UNIVERSIDADE FEDERAL DO CEARÁ

PLANO DE MELHORIA EM SEGURANÇA DA INFORMAÇÃO 2022

COORDENADORIA DE INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO

Superintendência de Tecnologia da Informação

Elaboração do Plano de Melhoria em Segurança da Informação

Histórico de Versões

Data	Versão	Descrição	Autor
xx/xx/2022	1.0	Versão inicial do plano	CISI

1. INTRODUÇÃO

1.1. MOTIVAÇÃO

O processo de transformação digital e a constante evolução do ambiente de Tecnologia da Informação e Comunicação (TIC) apresentam novos desafios para a área de Segurança da Informação (SegInfo) e, consequentemente, à Segurança Cibernética (SegCiber). Por outro lado, os órgãos de controle cada vez mais contribuem com a administração pública fornecendo guias e métricas que balizam a evolução da TIC na gestão pública. No caso do Tribunal de Contas da União (TCU), por meio do seu Índice de Governança de Tecnologia da Informação (IGovTI), ele vem auditando as instituições públicas e promovendo melhorias no seu desempenho. Dessa forma, existe a motivação adicional em atender as demandas do IGovTI no que se refere a Segurança da Informação e Segurança Cibernética.

1.2. FINALIDADE

Nortear as ações desta coordenadoria quanto aos controles e medidas de segurança cibernética a serem implementados e acompanhados, tendo em vista a redução dos níveis de riscos aos quais estão submetidos os ativos de TIC da Universidade Federal do Ceará (UFC), bem como o fornecimento de subsídios para composição do Plano Diretor de TIC (PDTIC) institucional .

1.3. OBJETIVOS

- Melhoria dos níveis de segurança cibernética desta universidade frente às evoluções do ambiente de TIC.
- Adequação de conformidade com a legislação vigente relacionada à Segurança da Informação.
- Nortear planejamento de ações necessárias da SegInfo e SegCiber em curto, médio e longo prazo para compor o PDTIC da instituição.

2. GUIAS DE REFERÊNCIAS

2.1. INSTRUÇÃO NORMATIVA GSI/PR Nº 3, DE 28 DE MAIO DE 2021

A Instrução Normativa GSI/PR nº 3, de 28 de Maio de 2021 (IN03), dispõe sobre os processos relacionados à gestão de Segurança da Informação a serem implementados nos órgãos e nas entidades da Administração Pública Federal (APF).

São listados os seguintes processos pela norma:

- Mapeamento de ativos de informação;
- Gestão de Riscos de Segurança da Informação;
- Gestão de Continuidade de Negócios em Segurança da Informação;
- Gestão de mudanças nos aspectos de Segurança da Informação; e
- Avaliação de conformidade de Segurança da Informação.

2.2. CONTROLES CIS V8

O Centro para Segurança da Internet, do inglês *Center for Internet Security® (CIS®)*, lidera a compilação de um conjunto de medidas e boas práticas para a melhoria da Segurana Cibernética de organizações conhecido como Controles CIS (*CIS Controls*). Estes controles são compilados com base no conhecimento e experiência de uma comunidade de especialistas provenientes de diversos setores como empresas, governo e academia.

Atualmente, em sua 8ª versão, são 18 controles, subdivididos em medidas e ações de segurança. Para sua implementação, são sugeridos os chamados Grupos de Implementação de Controles (*Controls Implementation Groups, IGs*). Estes grupos são compostos por um subconjunto de medidas de segurança de cada um dos 18 controles. A implementação das medidas de cada grupo reflete no posicionamento da organização quanto aos níveis de maturidade: IG1, IG2 e IG3.

2.3. QUESTIONÁRIO DE ACOMPANHAMENTO DE SEGURANÇA CIBERNÉTICA DO TCU

O Tribunal de Contas da União (TCU) publicou sua “Estratégia de Fiscalização em Segurança da Informação e Segurança Cibernética 2020-2023” para o acompanhamento e indução de uma boa gestão de Segurança da Informação e Segurança Cibernética no âmbito da APF.

Dentre seus instrumentos, está o questionário de Acompanhamento de Segurança Cibernética. Trata-se de um questionário de autoavaliação de controle interno (*Control Self Assessment, CSA*), disponibilizado aos gestores para obter dados e avaliar a adoção de controles críticos de segurança cibernética.

3. PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NA UFC

O Processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) é fundamental para a identificação e monitoramento de ameaças e para a implementação de controles de segurança em um ambiente computacional.

