
	Universidade Federal do Ceará		Página		1/11			
	Superintendência de Tecnologia da Informação - STI			Classificação				
	Coordenadoria de Infraestrutura e Segurança da Informação - CISI				C	X	R	

Processo de Gestão de Riscos de Segurança da Informação e Comunicação

Relatório de Gestão de Riscos

Escopo: XXXXXXXXXXXXXXXXXXXXXXX

*Informações foram retiradas e anonimizadas (Ex.: XXXX) por serem classificadas como restritas.

	Universidade Federal do Ceará		Página		2/11	
	Superintendência de Tecnologia da Informação - STI			Classificação		
	Coordenadoria de Infraestrutura e Segurança da Informação - CISI			C	X	R

Processo de Gestão de Riscos de Segurança da Informação e Comunicação

Relatório de Gestão de Riscos

Escopo: XXXXXXXXXXXXXXXXXXXXXXX

Amarildo Maia Rolim - Siape: XXXXX


Coordenadoria de Infraestrutura e Segurança da Informação - CISI

Coordenador

Rafael Bezerra Firmo- Siape: XXXXX

Coordenadoria de Infraestrutura e Segurança da Informação - CISI


GRISC-Agente responsável

	Universidade Federal do Ceará		Página		3/11	
	Superintendência de Tecnologia da Informação - STI			Classificação		
	Coordenadoria de Infraestrutura e Segurança da Informação - CISI			C	X	R

ÍNDICE

Apresentação	4
1. Gestão de Riscos de Segurança da Informação	4
2. Definição do escopo de atuação	5
3. Papéis envolvidos	6
4. Metodologia	7
5. Resultado do 1º Ciclo da GR na XXX - XXXX/XXX	8
6. Considerações finais	12

*Informações foram retiradas e anonimizadas (Ex.: XXXX) por serem classificadas como restritas.

	Universidade Federal do Ceará		Página		4/11	
	Superintendência de Tecnologia da Informação - STI			Classificação		
	Coordenadoria de Infraestrutura e Segurança da Informação - CISI			C	X	R

Apresentação

O objetivo deste documento é informar o resultado do primeiro ciclo do processo de Gestão de Riscos dos ativos de informação da Divisão XXXXXXXXX, subunidade subordinada à XXXXXXXXX.

Os resultados deste processo obtidos através da coleta de dados dos ativos da subunidade analisada servem como ferramenta auxiliar em nível de gestão para a tomadas de decisões estratégicas e organizacionais quanto à Segurança da Informação dos ativos de TI empregados na entrega de serviços do ambiente analisado.

O texto a seguir se inicia com uma discussão sobre a importância do processo de Gestão de Riscos e as necessidades para sua implementação. O relatório segue com a análise sobre as informações levantadas e os resultados encontrados.

1. Gestão de Riscos de Segurança da Informação e Comunicação

A Instrução Normativa Conjunta (INC) MP/CGU nº 1/2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal determina que:

Art. 1º Os órgãos e entidades do Poder Executivo federal deverão adotar medidas para a sistematização de práticas relacionadas à gestão de riscos, aos controles internos, e à governança.

Art. 13º Os órgãos e entidades do Poder Executivo federal deverão implementar, manter, monitorar e revisar o processo de gestão de riscos, compatível com sua missão e seus objetivos estratégicos, observadas as diretrizes estabelecidas nesta Instrução Normativa.


A Gestão de Riscos de Segurança da Informação e Comunicação (GRSIC) é um processo contínuo, bem estruturado e sistêmico cujo objetivo é assegurar uma proteção adequada para os elementos de valor da organização.

É desejável que a organização realize análises internas voltadas a estabelecer as condições iniciais apropriadas para a implementação da gestão de riscos. Para isso é necessário definir: o propósito dos investimentos em Segurança da Informação e Comunicação (SIC), o escopo de atuação da GRSIC e os papéis envolvidos no processo.

A Universidade Federal do Ceará (UFC) define os propósitos de investimento em SIC através de sua Política de Segurança da Informação e Comunicação (P01/STI/UFC de 08 de abril de 2021). Nela, destaca que devem ser considerados os seguintes aspectos: todo impacto associado aos ativos deve ser avaliado e, se possível, minimizado; e toda ação de segurança da informação deve ser feita com base na avaliação da criticidade dos Ativos.

Essa política define ainda que dentre as responsabilidades da área de Segurança da Informação e Comunicação desta instituição desenvolver ações relacionadas à gestão de riscos. Ressalta-se que o

*Informações foram retiradas e anonimizadas (Ex.: XXXX) por serem classificadas como restritas.

