ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

PLANO DE GESTÃO DE RISCOS DE TIC

Índice

1. Objetivo
2. Aplicabilidade
3. Referências Normativas
4. Metodologia de Gestão de Riscos
5. Processos de Gestão de Riscos
6. Implementação da Gestão de Riscos

1. Objetivo

Este documento tem por objetivo detalhar os processos de gestão de riscos, metodologia de riscos e a implementação da gestão de riscos em Serviços Críticos de Tecnologia da Informação e Comunicação /(TIC).

2. Aplicabilidade

Este documento tem aplicabilidade para toda a Secretaria de Tecnologia da Informação (SETIN), sem prejuízo da utilização de outras normas complementares específicas relativas ao processo de trabalho, projetos ou ações.

3. Referências Normativas

As principais referências para a elaboração deste plano foram a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), Portaria CNJ 162/2021, ISO/IEC 27005:2019, ISO/IEC 31000:2018, Processo de Gestão de Riscos e Metodologia de Gestão de Riscos do TJCE (Portaria 1186/2018 do TJCE).

4. Metodologia de Gestão de Riscos

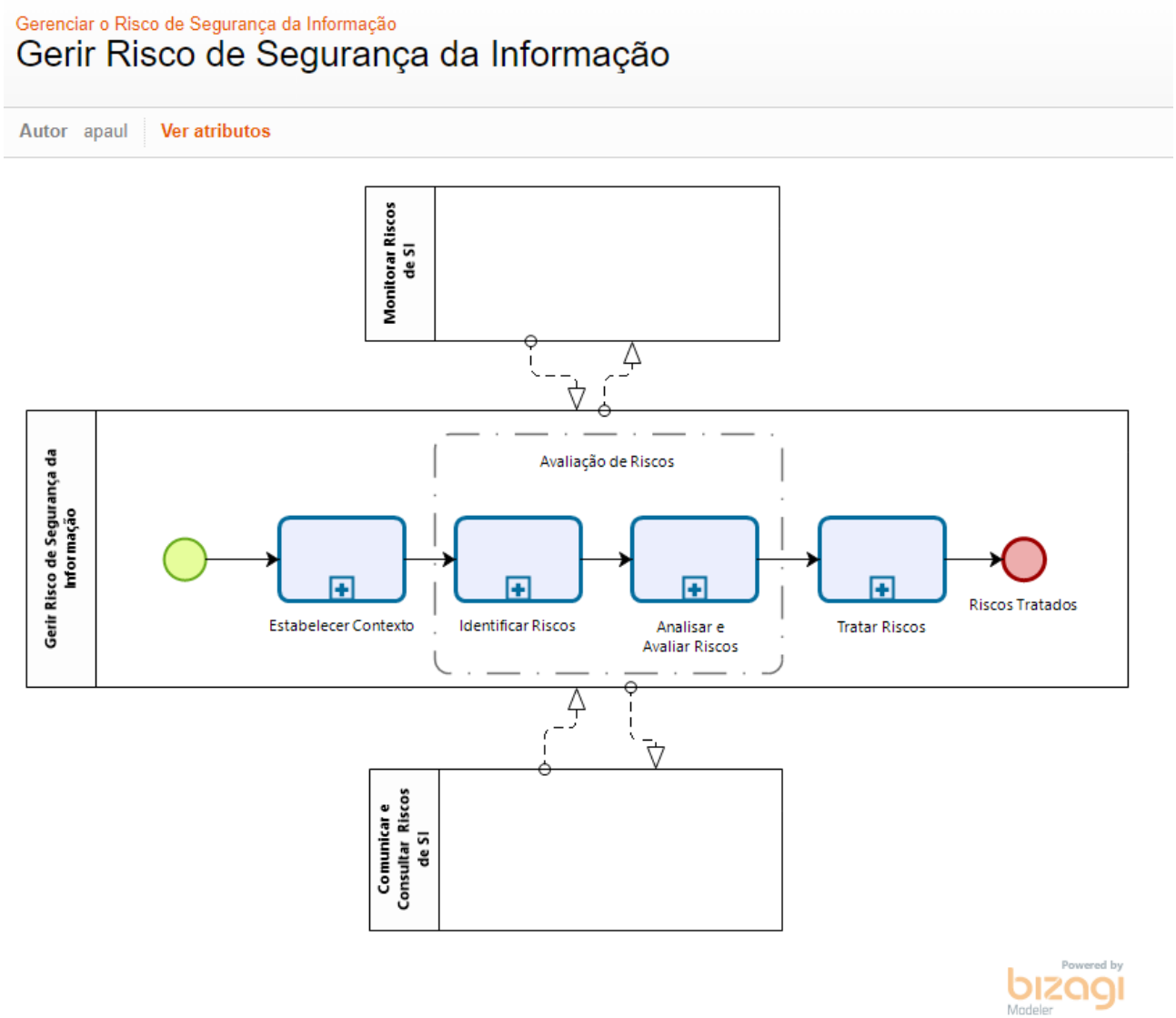
4.1. Deverá ser adotada como metodologia o conteúdo do Anexo VI – Norma de gestão de riscos – Metodologia de Gestão de Riscos de Segurança da Informação, Portaria 1186/2018 do TJCE que apresenta a Metodologia de Gestão de Riscos em Segurança da Informação para o Poder Judiciário do Estado do Ceará, bem como descreve os procedimentos correlatos ao referido Processo.

