MANUAL DE PROCESSO DE TRABALHO 5

IDENTIFICAÇÃO DO PROCESSO

PROCESSO DE TRABALHO DE ANÁLISE DE RISCOS DE SEGURANÇA CIBERNÉTICA		
OBJETIVO	Identificar os riscos de segurança associados a sistemas e serviços de tecnologia da informação do TRE-SE, bem como propor aos proprietários de ativos a adoção de medidas visando trazer os riscos para patamares de segurança considerados aceitáveis. **Observação**: A implementação de ações para responder aos riscos identificados não faz parte do escopo deste processo.	
MANUAL	**NÚMERO**	5
	NOME	RISCOS DE SEGURANÇA CIBERNÉTICA
	VERSÃO	3

VISÃO SISTÊMICA

PROCESSO DE ANÁLISE DE RISCOS DE SEGURANÇA CIBERNÉTICA	
ENTRADA(S)	Vulnerabilidades, necessidades de análises de riscos e incidentes de segurança cibernética
FORNECEDOR(ES)	Unidades solicitantes de avaliações de riscos e proprietários de ativos
SAÍDA(S)	Relatório de Riscos
CLIENTE(S)	Unidades solicitantes de avaliações de riscos

PROCESSO DE ANÁLISE DE RISCOS DE SEGURANÇA CIBERNÉTICA	
REGULAÇÃO	Política de Segurança da Informação da Justiça Eleitoral - Resolução TSE 23.644/21
RECURSO(S)	Sistema Eletrônico de Informações (SEI) Planilhas ou Sistemas

CADEIA DE VALOR

POSIÇÃO DO PROCESSO NA CADEIA DE VALOR	
MACROPROCESSO DE APOIO	Os macroprocessos de apoio garantem o suporte adequado aos processos finalísticos
MACROPROCESSO 13	Gestão de Tecnologia e Segurança Cibernética
PROCESSO 13.4	Gerir Segurança Cibernética
SUBPROCESSO 13.4.2	Análise de riscos de segurança cibernética

GESTOR DO PROCESSO

GESTOR DO PROCESSO	
UNIDADE	A Assessoria Técnica de Segurança Cibernética da STI (ASSEC/STI) é a unidade responsável pela gestão do processo, cabendo-lhe seu acompanhamento, controle e melhoria. Esta unidade também receberá as dúvidas e sugestões acerca do processo para análise e providências necessárias.

TERMOS E DEFINIÇÕES

TERMO	DEFINIÇÃO
ANÁLISE CUSTO-BENEFÍCIO	Refere-se à priorização dos riscos com base na análise dos custos da adoção de controles de segurança versus os benefícios que serão auferidos pelo negócio.
ANÁLISE QUALITATIVA DE RISCOS	Abordagem para análise de riscos na qual os participantes atribuem valores relativos a ativos, riscos, controles e impacto no negócio.
ATIVO	Qualquer coisa que tenha valor para a organização, tal como componentes de hardware e software, dados, pessoas, documentação etc.
CENÁRIO DE INCIDENTE	DESCRIÇÃO de uma ameaça explorando uma certa vulnerabilidade ou um conjunto de vulnerabilidades em um incidente de segurança cibernética.
CONFIDENCIALIDADE	Propriedade de que a informação não será disponibilizada ou divulgada a pessoas, entidades ou processos não autorizados.
CONTROLE DE SEGURANÇA CIBERNÉTICA	Qualquer processo, política, procedimento, diretriz, prática ou estrutura organizacional, de natureza administrativa, técnica, gerencial ou legal, utilizado para modificar o risco de segurança cibernética.
DISPONIBILIDADE	Propriedade de um sistema ou um recurso do sistema que garante que ele estará acessível e utilizável, por um usuário autorizado, quando necessário.
EXPOSIÇÃO	Predisposição de um sistema sofrer a ação de ameaças, devido a fatores ambientais.
IMPACTO (CONSEQUÊNCIA)	Resultado de um evento que afeta objetivos.
INTEGRIDADE	Propriedade de salvaguarda da exatidão e completeza de ativos.
PROBABILIDADE	Chance de algo acontecer, não importando se é de forma definida, medida ou determinada, objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos.

