultado gerado pelo Processo de GRTI.

Por meio do monitoramento, a Ebserh terá conhecimento sobre o andamento da GRTI como um todo, podendo, assim, identificar pontos de falhas e melhorias a serem implementadas, visando com que os resultados esperados possam ser alcançados.

O Subprocesso Monitorar Riscos deverá ser conduzido conforme apresentado na Figura 15.

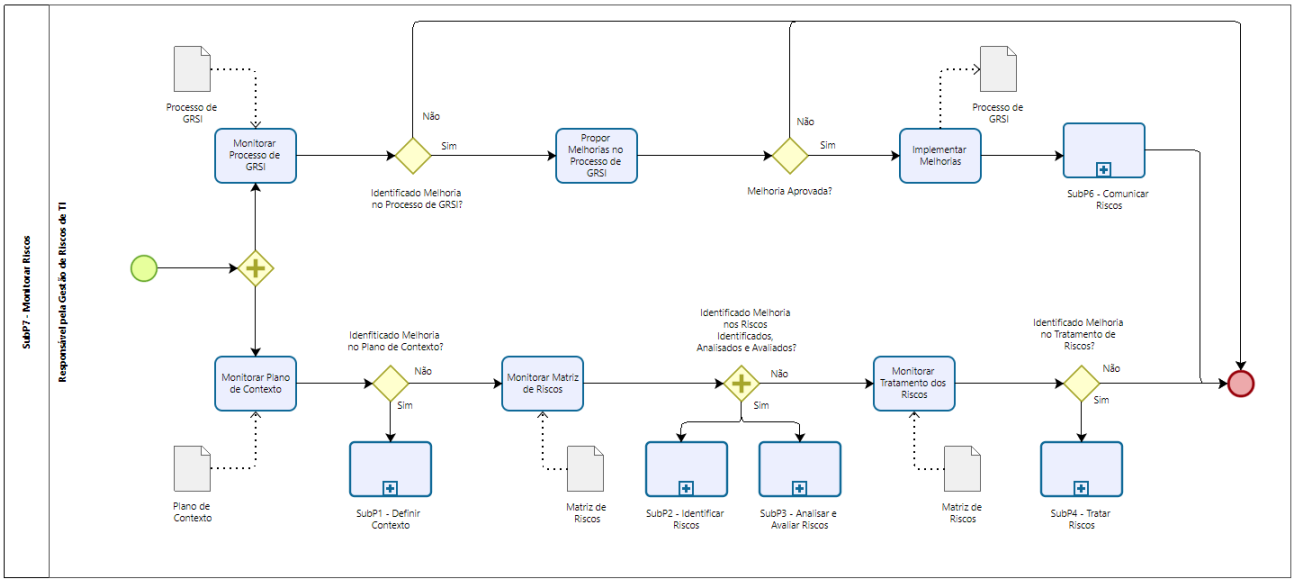

Figura 15 – Subprocesso 7 - Monitorar Riscos

2.7.1. Atividade Monitorar Processo de GRTI

Nesta atividade, é necessário monitorar todas as ações de todos os subprocessos de GRTI e verificar inconsistências e eventuais necessidades de ajustes, tanto para correção, quanto para aprimoramento do Processo e de seus artefatos.

Por se tratar de um subprocesso transversal, este deve ser executado continuamente, e se possível em períodos de tempo pré-determinados. O objetivo é identificar melhorias que podem estar relacionadas aos fluxos das atividades, documentos complementares, papéis do Processo, tempos de execução, documentos de controle, meios de comunicação ou quaisquer outros artefatos.

Se melhorias foram identificadas então elas devem ser propostas para serem avaliadas pelo Responsável pela Gestão de Riscos de Tecnologia da Informação.

Entrada: Processo de Gestão de Riscos de Tecnologia da Informação.

Saída: Melhorias identificadas.

2.7.2. Atividade Propor Melhorias no Processo de GRTI

Nesta atividade, com as melhorias identificadas, deve-se envolver as partes interessadas, para analisar os benefícios trazidos pelas melhorias propostas.

Com a aprovação formal das melhorias estas devem ser encaminhadas para implementação.

Entrada: Melhorias identificadas.

Saída: Melhorias aprovadas para implementação.

2.7.3. Atividade Implementar Melhorias

Nesta atividade, as melhorias aprovadas pelas partes interessadas devem ser implementadas.

A implementação deve seguir o formalismo da Ebserh em relação às alterações processuais e comunicada antes e depois de serem realizadas, garantindo a ideal preparação e consequente adaptação da Ebserh em razão de tais ajustes em seus Processos.

Entrada: Melhorias aprovadas para implementação.

Saída: Melhorias implementadas.

2.7.4. Atividade Monitorar Plano de Contexto

Monitorar o Plano de Contexto é atividade que deve ser realizada durante todo o ciclo de vida do Processo de GRTI, pois é a forma pela qual a Ebserh toma conhecimento sobre a correta execução deste Processo.

Além disto, monitorar o Plano de Contexto significa garantir que cada atividade da sua elaboração está sendo seguida e que nenhum elemento essencial está sendo desconsiderado, evitando a invalidação do Plano de Contexto e, consequentemente, toda a GRTI.

Entrada: Planilha Plano de Contexto do Plano de Riscos de TI da Ebserh.

Saída: Melhorias do Plano de Contexto identificadas e executadas conforme o subprocesso Definir Contexto.

2.7.5. Atividade Monitorar a Matriz de Riscos

A Matriz de Riscos é um elemento vivo do Processo de GRTI e evolui à medida que o escopo da GRTI é alterado e que novos resultados de análise são obtidos.