No ano de 2011, ainda informalmente, foram tomadas ações em direção a este processo na STI. No referido ano, foram catalogados 36 ativos primários (abstraído em serviços) e os seus respectivos 157 ativos de suporte. Sobre os ativos primários, foram levantadas: ameaças; vulnerabilidades; níveis de exposição, impacto e probabilidade; controles existentes; e sugestões de melhoria ou novos controles.

Para o levantamento realizado no período relatado acima, a STI não tinha uma equipe de segurança da informação formalmente instituída. As ações para formação da equipe tiveram seu início no final do ano de 2013, pelo recrutamento de servidores técnicos administrativos por meio de concurso público. Foram selecionados 3 analistas e 2 técnicos de Tecnologia da Informação. A instituição formalização da área da SegInfo na STI foi concretizada em 2016 com a oficialização da Divisão de Segurança da Informação (DSEI).

A DSEI atuou em parceria com as demais divisões da STI na compreensão do ambiente de TIC existente e na realização de ações de SegInfo na unidade. Ao longo do período desde o início do processo de formalização de divisão dedicada à especialidade, foram identificados processos necessários para a melhoria da maturidade organizacional em segurança da informação, dentre eles está o processo de GRSIC. Para a implementação deste processo na STI, foi adotada 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).

Em 2018, o processo foi iniciado formalmente na STI. O escopo do processo foi determinado com base no Escore de Risco (ER) de cada divisão - pontuação obtida como resultado da pré-análise dos ativos primários mapeados em parceria com as divisões participantes. Para esta fase foram considerados como ativos: os serviços; os processos e; as informações que cada divisão considerou como essencial para a realização de suas atividades-fim.

Como resultado foi totalizado a identificação de 133 ativos primários distribuídos nas 7 divisões atuantes da STI. Seguindo o critério de ranqueamento da divisão com maior nível de criticidade dos ativos identificados na pré-análise, a gestão de riscos seguiu uma abordagem vertical[1] na análise dos ativos e, de acordo com os critérios do ranque de criticidade foram selecionados, para tanto, os ativos sob responsabilidade da Divisão de Redes de Computadores (DRC) .

O escopo identificou 26 ativos primários para a divisão selecionada, resultando na análise de 63 ativos de suporte. Ao longo do processo, os níveis de risco de todos os ativos identificados foram mapeados e mensurados. Ao final do ciclo, foram entregues os Planos de Tratamento de Riscos (PTR) contendo sugestões para a implementação de controles de segurança para os ativos de suporte da DRC.

[1] Em uma abordagem vertical, o escopo da avaliação está limitado aos ativos de uma só divisão por ciclo. Consequentemente, neste tipo de abordagem a análise dos ativos de todas as divisões ocorre após várias iterações do processo.

4. METODOLOGIA A SER ABORDADA

Com base nos guias de referências adotados como norteadores do presente plano - apresentados no tópico 2 - consequentemente torna-se fundamental a definição de uma metodologia de aplicação das ações de melhoria a serem executadas. A sequência de atividades resultante desta definição é de suma importância para a determinação de um cronograma que envolva as diversas áreas definidas de acordo com cada fase deste plano. Nas subseções a seguir está o detalhamento da metodologia adotada para aplicação das melhorias na área de SegInfo na UFC . As fases gerais do processo estão ilustradas como na Figura 1 abaixo:

FIGURA 1 - FASES DO PLANO DE MELHORIAS

Fonte: CISI, 2022.

4.1. SELEÇÃO DE CONTROLES

As medidas de segurança apresentadas neste plano tomam como base os Controles CIS v8, especificamente aquelas listadas no Grupo de Implementação de Controles 1 (IG1). Nesse sentido, contemplando a Fase 1 deste Plano de Melhorias, foram priorizadas aquelas relacionadas aos 5 controles abordados no questionário de Acompanhamento de Segurança Cibernética, utilizado pelo Tribunal de Contas da União (TCU) em sua “Estratégia de Fiscalização em Segurança da Informação e Segurança Cibernética 2020-2023”. Os 5 controles estão descritos a seguir:

- 1 - Inventário e controle de ativos corporativos.
- 2 - Inventário e controle de ativos de software.
- 7 - Gestão contínua de vulnerabilidades.
- 14 - Conscientização sobre segurança e treinamento de competências.
- 17 - Gestão de respostas a incidentes.