TERMO	DEFINIÇÃO
RISCO	Combinação da probabilidade de ocorrência de um evento e sua consequência.

DOCUMENTO(S) DO PROCESSO

DOCUMENTO	NOME	ONDE É ENCONTRADO OU UNIDADE RESPONSÁVEL
D1	Solicitação de Análise de Riscos	SEI
D2	Planilha de Gerenciamento de Riscos Guia Definição de Escopo Guia Achados e Observações Guia Perfil dos Ativos Guia Controles de Segurança Guia Cenários de Incidentes	ASSEC/STI
D3	Modelos de Critérios para Análise dos Riscos	ASSEC/STI
D4	Relatório de Riscos	ASSSEC/STI

Observação: A critério do gestor do processo e participantes, a Planilha de Gerenciamento de Riscos pode ser substituída por outra ferramenta que melhor atenda os requisitos de registro das fases do processo, considerando os recursos tecnológicos disponíveis.

TRATAMENTO DE RISCOS

<table>
<tr><th colspan="2">EVENTO DE RISCO</th><th>AÇÃO</th><th>ATIVIDADE LIGADA AO RISCO</th></tr>
<tr><td colspan="2">1. Ataques cibernéticos direcionados à infraestrutura crítica</td><td>Identificação e classificação dos ativos críticos, testes de intrusão e auditorias periódicas, reduzindo a probabilidade e o impacto de ataques cibernéticos avançados, exploração de vulnerabilidades críticas, comprometimento de redes internas e serviços essenciais.</td><td rowspan="3">2. Levantamento de informações</td></tr>
<tr><td>Nível de Risco:
Alto</td><td>Resposta:
Mitigar</td><td rowspan="2">Unidade/Servidor responsável:
COINF / Titular da Unidade</td></tr>
<tr><td colspan="2">Controle:
Melhorar controle existente</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="2">2. Sobrecarga da equipe responsável</td><td>Ajuste de carga de trabalho, redistribuição, novos concursos/contratos.</td><td rowspan="3">2. Levantamento de informações</td></tr>
<tr><td>Nível de Risco:
Alto</td><td>Resposta:
Mitigar</td><td rowspan="2">Unidade/Servidor responsável:
STI / Titular da Unidade</td></tr>
<tr><td colspan="2">Controle:
Melhorar controle existente</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="2">EVENTO DE RISCO</th><th>AÇÃO</th><th>ATIVIDADE LIGADA AO RISCO</th></tr>
<tr><td colspan="2">3. Falhas de comunicação entre unidades</td><td>Garantir que todas as unidades do órgão público envolvidas nos processos de segurança da informação — áreas técnicas, administrativas e de gestão — mantenham comunicação eficiente, tempestiva e padronizada, evitando desencontros de informação que possam comprometer a identificação e mitigação de riscos de segurança cibernética.</td><td rowspan="3">2. Levantamento de informações</td></tr>
<tr><td>Nível de Risco:
Moderado</td><td>Resposta:
Mitigar</td><td rowspan="2">Unidade/Servidor responsável:
DG / Titular da Unidade</td></tr>
<tr><td colspan="2">Controle:
Melhorar controle existente</td></tr>
</table>

MATRIZ RACI

Definição e distribuição de papéis e responsabilidades que integram o processo Análise de Riscos de Segurança Cibernética.
R – **Responsável**: quem deve executar a atividade;
A – **Autoridade**: quem deve responder pela atividade;
C – **Consultado**: quem deve ou pode ser consultado durante a execução da atividade;
I – **Informado**: quem deve receber a informação de que uma atividade foi executada.