Monitorar a matriz significa tomar conhecimento sobre qualquer mudança relacionada aos riscos identificados, analisados e avaliados pela Ebserh. Da mesma forma, o monitoramento deve se dar também na estrutura operacional da matriz, identificando necessidades de ajustes ou correções que possam aprimorar a visão que a Ebserh tem dos riscos.

Entrada: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Melhorias da Matriz de Riscos identificadas e executadas conforme o subprocesso Identificar Riscos ou Analisar e Avaliar Riscos.

2.7.6. Atividade Monitorar Tratamento dos Riscos

Monitorar o Tratamento dos Riscos está diretamente relacionado à tomada de conhecimento por parte da Ebserh sobre a correta aplicação dos controles necessários para a mitigação de riscos, total ou parcialmente.

Neste contexto, monitorar a atividade de tratamento é essencial para que os riscos identificados não sofram alterações que possam trazer prejuízos à Ebserh, enquanto ainda não foram tratados.

Entrada: Planilha Matriz de Riscos do Plano de Riscos de TI da Ebserh.

Saída: Melhorias da Matriz de Riscos identificadas e executadas conforme o subprocesso Tratar Riscos.

3. Monitoramento de Valor do Processo

O Processo de Gestão de Riscos de TI deve ser monitorado quanto ao valor do seu propósito, isto é, se o Processo habilita a proteção adequada aos ativos de TI, de maneira contínua e sistemática.

Esse monitoramento é realizado através da verificação de Fator Crítico de Sucesso (FCS), isto é, condições que identificam se a execução do Processo está atingindo a qualidade esperada frente ao propósito do Processo, cujo acompanhamento é realizado através dos Indicadores de Desempenho, associados por FCS.

Fator Crítico de Sucesso 1	Melhorias em Gestão de Riscos		
Indicador de Desempenho	**Período**	**Objetivo**	**Captura de Dados**
ID 1 – O número de melhorias sugeridas para os procedimentos e controles de segurança foram implementadas.	Trimestral	Objetivo: Acompanhar o percentual de implementações de melhorias nos procedimentos e controles de segurança Fórmula: ((# melhorias propostas - # melhorias rejeitadas) / # melhorias propostas) * 100	Subprocesso 7 – Monitorar Riscos Atividade – Propor melhorias no Processo GRTI
ID 2 – Diminuição no número de não conformidade de segurança detectadas durante as auditorias e testes de segurança.	Trimestral	Objetivo: Acompanhar o percentual de não conformidades detectadas de segurança da informação durante as auditorias e testes de segurança. Fórmula: ((# de não conformidades - # auditorias e testes realizados) / # auditorias e testes realizados) * 100	Subprocesso 2 – Identificar Riscos Atividade – Identificar Riscos
Fator Crítico de Sucesso 2	**O negócio está protegido contra violações de segurança**		
ID 3 - Aumento da porcentagem em conformidades com SLA para cláusulas de segurança	Trimestral	Objetivo: Controlar o percentual de incidentes ocorridos devido aos riscos não tratados Fórmula: ((# incidentes não tratados - # incidentes ocorridos) / # incidentes ocorridos) * 100	Subprocesso 4 – Tratar Riscos Atividade - Plano de Tratamento de Riscos

Para acompanhamento do desempenho do Processo de Gestão de Riscos de TI, os artefatos Planilha de Gestão de Risco e Checklist de Riscos ficarão disponíveis e acessíveis à equipe de cada HUF, compartilhada no Teams em: Equipe/Gestão de Risco na pasta Arquivos.

4. Referências

As seguintes referências são base de conhecimento para a estruturação deste Relatório do Processo de Gestão de Riscos:

- ABNT NBR ISO IEC 31000:2009, Gestão de Riscos – Princípios e diretrizes.
- ABNT NBR ISO IEC 27001:2013, Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da Segurança da Informação – Requisitos.
- ABNT NBR ISO IEC 27002:2013, Tecnologia da informação – Técnicas de segurança – Código de prática para controles de Segurança da Informação.
- ABNT NBR ISO IEC 27005:2011, Tecnologia da informação – Técnicas de segurança – Gestão de riscos de Segurança da Informação.
- Instrução Normativa Nº. 01/DSIC/GSIPR, Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta.
- Norma Complementar Nº. 02/IN01/DSIC/GSIPR, Metodologia de Gestão de Segurança da Informação e Comunicações.
- Norma Complementar Nº. 04/IN01/DSIC/GSIPR, Diretrizes para o Processo de Gestão de Riscos de Segurança da Informação e comunicações.
- Política de Gestão de Riscos e Controles Internos – Ebserh.
- Regimento Interno - Ebserh (3ª Revisão), aprovado na 49ª Reunião do Conselho de Administração, realizada no dia 10 maio de 2016.
- Arquitetura de Processos e Arquitetura Organizacional da Rede Ebserh - Cadeia de Valores.
- Política de Segurança da Informação – Ebserh.

5. Glossário e principais conceitos

Para manter o entendimento claro do vocabulário, modelos, etc., utilizados na elaboração deste Processo de Gestão de Risco, os conceitos que servem de base e são citadas ao longo do relatório encontram-se, também, no Dicionário de Referência de TI disponível na Intranet em: http://intranet.ebserh.gov.br/tecnologia-da-informacao/dicionario.

6. Anexos

Apêndice 1 – Planilha Plano de Riscos de TI

Apêndice 2 – Planilha Checklist de Riscos de TI