Plano de Gestão de Riscos de Segurança da Informação

UNIVERSIDADE FEDERAL DE PERNAMBUCO
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

UFPE

Plano de Gestão de Riscos de Segurança da Informação

Gestor de Segurança da Informação e Superintendente da STI

Marco Aurelio Benedetti

Diretora da Diretoria de Governança e Gestão de Tecnologia da Informação da STI

Rosângela Saraiva Carvalho

Grupo de Trabalho

André Souto Soares Afonso

Bartolomeu Alves Bezerra II

Daniel Wanderley Vieira

Denisson Paulo de Albuquerque

Diogo Moura Dias

Francisco Juvenal Feitosa Neves Junior

Lucindo Albuquerque de Melo

Maria Betania Martins da Silva

Pedro Corrêa de Araújo Neto

Xerxes Xavier Lins

Recife - 2022

Sumário

1. Introdução

O Plano de Gestão de Riscos de Segurança da Informação tem por objetivo direcionar e controlar os riscos dos ativos de segurança da informação, a fim de adequá-los aos níveis aceitáveis para a Universidade Federal de Pernambuco (UFPE). Este documento tem como escopo os ativos físicos e lógicos presentes na Superintendência de Tecnologia da Informação (STI) e voltado para gestores e colaboradores da UFPE.

Este plano é alinhado à:

- Política de Segurança da Informação da UFPE de 2022;
- Política de Gestão de Riscos da UFPE de 2017;
- Instrução Normativa GSI/PR Nº 03 de 2021;
- ABNT NBR ISO/IEC 27005 de 2019;
- ABNT NBR ISO/IEC 31000 de 2018.

Assim, este documento estabelece um plano de ação contendo o processo de gestão de riscos de segurança da informação com vistas a orientar sobre: a identificação, a análise, a avaliação, o tratamento, o monitoramento e a comunicação dos riscos inerentes aos recursos, serviços e sistemas informatizados da UFPE.

Para que o objetivo geral seja alcançado, foram definidos os seguintes objetivos específicos:

a) Definir o escopo e a abrangência dos ativos a serem analisados;
b) Definir os papéis e responsabilidades de cada integrante do processo de gestão de riscos;
c) Definir as atividades e tarefas que compõem o processo de gestão de riscos;
d) Definir as técnicas para identificação, análise, avaliação, tratamento, monitoramento e comunicação de riscos.

2. Definições e Abreviações

Ativo: “qualquer coisa que tenha valor para a organização, material ou não” (Brasil, 2019);

Ativo de informação: “meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso” (Brasil, 2019);

Backup ou Cópia de Segurança: “conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada” (Brasil, 2019);

Escopo: Limite ou abrangência de uma operação;

GSI/PR: Gabinete de Segurança Institucional da Presidência da República;

GTGRSI[1]: Grupo de Trabalho de Gestão de Riscos de Segurança da Informação

Impacto: efeito de uma ação, consequência;

Mitigar: fazer com que fique mais brando, mais tênue, atenuar;

Nível de Severidade: refere-se a escala relativa a gravidade do risco;

Probabilidade: chance de que algo ocorra;

Responsável pelo ativo: coordenação ou diretoria responsável pela sua produção, desenvolvimento, manutenção, utilização e segurança, podendo não ter direito de propriedade sobre o ativo.

Risco: potencial associado à exploração de uma ou mais vulnerabilidades de um ou um conjunto de ativo de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

SIG@: Sistema de informações e gestão acadêmica ;

SIGAA: Sistema integrado de gestão de atividades acadêmicas

SIGRH: Sistema integrado de gestão de recursos humanos;

SIPAC: Sistema integrado de gestão de patrimônio, administração e contratos;

Software: conjunto de componentes lógicos de um computador ou sistema de processamento de dados;

STI: Superintendência de Tecnologia da Informação;

UFPE: Universidade Federal de Pernambuco.