ATIVIDADE	Solicitante	ASSEC	ETIR
1. SOLICITAÇÃO DE ANÁLISE DE RISCOS E DEFINIÇÃO DE ESCOPO			
1.1 SOLICITAR análise de riscos	R/A	-	-
1.2 AVALIAR a viabilidade da análise	C/I	R/A	C
1.3 ESTABELECER escopo	C	R/A	C
1.4 ENCERRAR processo - análise inviável	R/A	-	-
2. LEVANTAMENTO DE INFORMAÇÕES			
2.1 ELABORAR artefatos	C	R/A	C
2.2 COLETAR informações	C	R/A	C
2.3 FORNECER informações	C	-	R/A
2.4 CONSOLIDAR informações	-	R/A	-
3. DEFINIR CRITÉRIOS DE AVALIAÇÃO			
3.1 PREPARAR catálogos	-	R/A	C
3.2 ELABORAR matriz de cenários	-	R/A	C
3.3 DEFINIR escala de impacto	-	R/A	C
3.4 DEFINIR critérios para probabilidades	-	R/A	C
3.5 FIXAR critérios de avaliação	-	R/A	C
3.6 VALIDAR critérios de avaliação	C	I	R/A
3.7 CONFIGURAR Planilha de Riscos	-	R/A	-
4. ANÁLISE E AVALIAÇÃO DE RISCOS			
4.1 PROGRAMAR reunião para análise	C	R/A	C
4.2 IDENTIFICAR elementos dos cenários	C	R/A	C
4.3 DEFINIR medidas de segurança	C	R/A	C
4.4 DEFINIR tratamento de riscos	C	R/A	C
4.5 IDENTIFICAR risco residual	C	R/A	C
4.6 ELABORAR relatório	-	R/A	C

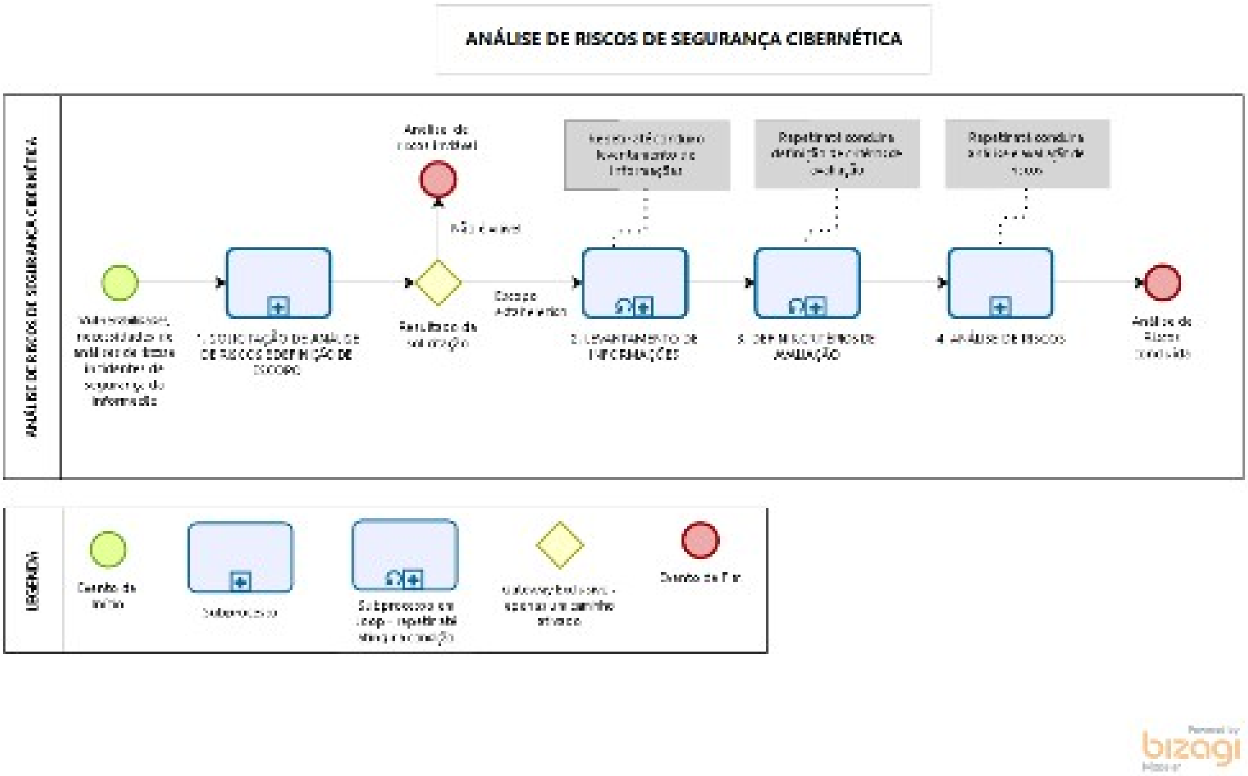
ATIVIDADE	Solicitante	ASSEC	ETIR
4.7 ANALISAR relatório	R/A	C	-