Diante dos critérios elencados, dentre as 56 medidas de segurança do grupo de implementação IG1, foram selecionadas 20 medidas de segurança listadas com seus respectivos controles no Quadro 1, essas medidas já serão aplicadas para o atendimento da Fase 2 de Diagnóstico Inicial.

QUADRO 1 - CONTROLES E MEDIDAS DE SEGURANÇA

Controle	
	Medida de Segurança
1 - Inventário e controle de ativos corporativos	
	1.1 - Estabelecer e manter um inventário detalhado de ativos corporativos
	1.2 - Endereçar ativos não autorizados
2 - Inventário e controle de ativos de software	
	2.1 - Estabelecer e manter um inventário de software
	2.2 - Assegurar que o software autorizado seja atualmente suportado
	2.3 - Abordar o software não autorizado
7 - Gerenciamento contínuo de vulnerabilidades	
	7.1 - Estabelecer e manter um processo de gerenciamento de vulnerabilidades
	7.2 - Estabelecer e manter um processo de remediação
	7.3 - Executar o gerenciamento automatizado de patches do sistema operacional

	7.4 - Executar o gerenciamento automatizado de patches de aplicações
14 - Conscientização sobre segurança e treinamento de competências	
	14.1 - Estabelecer e manter um programa de conscientização sobre segurança
	14.2 - Treinar membros da força de trabalho para reconhecer ataques de engenharia social
	14.3 - Treinar membros da força de trabalho em práticas recomendadas de autenticação
	14.4 - Treinar a força de trabalho nas melhores práticas de manuseio de dados
	14.5 - Treinar membros da força de trabalho sobre as causas da exposição não intencional de dados
	14.6 - Treinar Membros da força de trabalho no Reconhecimento e Comunicação de Incidentes de Segurança
	14.7 - Treinar a força de trabalho sobre como identificar e comunicar se o seus ativos corporativos estão faltando atualizações de segurança
	14.8 - Treinar a força de trabalho sobre os perigos de se conectar e transmitir dados corporativos em redes inseguras
17 - Gerenciamento de respostas a incidentes	
	17.1 - Designar Pessoal para Gerenciar Tratamento de Incidentes
	17.2 - Estabelecer e manter informações de contato para relatar incidentes de segurança
	17.3 - Estabelecer e manter um processo corporativo para relatar incidentes

Fonte: CISI, 2022.

O detalhamento dos controles e das medidas de segurança podem ser encontrados na documentação dos Controles CIS disponível publicamente em seu sítio oficial disponibilizado na Internet[2].

4.2. DIAGNÓSTICO INICIAL

Uma nova fase de pré-análise será executada sobre os ativos primários da STI, com a finalidade de atualizar o mapeamento de ativos primários desta unidade em relação aos resultados obtidos em 2018. Esta atividade será realizada através da aplicação de entrevistas com os gestores das divisões que compõem a STI.

Ainda durante a pré-análise, a implementação das medidas de segurança listadas na seção anterior será avaliada através de questionários que também serão enviados aos gestores das divisões que compõem a STI.

Serão considerados os resultados das fases ocorridas anteriormente do processo de GRSIC. Estes resultados auxiliarão na seleção dos próximos ativos a serem analisados e no acompanhamento da implementação, ou até na avaliação, dos controles sugeridos ou adotados anteriormente.

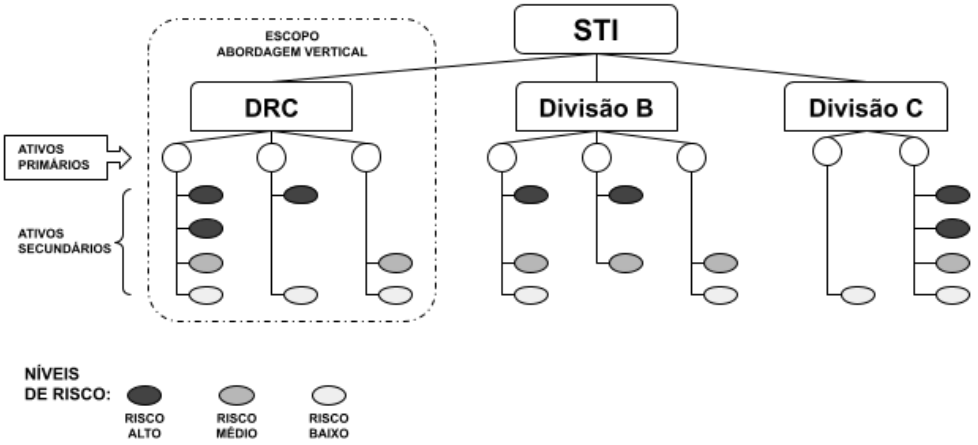
Uma vez concluída a pré-análise, será iniciado um novo ciclo do processo de GRSIC, aplicando melhorias quanto à seleção de ativos de forma mais abrangente em relação às divisões e a observação dos Controles CIS selecionados neste documento. Os detalhes das melhorias estão descritos na seção a seguir.