	Universidade Federal do Ceará		Página		5/11	
	Superintendência de Tecnologia da Informação - STI			Classificação		
	Coordenadoria de Infraestrutura e Segurança da Informação - CISI			C	X	R

departamento citado, foi implementado nesta universidade através da Coordenadoria de Infraestrutura e Segurança da Informação (CISI), coordenadoria da Superintendência de Tecnologia da Informação (STI).

A definição do escopo de atuação e dos papéis envolvidos durante o processo serão descritos nas seções seguintes.

2. Definição do escopo de atuação

De acordo com a INC CGU/MP nº 01/2016:

Art. 3º, § 3º Os componentes dos controles internos da gestão e do gerenciamento de riscos aplicam-se a todos os níveis, unidades e dependências do órgão ou da entidade pública.

Art. 4º Os controles internos da gestão devem integrar as atividades, planos, ações, políticas, sistemas, recursos e esforços de todos que trabalhem na organização, sendo projetados para fornecer segurança razoável de que a organização atingirá seus objetivos e missão.

Segundo a Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração de Recursos da Tecnologia da Informação – SISP do Poder Executivo Federal (MGR-SISP), a GRSIC pode ser iniciada em qualquer nível organizacional, podendo ocorrer em diferentes níveis de detalhamento, abordando medidas de proteção mais gerais, aplicáveis à organização como um todo ou a setores dessa.


Após a realização da Pré análise, foi identificado que a primeira divisão a ser iniciado o processo seria a Divisão XXXXXXXX.

O processo seguiu tendo por base os ativos primários listados na pré análise, quais sejam os ativos de informação, serviços e processos. Nesse processo foram registrados os ativos que suportam estes ativos primários.

No processo de Gestão de Riscos foram realizadas as seguintes fases:

- 1 - Identificação de Ativos
- 2 - Identificação de Ameaças
- 3 - Identificação de Controles
- 4 - Identificação de Vulnerabilidades
- 5 - Estimativa de Riscos (Impacto x Probabilidade)
- 6 - Consolidação dos mapas de Riscos

*Informações foram retiradas e anonimizadas (Ex.: XXXX) por serem classificadas como restritas.

	Universidade Federal do Ceará		Página		6/11	
	Superintendência de Tecnologia da Informação - STI			Classificação		
	Coordenadoria de Infraestrutura e Segurança da Informação - CISI			C	X	R

7 - Elaboração dos Planos de Tratamento de Riscos

8 - Acompanhamento / Próximo Ciclo

Os ativos de suporte listados na fase de identificação de ativos são aqueles limitados aos ativos que suportam os ativos primários indicados na Pré-Análise. E a partir desta identificação de ativos, foram realizadas as identificações das ameaças, controles e vulnerabilidades, relacionadas a estes ativos de suporte.

Para geração dos mapas de riscos, isto é, para obter os valores de Riscos de cada ameaça identificada, foi realizada a estimativa do IMPACTO caso a ameaça acontecesse, e qual a PROBABILIDADE da ameaça acontecer. Baseado no histórico de incidentes, da estrutura, configuração, local do ativo de suporte, pelo conhecimento do servidor consultado sobre este ativo, e outra informação relevante que possa influenciar na estimativa de impacto e probabilidade.

Por fim, é elaborado os Planos de Tratamento de Riscos (PTRs) baseados nos mapas de riscos gerados e a partir dos PTRs serão feitos os acompanhamentos até ou no próximo ciclo deste processo.

Inicialmente os ativos de suporte iniciaram com um quantitativo de XX ativos, com o passar do tempo, durante o processo, foram atualizados o quantitativo para XX. Devido a ativos que foram descontinuados, ou aqueles que foram retirados por não fazer mais sentido ele estar presente na lista de ativos ou mesmo por aglutinação entre ativos, por fazer parte de um mesmo sistema ou foram aglutinados para gerar nova organização da identificação, separando alguns ativos por contexto para otimizar as análises.

3. Papéis envolvidos

Para a implementação e atualização da GRSIC, é necessário o envolvimento de profissionais em cada um dos níveis da organização (estratégico, tático e operacional). A Instrução Normativa Conjunta (INC) MP/CGU nº 1/2016 destaca:

Art. 19º O dirigente máximo da organização é o principal responsável pelo estabelecimento da estratégia da organização e da estrutura de gerenciamento de riscos, incluindo o estabelecimento, a manutenção, o monitoramento e o aperfeiçoamento dos controles internos da gestão.