AUTORES DO MANUAL

MANUAL ELABORADO POR	
UNIDADES	STI/ASSEC - Secretaria de Tecnologia da Informação/Assessoria Técnica de Segurança Cibernética
	SEORG - Seção de Otimização de Processos Organizacionais

SOBRE A VERSÃO

VERSÃO	RESUMO DAS ALTERAÇÕES	RESPONSÁVEL
1	Versão inicial.	Autores do Manual
2	Revisão do mapeamento do processo e alteração do manual para o novo modelo padrão elaborado pela SEORG.	SEORG
3	Revisão do mapeamento do processo e alteração do manual para adequá-lo à nova estrutura e normativos relacionados à segurança cibernética no TRE-SE.	ASSEC/SEORG


ANÁLISE DE RISCOS DE SEGURANÇA CIBERNÉTICA
4. ANÁLISE DE RISCOS

1. SOLICITAÇÃO DE ANÁLISE DE RISCOS E DEFINIÇÃO DE ESCOPO

DESCRIÇÃO

Subprocesso

2. LEVANTAMENTO DE INFORMAÇÕES

DESCRIÇÃO

A Assessoria Técnica de Segurança Cibernética (ASSEC) deve coletar informações relacionadas aos ativos sob análise para subsidiar a tomada de decisões, de sorte que o êxito da análise de riscos está intimamente relacionado à qualidade dos dados obtidos.
As atividades deste subprocesso devem ser repetidas até que a ASSEC considere o levantamento de dados satisfatório.

3. DEFINIÇÃO DE CRITÉRIOS DE AVALIAÇÃO

DESCRIÇÃO

Será adotada a análise qualitativa de riscos, que utilizará escalas com atributos qualificadores para descrever o impacto no negócio decorrente da concretização de um cenário de incidente, a probabilidade de ocorrência desses incidentes, bem como o grau de risco para todos os cenários considerados relevantes.
As atividades deste subprocesso deverão ser repetidas até que a Assessoria Técnica de Segurança Cibernética considere os critérios estabelecidos satisfatórios.
As escalas sugeridas devem ser adaptadas ou ajustadas para se adequarem às circunstâncias.
Para calcular o grau de risco, relacionado a cada cenário de incidente, será utilizada a seguinte fórmula:

RISCO = IMPACTO X PROBABILIDADE

A variável "Impacto" será estimada a partir de uma escala de valores, conforme exibido no Documento 2.