3. Escopo e Abrangência

Este plano tem como alvo os ativos gerenciados pela STI e localizados fisicamente na STI,. Os ativos a serem analisados serão:

- Colocation (Hospedagem), quanto ao serviço de colocation;
- Equipamentos de armazenamento, processamento e distribuição de dados;
- Estações de trabalho;
- Infraestrutura física do datacenter;
- Colaboradores, tais como servidores públicos, bolsistas e terceirizados;
- Sistema de backup;
- Sistemas da UFPE, tais como SIG@, SIPAC, SigRH;
- Sistemas de terceiros, tais como as parcerias com o Google e Microsoft;

[1] GTRSI: Designados pela portaria Nº 344, de 26 de Janeiro de 2022, da UFPE.

4. Papéis e responsabilidades

- **Coordenação de Segurança da Informação**
    - Monitorar e analisar criticamente documentos produzidos pelo GTRSI e atualizá-los, quando pertinente.
- **Gestor de segurança da Informação**:
    - Coordenar o processo de gestão de riscos de segurança da informação;
    - Designar o grupo de trabalho de gestão de riscos de segurança da informação;
    - Aprovar os documentos elaborados pelo grupo de trabalho de gestão de riscos de segurança da informação;
    - Propor medidas preventivas à alta administração da instituição.
- **Grupo de trabalho de gestão de riscos de segurança da informação:**
    - Elaborar o Plano de Gestão de Riscos de Segurança da Informação;
    - Elaborar relatório de identificação, análise e avaliação dos riscos de segurança da informação;
    - Elaborar relatório de tratamento de riscos de segurança da informação;
    - Comunicar e consultar as partes interessadas nos riscos dos ativos.
- **Responsável pelo ativo.**
    - Colaborar com o GT GRSI na identificação dos riscos existentes no ativos;
    - Colaborar com o GT GRSI na escolha da estratégia e a abordagem a ser utilizada no controle do risco.
- **Responsável pela implantação do controle**
    - Poderá ser o responsável pelo ativo ou alguém indicado pela STI;
    - Implantar os controles definidos no relatório de tratamento de riscos de segurança da informação

5. Processo de gestão de riscos

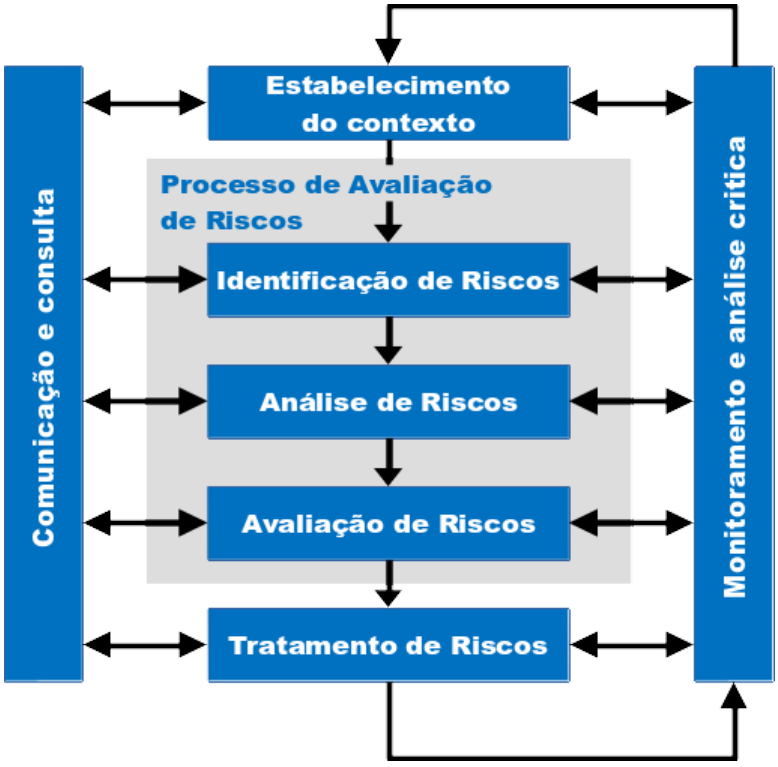
O processo de gestão de riscos de segurança da informação, a ser executado durante a vigência deste plano, possui as seguintes etapas:

- Estabelecimento do Contexto;
- Processo de Avaliação de Riscos;
    - Identificação de risco;
    - Análise de risco;

- Avaliação de riscos.
- Tratamento de Riscos;
- Monitoramento e Análise Crítica e
- Comunicação e Consulta.

Uma visão de alto nível do processo de gestão de riscos pode ser observada na figura abaixo.