Art. 20º Cada risco mapeado e avaliado deve estar associado a um agente responsável formalmente identificado.

§1º O agente responsável pelo gerenciamento de determinado risco deve ser o gestor com alçada suficiente para orientar e acompanhar as ações de mapeamento, avaliação e mitigação do risco.

De acordo com a MGR-SISP, são previstos os seguintes papéis:

- Autoridade Competente (AC): tomador de decisões;

*Informações foram retiradas e anonimizadas (Ex.: XXXX) por serem classificadas como restritas.

	Universidade Federal do Ceará		Página		7/11	
	Superintendência de Tecnologia da Informação - STI			Classificação		
	Coordenadoria de Infraestrutura e Segurança da Informação - CISI			C	X	R

- Gestor de Riscos (GR): encarregado pela condução e acompanhamento do processo;
- Responsável pela Unidade da Organização (RUO): chefe/diretor da unidade organizacional;
- Responsável por Ativos (RA): membro indicado pelo RUO para participar do processo e fornecer as informações solicitadas pelo GR.

Para a execução da fase de Pré-Análise sob o escopo desta secretaria, os papéis acima foram definidos da seguinte maneira: o superintendente da XXX e o coordenador da CISI como AC; na área da Segurança da Informação temos os agentes responsáveis, para realizar e organizar o processo; o diretor da divisão como RUO, onde este último designou seus representantes como RAs. Sendo que os RA são aqueles que mais conhecem os ativos que puderam contribuir para estimar e prestar as informações necessárias para execução deste processo.

4. Metodologia

Após a realização da Pré-Análise, foi iniciado o processo de Gestão e Riscos na divisão da XXX, ainda em 2018. O processo foi realizado em todas as suas fases, Identificação de Ativos, Identificação Ameaças e Controles, Identificação de Vulnerabilidades, Estimativa de Riscos (Impacto x Probabilidade), gerando assim o Mapa de Riscos dos ativos relacionados.

Durante este período tivemos pandemia, troca de gestores da divisão XXX e mudanças também no próprio processo. Mudanças estas que se fizeram necessárias para buscar melhoria e eficiência neste processo que estava tão detalhado e tão granulado que fez com que o resultado final se prolongasse tanto.


Foram feitas reuniões entre a área de segurança e a coordenadoria da XXXX para alcançarmos uma mudança de abordagem no processo de maneira geral, isto é, mudança nos artefatos e na condução desta atividade juntamente com os consultados indicados pela XXX.

Artefatos, comunicação, entrega e recebimento de informações, reuniões, tudo foi ajustado para chegar ao objetivo final desse primeiro ciclo do processo de gestão de riscos.

Durante o processo, como já dito anteriormente, foram atualizadas algumas informações para buscar manter a atualização do processo em si, para garantir que o retrato final fosse o mais atual possível, mesmo depois de um processo mais longo. Foram retirados ativos descontinuados, e aglutinados ativos que faziam parte de um mesmo contexto para finalizar a análise.

As planilhas dos Mapas de Riscos ficaram mais diretas e mais fáceis de realizar a análise. As vulnerabilidades foram elencadas ou transformadas em vulnerabilidades de níveis estratégicos, menos técnicas.

*Informações foram retiradas e anonimizadas (Ex.: XXXX) por serem classificadas como restritas.

	Universidade Federal do Ceará		Página		8/11	
	Superintendência de Tecnologia da Informação - STI			Classificação		
	Coordenadoria de Infraestrutura e Segurança da Informação - CISI			C	X	R

A obtenção das informações para a geração do Mapa de Riscos que antes era exclusiva via reuniões, passaram a ter a opção do envio do Mapa de Riscos para que o consultado tivesse a opção de preencher com o apoio de manuais com orientações e também de reuniões para o apoio ao preenchimento dos referidos mapas de riscos.

A partir dos Mapas de Riscos, foram gerados os Planos de Tratamento de Riscos (PTR), que visam apoiar o gestor com as informações de ameaças e controles, para que possa definir ações necessárias para minimizar os riscos descritos.

No próximo ciclo, serão utilizados os PTRs para acompanhar as ações que já foram realizadas, verificar se os controles vão atender ao propósito do tratamento esperado do risco. No próximo ciclo também podemos verificar se os mapas de riscos e ativos primários e de suporte precisam ser atualizados. Em suma, vamos atualizar as informações e verificar os controles.

5. Resultado do 1º Ciclo STI-XXX

A criticidade dos riscos foi mensurada de acordo com seus níveis de:

- Confidencialidade (*C*);
- Integridade (*I*) e
- Disponibilidade (*D*).