Para cálculo da "Probabilidade" de uma ameaça explorar uma vulnerabilidade ou um conjunto de vulnerabilidades será utilizada a seguinte fórmula:

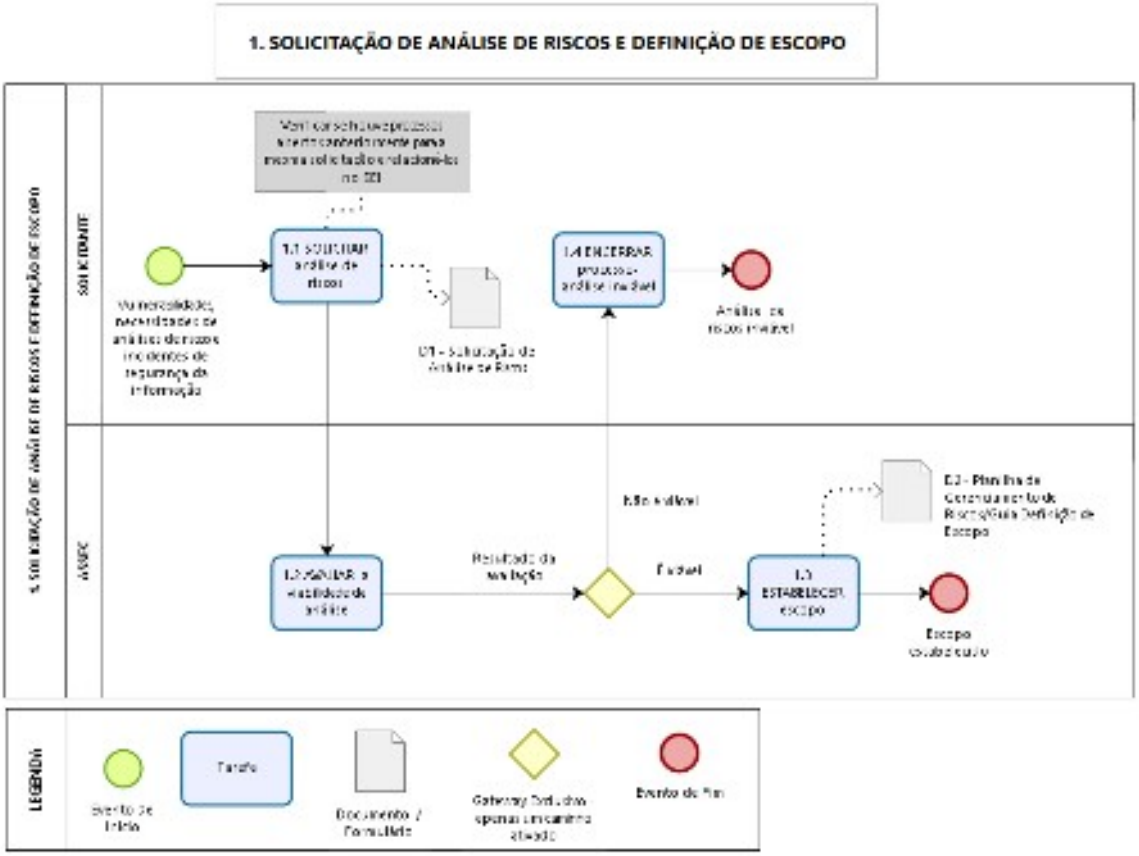
PROBABILIDADE = ((EXPOSIÇÃO + FREQUÊNCIA)/2) X (ÍNDICE DE INVERSÃO))

As variáveis de “Exposição” e “Frequência”, bem como o “Índice de Inversão” também serão estimados a partir de escalas customizadas de valores (vide Documento 2).

4. ANÁLISE DE RISCOS

DESCRIÇÃO

Subprocesso


1. SOLICITAÇÃO DE ANÁLISE DE RISCOS E DEFINIÇÃO DE ESCOPO
SOLICITANTE
GESEC
Não viável
Viável
LEGENDA

1. SOLICITAÇÃO DE ANÁLISE DE RISCOS E DEFINIÇÃO DE ESCOPO

1.1 SOLICITAR análise de riscos

DESCRIÇÃO

- Preencher o Formulário Solicitação de Análise de Riscos, disponível no Sistema Eletrônico de Informações (SEI), e tramitá-lo para o Assessoria Técnica de Segurança Cibernética (ASSEC).
- Verificar se houve processo aberto anteriormente para a mesma solicitação e relacioná-los no SEI.
- Manter o processo aberto até se chegar a um dos seguintes resultados: indeferimento, adiamento ou emissão de Relatório de Riscos.