5. Processos de Gestão de Riscos

5.1. Processos de Gestão de Riscos:

Macroprocesso Gerir o Risco de Segurança da Informação que é dividido nos seguintes processos: Estabelecer Contexto, Identificar Riscos, Analisar e Avaliar Riscos, Tratar Riscos, Comunicar e Consultar Riscos de SI e Monitorar Riscos de SI.

5.1.1. Macroprocesso Gerir o Risco de Segurança da Informação



5.1.2. O detalhamento dos processos Estabelecer Contexto, Identificar Riscos, Analisar e Avaliar Riscos, Tratar Riscos, Comunicar e Consultar Riscos de SI e Monitorar Riscos de SI estão no ANEXO I – Gerenciar o Risco de Segurança da Informação.

6. Implementação da Gestão de Riscos

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

6.1. Indicador 1: Índice de Serviços Críticos com Gestão de Risco (ANEXO II – INDICADORES E METAS DESDOBRAMENTO DA ESTRATÉGIA – SETIN ,PORTARIA Nº 986/2021)

Indicador 1: Índice de Serviços Críticos com Gestão de Risco						
Objetivo Estratégico	Fortalecer a inteligência de dados e a segurança da informação					
Objetivo de Contribuição	Proporcionar segurança, disponibilidade e confiabilidade às informações dos sistemas, plataformas e ferramentas institucionais					
Descrição do indicador	Mede o percentual de serviços críticos que possuem a gestão de risco implementada ao(s) seu(s) processo(s)					
Orientação	↑ (maior-melhor)					
Frequência de medição	Mensal					
Como medir	Número de serviços críticos com gestão de risco / total de serviços críticos					
Forma de acompanhamento e/ou fonte de consulta	1 - Planilha do setor contendo os serviços com gestão de risco; 2 - Ferramento Risk manager					
Responsável pelos dados	Adarildo de Brito Figueiredo					
Linha de base	7% (2020)					
Descrição da Meta	Ter 100% de serviços críticos com gestão de risco até 2026					
Metas anuais	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**
	13%	27%	40%	53%	80%	100%
Gestor das Metas	Supervisor Operacional do Serviço de Segurança da Informação.					
Observações	-					