Considerando a gravidade e a extensão de danos causados à organização, às pessoas ou a outras organizações em consequência a eventuais violações de segurança, e a resiliência de cada divisão quanto aos ativos, foram utilizados os seguintes níveis, cada um com um peso atribuído:


- Muito baixo ($MB = 1$);
- Baixo ($B = 2$);
- Médio ($M = 3$);
- Alto ($A = 4$) e
- Muito alto ($MA = 5$).

Ao classificar os 63 ativos de suporte, obteve-se a distribuição vista na Figura 1. Cada coluna representa a classificação de todos os ativos informados em relação à confidencialidade, integridade e disponibilidade vistos individualmente.

O nível de risco do ativo (R_{ATIVO}) foi obtida em função dos três critérios relacionada com a probabilidade, é calculada através da seguinte fórmula:

$$R_{ATIVO} = \max(C, I, D) \times Probabilidade, \text{ onde } \max \text{ é a função máximo.}$$

*Informações foram retiradas e anonimizadas (Ex.: XXXX) por serem classificadas como restritas.

	Universidade Federal do Ceará		Página		9/11	
	Superintendência de Tecnologia da Informação - STI			Classificação		
	Coordenadoria de Infraestrutura e Segurança da Informação - CISI			C	X	R

Dessa forma, um ativo com baixa criticidade em um dos aspectos e um alto valor em outro não seria avaliado, erroneamente, como um ativo de baixa criticidade. Esse comportamento é normal, por exemplo: podem haver ativos cujo impacto sobre a confidencialidade seja baixo, porém não possa ficar indisponível.

Ao final foram classificados os ativos baseados nos riscos estimados tendo vista a ordenação baseadas naqueles que tiveram mais riscos de níveis Muito Alto, em seguida, Alto, Médio, Baixo e por sua vez Muito Baixo, como podemos ver na Figura 1.

Figura 1 - Resultado - Ativos ordenados baseados em seus riscos

Informação retirada por ser classificada como Restrita


Nesse resultado da Figura 1, podemos verificar que foram analisadas os XX ativos de suporte, e estimados os riscos das ameaças relacionadas a cada ativo de suporte listado.

Ao todo foram analisadas XXX ameaças divididas nesses XX ativos. Vale destacar que não são 392 ameaças diferentes, uma vez que existem ameaças que está presente no Mapa de Riscos de vários Ativos. Este resultado informa que foram analisados este montante de ameaças nos ativos de suporte.

O que podemos retirar desse resultado é a quantidade de Níveis de Riscos, encontrados:

Muito Alto: **XX**
Alto: **XX**
Médio: **XX**
Baixo: **XX**
Muito Baixo: **XX**

*Informações foram retiradas e anonimizadas (Ex.: XXXX) por serem classificadas como restritas.

	Universidade Federal do Ceará	Página	10/11	
	Superintendência de Tecnologia da Informação - STI	Classificação		
	Coordenadoria de Infraestrutura e Segurança da Informação - CISI	C	X	R