EXECUTANTE

Solicitante

D1 - Solicitação de Análise de Riscos

DESCRIÇÃO

D1- Formulário de Solicitação de Análise de Riscos
Onde é encontrado ou unidade responsável: SEI

1.2 AVALIAR a viabilidade da análise

DESCRIÇÃO

- Avaliar a oportunidade e conveniência da realização da análise de riscos, considerando a disponibilidade de recursos humanos, a estimativa de tempo necessária para execução das atividades, dentre outros fatores.
- O indeferimento ou adiamento do pedido deve ser fundamentado.

EXECUTANTE

Assessoria Técnica de Segurança Cibernética (ASSEC)

1.3 ESTABELECER escopo

DESCRIÇÃO

- Definir o escopo da avaliação de riscos, ou seja, quais ativos deverão ter seus riscos avaliados.

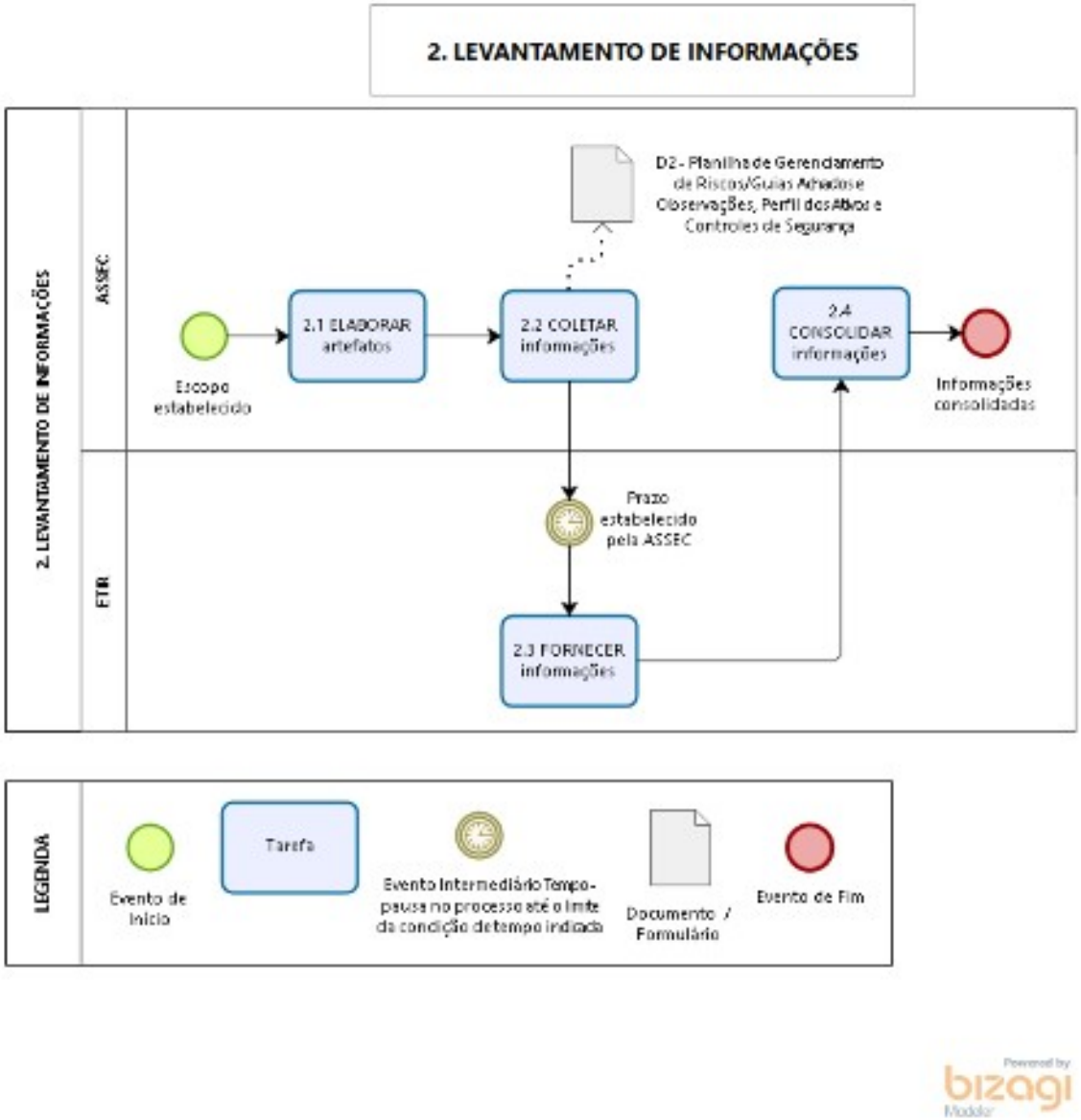
- Preencher a Guia Definição de Escopo da Planilha de Gerenciamento de Riscos, em conjunto com o Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