Processo de Gestão de Risco



Fonte: ABNT NBR ISO 31000:2018

5.1. Estabelecimento do contexto

Ao iniciar as atividades para a elaboração do Plano de Gestão de Riscos de Segurança da Informação, a primeira tarefa consiste em compreender o ambiente no qual o trabalho será desenvolvido, definir o escopo e a abrangência a serem considerados no referido processo de gestão de riscos, definir as etapas, os níveis de riscos e os tipos de riscos a serem considerados. O estabelecimento do contexto tem como produto este documento, o "**Plano de Gestão de Riscos de Segurança da Informação**". Caberá ao GT GRSI a execução desta atividade.

5.2. Processo de Avaliação de Riscos

O processo de avaliação de riscos é a etapa onde os riscos são identificados, quantificados ou descritos qualitativamente, priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes.

Esta etapa é subdividida em:

- Identificação de Riscos;
- Análise de Riscos;
- Avaliação de Riscos.

O processo de avaliação de riscos tem como produto o "**Relatório de identificação, análise e avaliação dos riscos de segurança da informação**" que deverá ser elaborado com base no modelo estabelecido. Caberá ao GT GRSI a realização destas atividades.

5.2.1. Identificação de Riscos

O propósito da identificação de riscos é determinar o que pode causar uma perda potencial e deixar claro como, onde e porque a perda pode acontecer. Os riscos identificados devem estar associados a cada ativo de informação, considerando as ameaças envolvidas, as vulnerabilidades existentes e as ações de segurança da informação já implementadas. Esta etapa será realizada a partir de reuniões do GT GRSI e subdivide-se nas etapas a seguir:

Identificação dos ativos: Os ativos serão selecionados para análise considerando o escopo estabelecido no capítulo 3 e o mapeamento dos ativos realizado pela STI. É importante que um responsável seja identificado para cada ativo, sendo este denominado responsável pelo ativo.

Identificação dos controles existentes: Levantamento dos controles existentes e planejados, para tal pode ser necessário consulta ao PEI (Plano Estratégico Institucional), PDI (Plano de Desenvolvimento Institucional), PAI (Plano de Ação Institucional) e PDTI (Plano Diretor de Tecnologia da Informação). A identificação visa reduzir o retrabalho e validação para assegurar que os controles estão funcionando corretamente.

Identificação de riscos: Estudo baseado nas ameaças e vulnerabilidades dos ativos. Uma ameaça tem o potencial de comprometer ativos como informações, processos e sistemas. Ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais. Vulnerabilidade é uma condição que, quando explorada, pode resultar em uma violação de segurança. A presença de uma vulnerabilidade não causa prejuízo por si só, pois precisa haver uma ameaça presente para explorá-la. Uma vulnerabilidade que não tem uma ameaça correspondente pode não requerer a implementação de um controle no presente momento, mas convém que ela seja reconhecida como tal e monitorada, no caso de haver mudanças. Os tipos de riscos a serem analisados deverão seguir conforme listado no capítulo 6.

Identificação das consequências: Identifica o prejuízo ou as consequências para a organização que podem decorrer de um cenário de incidente. Um cenário de

incidente é a descrição de uma ameaça explorando uma certa vulnerabilidade ou um conjunto delas, caracterizando assim um incidente de segurança da informação.

5.2.2. Análise de Riscos

Na análise de riscos, para cada um dos riscos identificados na etapa anterior, o GT GRSI deve seguir os seguintes passos: a) Avaliar as consequências e, b) A probabilidade de ocorrer um incidente. Com isso, definir o nível desse risco.

Na avaliação das consequências é analisado o impacto sobre o negócio, o que pode ser causado por incidentes relacionados à segurança da informação devido à exploração do risco.

O impacto vai ser avaliado segundo a escala a seguir:

Escala do impacto	
Muito Baixo	Compromete minimamente o fornecimento do serviço oferecido à sociedade.
Baixo	Compromete em alguma medida o fornecimento do serviço oferecido à sociedade.
Médio	Compromete razoavelmente o fornecimento do serviço oferecido à sociedade.
Alto	Compromete a maior parte do serviço oferecido à sociedade.
Muito Alto	Compromete totalmente ou quase totalmente o serviço oferecido à sociedade.