[2] CIS Critical Security Controls. Disponível em: <https://www.cisecurity.org/controls>. Acesso em: Agosto de 2022.

4.3. ADEQUAÇÃO DA METODOLOGIA DE RISCOS

A abordagem vertical, adotada anteriormente, mostrou-se eficaz, porém ineficiente. Enquanto o processo executava nos ativos da DRC, os demais ativos de outras divisões permaneceram descobertos (não analisados) por um longo período de tempo ao qual durou o ciclo. A Figura 2 exemplifica a seleção do escopo seguindo uma abordagem vertical.

FIGURA 2 - ABORDAGEM VERTICAL

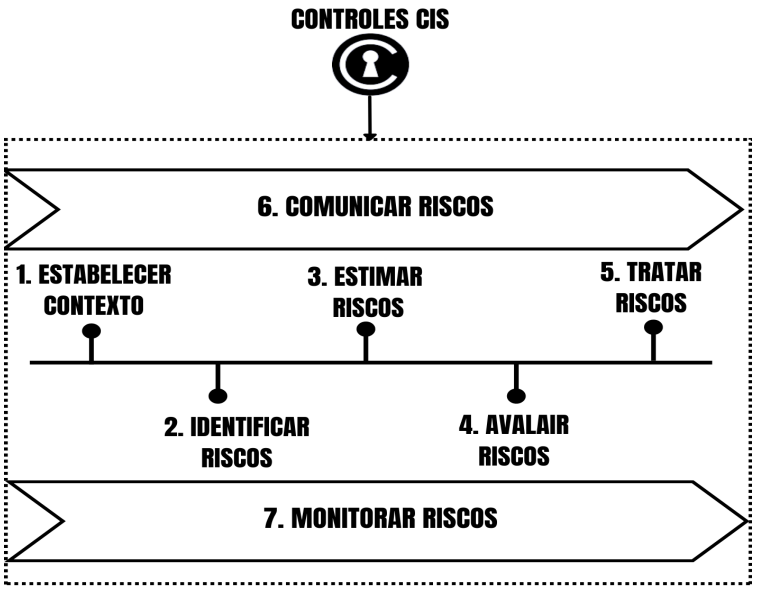


Fonte: CISI, 2022.

Como consequência, ações de segurança sob os demais ativos da STI foram realizadas *ad hoc*, ou seja, demais ações envolvendo a área da SegInfo eram realizadas sob demanda, não seguindo um processo formal e não observando o impacto dos níveis de riscos dos ativos.

A primeira adequação a ser realizada será a integração das medidas de segurança listadas neste plano e pelo Processo de GRSIC estabelecido e, em funcionamento nesta Coordenadoria, visando monitorar os níveis de risco dos ativos analisados e mapear os respectivos controles implementados. A Figura 3 ilustra o fluxo desta integração.