EXECUTANTE
Assessoria Técnica de Segurança Cibernética (ASSEC)

D2 - Planilha de Gerenciamento de Riscos/Guia Definição de Escopo
DESCRIÇÃO
D2 - Planilha de Gerenciamento de Riscos/Guia Definição de Escopo
Planilha de Gerenciamento de Riscos
Guia Definição de Escopo
Guia Achados e Observações
Guia Perfil dos Ativos
Guia Controles de Segurança
Guia Cenários de Incidentes
Onde é encontrado ou unidade responsável: ASSEC/STI

1.4 ENCERRAR processo-análise inviável
DESCRIÇÃO
Encerrar o processo no SEI.

EXECUTANTE
Solicitante


2. LEVANTAMENTO DE INFORMAÇÕES
2. LEVANTAMENTO DE INFORMAÇÕES
ASSEC
D2 - Planilha de Gerenciamento de Riscos/Guias Adotados e Observações, Perfil dos Ativos e Controles de Segurança
Escopo estabelecido
2.1 ELABORAR artefatos
2.2 COLETAR informações
2.4 CONSOLIDAR informações
Informações consolidadas
FTIR
Prazo estabelecido pela ASSEC
2.3 FORNECER informações
LEGENDA
Evento de Início
Tarefa
Evento Intermediário Tempo - pausa no processo até o limite da condição de tempo indicada
Documento / Formulário
Evento de Fim

2. LEVANTAMENTO DE INFORMAÇÕES

DESCRIÇÃO

A Assessoria Técnica de Segurança Cibernética (ASSEC) deve coletar informações relacionadas aos ativos sob análise para subsidiar a tomada de decisões, de sorte que o êxito da análise de riscos está intimamente relacionado à qualidade dos dados obtidos.
As atividades deste subprocesso devem ser repetidas até que a ASSEC considere o levantamento de dados satisfatório.

☐ 2.1 ELABORAR artefatos

DESCRIÇÃO

- Elaborar uma lista de documentos para fins de identificação de achados e observações relacionados aos ativos sob análise.
- Os documentos serão requisitados à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).
- Exemplos de informações que podem ser solicitadas:
Análises de risco executadas anteriormente;
Relatórios de auditorias realizadas internamente ou por órgãos de controle, sobretudo o Tribunal de Contas da União (TCU) e o Conselho Nacional de Justiça (CNJ);
Questionários de avaliação de governança aplicados pelo TCU e CNJ;
Testes de penetração realizados;
Análises de vulnerabilidades realizadas;
Políticas de segurança e procedimentos relacionados aos ativos sob análise;
Planos de recuperação de desastre;
Análises de Impacto no Negócio (AIN);
Guias de hardening ou checklists de configuração utilizados etc.