6.2. Serviços Críticos

6.2.1. Acesso à internet;

6.2.2. Ambiente de virtualização;

6.2.3. Gerência de Identidades – Active Directory;

6.2.4. Correio eletrônico;

6.2.5. Servidores Virtuais e Físicos;

6.2.6. Banco de Dados;

6.2.7. Site do TJCE;

6.2.8. Rede de Dados e Conectividade relativo aos equipamentos dos datacenters do TJCE e Fórum Clóvis Beviláqua;

6.2.9. Backup e Restore;

6.2.10. Balanceadores de Aplicações;

6.2.11. Storages;

6.2.12. Firewalls;

6.2.13. Videoconferência (Equipamentos concentradores e de gerência).

6.3. Matriz de Análise e Avaliação de Riscos

MATRIZ DE ANÁLISE E AVALIAÇÃO DE RISCOS										
Sistema Crítico	**Gestor do Risco**	**Eventos de Riscos**	**Causa**	**Consequencias**	**Probabilidade (P)**	**Severidade (S)**	**Relevancia (R)**	**Medida Do Risco (PxSxR)**	**Nível Medida De Risco**	**RespostaAo Risco**
Acesso à internet;	Gerencia de Infraestrura de TI	Vulnerabilidade	Ser explorada Pelas Ameaças	Comprometimento de Segurança dos Ativos	2	2	3	12	Baixo	Aplicar controles/recomendações de Segurança conforme documentos De segurança dos fabricantes
Ambiente de virtualização;	Gerencia de Infraestrura de TI	Vulnerabilidade	Ser explorada Pelas Ameaças	Comprometimento de Segurança dos Ativos	3	5	5	75	Muito Alto	Aplicar controles/recomendações de Segurança conforme documentos De segurança dos fabricantes
Gerência de Identidades – Active Directory;	Serviço de Segurança da Informação	Vulnerabilidade	Ser explorada Pelas Ameaças	Comprometimento de Segurança dos Ativos	3	5	5	75	Muito Alto	Aplicar controles/recomendações de Segurança conforme documentos De segurança dos fabricantes
Correio eletrônico;	Gerencia de Infraestrura de TI	Vulnerabilidade	Ser explorada Pelas Ameaças	Comprometimento de Segurança dos Ativos	5	4	4	80	Muito Alto	Aplicar controles/recomendações de Segurança conforme documentos De segurança dos fabricantes
Servidores Virtuais e Físicos;	Gerencia de Infraestrura de TI	Vulnerabilidade	Ser explorada Pelas Ameaças	Comprometimento de Segurança dos Ativos	3	5	5	75	Muito Alto	Aplicar controles/recomendações de Segurança conforme documentos De segurança dos fabricantes
Banco de Dados;	Gerencia de Infraestrura de TI	Vulnerabilidade	Ser explorada Pelas Ameaças	Comprometimento de Segurança dos Ativos	3	5	4	60	Muito Alto	Aplicar controles/recomendações de Segurança conforme documentos De segurança dos fabricantes
Site do TJCE;	Gerencia de Sistemas	Vulnerabilidade	Ser explorada Pelas Ameaças	Comprometimento de Segurança dos Ativos	5	4	4	80	Muito Alto	Aplicar controles/recomendações de Segurança conforme documentos De segurança dos fabricantes
Rede de Dados e Conectividade relativo aos equipamentos dos datacenters do TJCE e Fórum Clóvis Beviláqua;	Gerencia de Infraestrura de TI	Vulnerabilidade	Ser explorada Pelas Ameaças	Comprometimento de Segurança dos Ativos	3	5	5	75	Muito Alto	Aplicar controles/recomendações de Segurança conforme documentos De segurança dos fabricantes
Backup e Restore;	Serviço de Segurança da Informação	Vulnerabilidade	Ser explorada Pelas Ameaças	Comprometimento de Segurança dos Ativos	3	5	5	75	Muito Alto	Aplicar controles/recomendações de Segurança conforme documentos De segurança dos fabricantes
Balanceadores de Aplicações;	Serviço de Segurança da Informação	Vulnerabilidade	Ser explorada Pelas Ameaças	Comprometimento de Segurança dos Ativos	3	5	5	75	Muito Alto	Aplicar controles/recomendações de Segurança conforme documentos De segurança dos fabricantes
Storages;	Gerencia de Infraestrura de TI	Vulnerabilidade	Ser explorada Pelas Ameaças	Comprometimento de Segurança dos Ativos	3	5	5	75	Muito Alto	Aplicar controles/recomendações de Segurança conforme documentos De segurança dos fabricantes
Firewalls;	Serviço de Segurança da Informação	Vulnerabilidade	Ser explorada Pelas Ameaças	Comprometimento de Segurança dos Ativos	3	5	5	75	Muito Alto	Aplicar controles/recomendações de Segurança conforme documentos De segurança dos fabricantes
Videoconferência (Equipamentos Concentradores e de gerência).	Gerencia de Infraestrura de TI	Vulnerabilidade	Ser explorada Pelas Ameaças	Comprometimento de Segurança dos Ativos	4	3	4	48	Alto	Aplicar controles/recomendações de Segurança conforme documentos De segurança dos fabricantes

6.4. Metas Anuais

DESCRIÇÃO DA META	METAS ANUAIS						
	LINHA DE BASE (VO)	2021	2022	2023	2024	2025	2026
Ter 100% de serviços críticos com gestão de risco até 2026.	7% (2020)	13%	27%	40%	53%	80%	100%