FIGURA 3 - CONTROLES CIS E O PROCESSO DE GRSIC

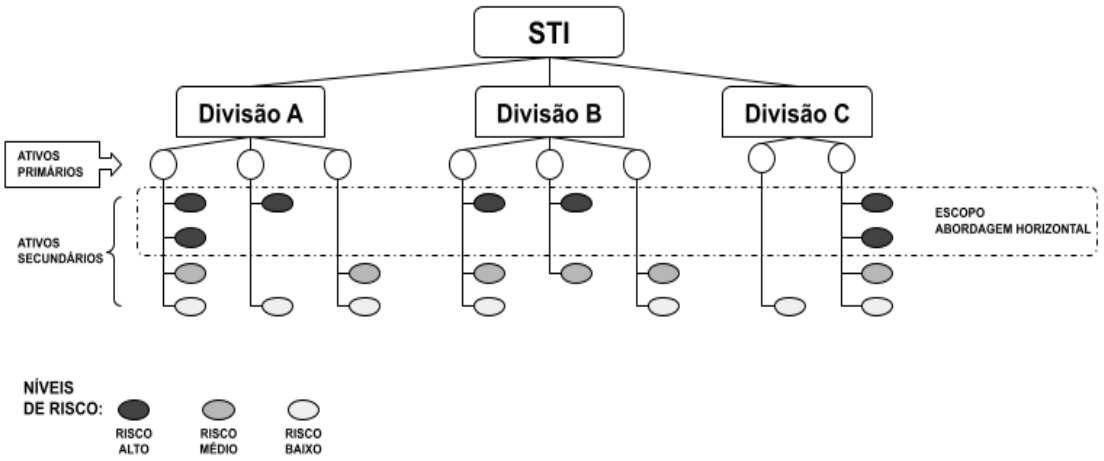


Fonte: CISI, 2022.

Outra ação de melhoria está ligada à delimitação do escopo de cada ciclo do processo. Será adotada uma abordagem horizontal[3] quanto aos ativos a serem analisados, aumentando a abrangência do processo para mais divisões em um mesmo ciclo. Para a seleção dos ativos, será adotado como critério os níveis de risco específicos dos ativos. Para ilustrar esta abordagem a Figura 4 apresenta um cenário onde o escopo é composto pelos ativos com *nível de risco alto*, onde são selecionados os ativos secundários dentre todas as divisões da STI que satisfazem esse critério.

[3] Em uma abordagem horizontal, o escopo da avaliação seleciona ativos nas diversas divisões por ciclo, seguindo um critério de corte. Ou seja, esse critério é observado em várias divisões paralelamente.

FIGURA 4 - EXEMPLO COM ABORDAGEM HORIZONTAL



Fonte: CISI, 2022.

Além de mais abrangente entre as divisões, o escopo de cada ciclo possui uma quantidade menor de ativos secundários a serem analisados em relação ao escopo da abordagem vertical, adotada no passado. Consequentemente, a totalidade dos ativos será atingida ao final da execução de vários ciclos do processo de gestão de risco. A Figura 5 ilustra os ativos sendo selecionados em ciclos diferentes.

FIGURA 5 - SELEÇÃO DE ATIVOS POR CICLO

Fonte: CISI, 2022.

Após a implementação das medidas de segurança listadas neste plano, naturalmente poderá haver a necessidade de realinhamento do plano após o cumprimento da iteração do ciclo. Neste momento, sugere-se optar entre:

- Implementar as medidas de segurança recomendadas nos demais controles do grupo de implementação IG1 não contempladas no Quadro 1 deste plano, ou seja, abranger mais controles para implementar o nível de maturidade;
- Implementar as medidas de segurança recomendadas nos controles do grupo de implementação IG2, considerando apenas os controles já contemplados no Quadro 1, ou seja, avançar no nível de maturidade dos controles já implementados.

5. CRONOGRAMA

O cronograma apresentado na Tabela 1 a seguir busca apresentar as atividades que serão realizadas neste plano, contemplando as etapas da metodologia de melhoria definida. Essas atividades serão monitoradas de acordo com a previsão de entrega de cada uma delas.

TABELA 1 - CRONOGRAMA DE ATIVIDADES

Fases	Atividades	Atores	Artefatos	Prazos
Seleção de Controles	Selecionar controles a serem analisados prioritariamente	CISI	Plano de Melhoria em Segurança da Informação	agosto/2022
Diagnóstico Inicial	Analisar a situação da Segurança em relação aos controles escolhidos	CISI	Questionário da pré-análise	dezembro/2022
Diagnóstico Inicial	Preencher Planilha de Controle	CISI	Questionário da pré-análise	dezembro/2022
Diagnóstico Inicial	Criar Painel PowerBI com transparência da informações	CISI	Publicação do Painel no sítio da STI	dezembro/2022
Adequação da metodologia de riscos de acordo com os	Definir nova abordagem de gestão de riscos	CISI	Apresentação - abordagem horizontal e percentuais de	agosto/2022

controles selecionados			risco	
Adequação da metodologia de riscos de acordo com os controles selecionados	Definir os critérios de seleção de escopo (Corte sobre o percentual de ativos e quais controles na iteração)	CISI	Manual da Gestão de Riscos a ser abordada	dezembro/2022
Adequação da metodologia de riscos de acordo com os controles selecionados	Iniciar o novo ciclo de Gestão de Riscos	CISI/ Áreas envolvidas	Apresentação para os gestores das áreas envolvidas	dezembro/2022

Fonte: CISI, 2022.