Níveis de Risco

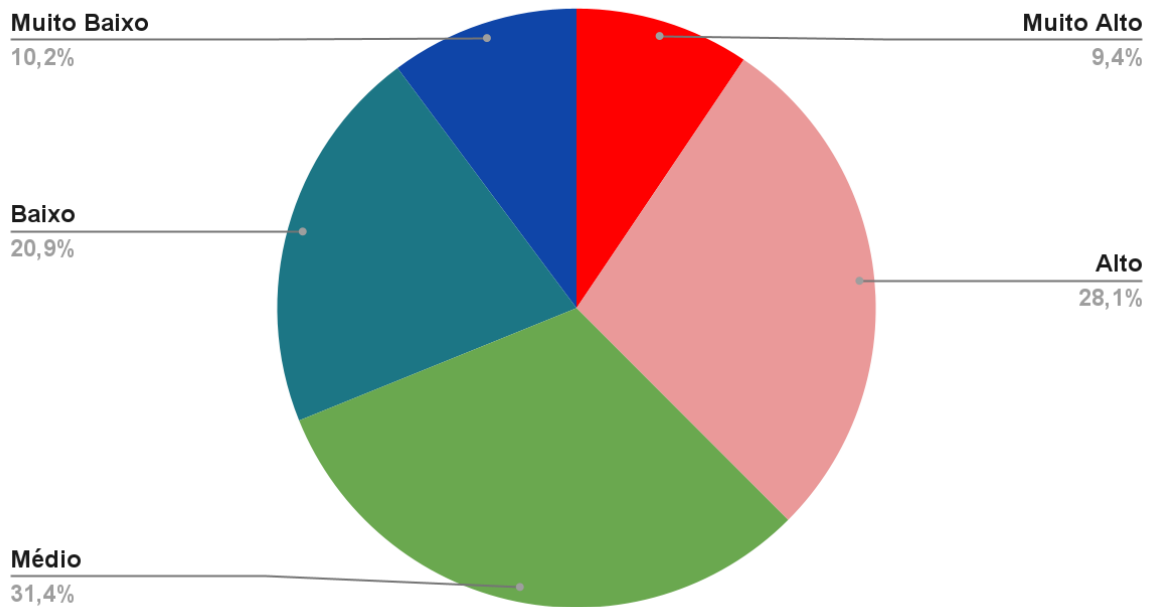



Gráfico 1 - Separados pelos 5 Níveis de Riscos

Gráfico 2 - Separados por níveis de Riscos Mais Altos e os medianos para baixo

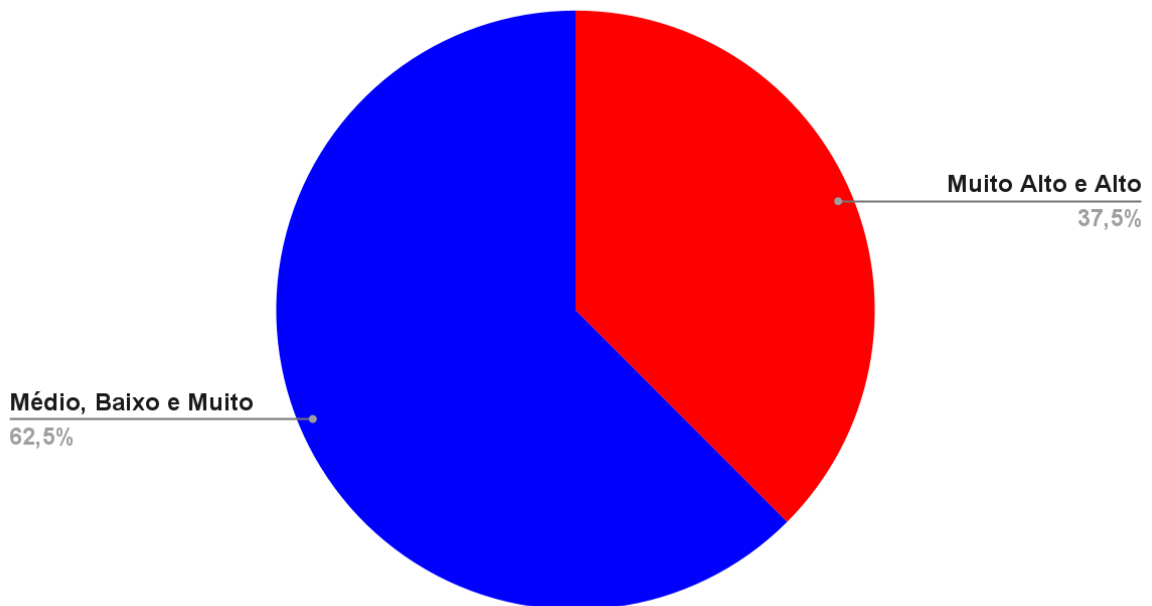
Podemos perceber que os riscos em sua maioria são riscos estimados de Médio, Baixo e Muito Baixo. Os que foram estimados com Riscos mais altos são 37,5% do total de ameaças analisadas.

Outro ponto para se observar do resultado é que os Níveis Muito Alto se concentraram em 16 dos XX ativos, enquanto os de nível Alto, foram encontrados em 45 dos XX ativos. De forma que os de Níveis Muito Alto, foi uma média 2,31 por ativo, enquanto os de nível Alto, foi uma média de 2,44 por ativo. O que significa dizer que, em média, são poucas ameaças de níveis Alto e Muito Alto por ativo.

*Informações foram retiradas e anonimizadas (Ex.: XXXX) por serem classificadas como restritas.

	Universidade Federal do Ceará		Página		11/11	
	Superintendência de Tecnologia da Informação - STI			Classificação		
	Coordenadoria de Infraestrutura e Segurança da Informação - CISI			C	X	R

Níveis de Riscos - Altos x Medianos pra Baixo



6. Considerações finais

Informação retirada por ser classificada como Restrita

*Informações foram retiradas e anonimizadas (Ex.: XXXX) por serem classificadas como restritas.