Na avaliação da probabilidade de ocorrer um incidente é feita uma análise dos riscos frente aos controles existentes. Portanto a probabilidade é a chance de um incidente de segurança da informação ocorrer considerando os controles existentes. Para estimar a probabilidade será usada uma escala qualitativa de cinco níveis, conforme descrito a seguir:

Escala de Probabilidade	
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.

Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.
Muito Alta	Praticamente certa. De forma inequívoca, o evento ocorrerá. As circunstâncias indicam explicitamente essa possibilidade.

Para a definição do nível de severidade do risco é estimada uma combinação da probabilidade entre um cenário de incidente e suas consequências, conforme a tabela a seguir:

Nível de Severidade do Risco						
Impacto	Muito Alto	5	10	15	20	25
	Alto	4	8	12	16	20
	Médio	3	6	9	12	15
	Baixo	2	4	6	8	10
	Muito Baixo	1	2	3	4	5
		Muito Baixa	Baixa	Média	Alta	Muito Alta
		Probabilidade				

Fonte: Manual de gestão de riscos operacionais - UFPE

Podendo ser então considerado:

Nível de severidade	
1 à 3	Baixo
4 à 6	Médio
8 à 12	Alto
15 à 25	Crítico

5.2.3. Avaliação de Riscos

A avaliação do risco envolve a comparação do nível de risco do ativo com o limite de exposição a riscos, a fim de determinar que riscos a UFPE está disposta a aceitar. Espera-se que com os resultados do tratamento ao nível de risco real fique abaixo do limite de exposição tolerável.

A ação prática do GTGRSI nesta fase deve ser: identificar, na matriz probabilidade e impacto, os riscos cujos níveis estão acima do limite de exposição a

riscos (altos e críticos) e, para esses riscos, identificar as respectivas fontes, causas e consequências; os riscos que estão na faixa verde, abaixo do limite de exposição, deverão ser aceitos e reavaliados periodicamente seguindo a etapa de “Monitoramento e análise crítica”.

5.3. Tratamento de Riscos

Tratamento de riscos compreende o planejamento de ações para modificar o nível de severidade do risco. O nível de severidade do risco pode ser modificado por meio de medidas para resposta ao risco que mitiguem, evitem ou compartilhem esses riscos.

O tratamento de riscos tem como produto o “**Relatório de tratamento de riscos de segurança da informação**” que deverá ser elaborado com base no modelo estabelecido.

O GTGRSI inicia esta etapa com a priorização dos riscos apresentados na matriz de probabilidade e impacto. Em seguida serão avaliados e discutidos as possíveis abordagens para o controle do risco. Será então discutido com o responsável pelo ativo a estratégia e a abordagem a ser utilizada no controle do risco. As estratégias que podem ser utilizadas são: mitigar, aceitar, evitar e compartilhar o risco, conforme tabela abaixo.

Estratégia	Descrição
Mitigar	O risco precisa ser gerenciado pela inclusão, exclusão ou alteração de controles, para que o risco residual possa ser reavaliado e considerado aceitável.
Aceitar	O objetivo dessa resposta é avaliar se os demais tipos de respostas ao risco são viáveis. Em algumas situações, como: risco de baixo nível ou custo desproporcional ao benefício do tratamento, a opção mais adequada é aceitar ou reter o risco. Esses riscos devem ser reavaliados periodicamente para controlar a sua alteração.
Evitar	Inclui basicamente a descontinuação das atividades que geram os riscos. Evitar riscos pode implicar a descontinuação de um software, a alienação de um equipamento ou a extinção de uma divisão ou processo de trabalho.
Compartilhar	Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco. As técnicas comuns compreendem a aquisição de produtos de seguro, a terceirização de uma atividade e outras.

As estratégias a serem adotadas preferencialmente serão de acordo com o nível de severidade do risco, conforme a tabela abaixo:

Nível de severidade do risco	Estratégia a ser adotada
1 à 3	Aceitar
4 à 6	Aceitar / Mitigar
8 à 12	Mitigar / Evitar / Compartilhar
15 à 25	Mitigar / Evitar / Compartilhar

Conclui-se esta atividade com a elaboração do "**Relatório de tratamento de riscos de segurança da informação**" que deve conter o risco, o controle proposto, o prazo para implantação do controle, o responsável pela implantação do referido controle e o nível de risco esperado após a implantação do controle. O responsável pela implantação do controle poderá ser o responsável pelo ativo ou alguém indicado pela STI. Caberá ao GTGRSI, com o apoio dos responsáveis pelos ativos, a realização desta atividade.

5.4. Monitoramento e análise crítica

O monitoramento trata da revisão e avaliação periódica da gestão de riscos, objetivando aprimorar continuamente a qualidade dos serviços oferecidos. Caberá à Coordenação de Segurança da Informação, anualmente, a realização desta atividade.

O monitoramento consiste em comparar o que está exposto no "**Relatório de identificação, análise e avaliação dos riscos de segurança da informação**", bem como no "**Relatório de tratamento de riscos de segurança da informação**" com o cenário do momento em que ocorrer o monitoramento. Em caso de ser observada alguma alteração deve ser realizado uma reedição dos referidos relatórios e encaminhado ao gestor de segurança da informação.

5.5. Comunicação e consulta

A atividade de comunicação e consulta refere-se à identificação das partes interessadas e ao compartilhamento de informações relativas à gestão de riscos sobre determinado ativo, observada a classificação da informação quanto ao sigilo. Esta atividade fornece as informações relativas ao risco e ao seu tratamento para todos aqueles que possam influenciar ou ser influenciados por esse risco, sob pena de ele se materializar plenamente. A atividade deve ser realizada durante todo o processo de gestão de riscos pelo GTGRSI.

6. Tipos de Risco

Os ativos serão analisados conforme as vulnerabilidades abaixo relacionadas:

- Armazenamento de datas e horas incorretas
- Armazenamento de senhas em texto não criptografado
- Falta de conscientização em segurança
- Fragilidade de acesso físico ou lógico
- Inexistência de uma trilha de auditoria ("logs")
- Inexistência de cópias de segurança (“backup”)
- Inexistência de um procedimento formal para o registro e a remoção de usuários
- Fornecimento de energia instável
- Localização física suscetível a desastres naturais
- Software sem atualizações
- Software sem suporte do fabricante
- Trabalho não supervisionado de pessoal de limpeza ou de terceirizados
- Tráfego sensível desprotegido
- Transferência de senhas em texto não criptografado
- Treinamento insuficiente em segurança

Poderão ser adicionadas outras vulnerabilidades intrínsecas diretamente ao ativo conforme necessidade.

7. Revisão do documento

Este plano deverá ser revisado e atualizado a cada quatro anos, a contar da sua vigência ou quando o gestor de segurança da informação considerar necessário.

8. Referências

ABNT NBR ISO 31000, **Gestão de riscos – Princípios e diretrizes**

ABNT NBR ISO/IEC 27005, **Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação**

Brasil, **Glossário de Segurança da Informação,** 26 de setembro de 2019 disponível em : https://www.gov.br/gsi/pt-br/assuntos/dsi/glossario-de-seguranca-da-informacao-1 , acesso: 15 de setembro de 2022.

Brasil, **Instrução Normativa GSI/PR Nº 03**, de 28 de maio de 2021

Política de Gestão de Riscos, Portaria Normativa Nº03, de 5 de maio de 2017 da Universidade Federal de Pernambuco.

Política de Segurança da Informação, Resolução Nº05/2022 do Conselho Administrativo da Universidade Federal de Pernambuco, 21 de Julho de 2022

Emitido em 18/01/2023

ANEXOS Nº 327/2023 - DGGTIC-STI (11.29.20)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 20/01/2023 17:38)
MARCO AURELIO BENEDETTI RODRIGUES
SUPERINTENDENTE - TITULAR
STI (11.29)
Matrícula: 1512338

(Assinado digitalmente em 19/01/2023 14:39)
ROSANGELA SARAIVA CARVALHO
DIRETOR - TITULAR
DGGTIC-STI (11.29.20)
Matrícula: 1133617

Para verificar a autenticidade deste documento entre em http://sipac.ufpe.br/documentos/ informando seu número: **327**, ano: **2023**, tipo: **ANEXOS**, data de emissão: **18/01/2023** e o código de verificação: **df939f1e78**