- Adicionalmente, podem ser elaborados questionários de coleta de dados que serão utilizados em entrevistas com o Grupo de Especialistas.
- Uma fonte valiosa de consulta são as Review Questions (questões de inspeção), disponíveis na seção Catálogos de Ameaças, do IT-Grundschutz Catalogues (GSK).
- Exemplos de perguntas que podem ser feitas aos Proprietários de Ativos:
Qual a importância do ativo de informação para o negócio?
Quais são os processos de negócio suportados pelo serviço/sistema sob análise?;
No tocante à segurança cibernética, qual a classificação das informações (confidencialidade, integridade e disponibilidade) armazenadas, processadas ou transmitidas pelo serviço/sistema?

Existem leis ou regulamentos estabelecendo requisitos de confidencialidade, integridade e disponibilidade do sistema/serviço?
As informações armazenadas, processadas ou transmitidas pelo serviço/sistema estão sendo protegidas de acordo com a classificação de segurança a elas atribuída?
Já ocorreram incidentes de segurança (perda de informações, acesso indevido, indisponibilidades etc.)?
Quem são os usuários do sistema/serviço e qual seu nível de privilégio?
Como é realizado o controle de acesso ao sistema/serviço?
Qual o tempo tolerável de indisponibilidade do sistema/serviço e quais as consequências para o negócio?
Na ocorrência de indisponibilidade do sistema/serviço, existem procedimentos alternativos (documentados e de conhecimento de toda a equipe) que permitam a continuidade dos trabalhos?
É possível identificar alguma fraqueza (vulnerabilidade) nos procedimentos ou no próprio sistema/serviço em questão?
Qual evento ou entidade (ameaça) tem potencial para prejudicar o sistema/serviço?

- Exemplos de perguntas que podem ser feitas aos Responsáveis Técnicos:
Os Responsáveis Técnicos têm conhecimento da classificação de segurança (realizada pelos Proprietários da Informação) atribuída às informações armazenadas, processadas ou transmitidas pelo serviço/sistema?
As informações armazenadas, processadas ou transmitidas pelo serviço/sistema estão sendo protegidas de acordo com a classificação de segurança correspondente?
Qual é a arquitetura (componentes e seus relacionamentos com outros sistemas, formas de armazenamento, processamento e transmissão de dados etc.) do sistema/serviço?
Quais os componentes de hardware e software envolvidos (servidores, switches, firewalls, sistemas operacionais, sistema gerenciador de banco de dados etc.)?
Quais ameaças têm potencial para prejudicar o sistema/serviço?
É possível identificar vulnerabilidades nos procedimentos ou no próprio sistema/serviço em questão?
Já ocorreram incidentes de segurança (perda de informações, acesso indevido, indisponibilidades, etc.)?
Quais controles de segurança cibernética (processo, política, procedimento, diretriz, prática ou estrutura organizacional, que modificam o risco) estão implementados atualmente e qual sua efetividade?

Observação: A lista de documentos solicitados e o conteúdo dos questionários de levantamento de dados variam em função dos ativos envolvidos na análise de riscos.

EXECUTANTE
Assessoria Técnica de Segurança Cibernética (ASSEC)

2.2 COLETAR informações

DESCRIÇÃO
- Solicitar à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) os documentos identificados na atividade anterior ou realizar entrevistas/oficinas para coleta de informações.
- Estabelecer prazo para o envio em conjunto com a Equipe de Prevenção, Tratamaneto e Resposta a Incidentes Cibernéticos (ETIR).
- Preencher as Guias Achados e Observações, Perfil dos Ativos e Controles de Segurança da Planilha de Gerenciamento de Riscos.

EXECUTANTE
Assessoria Técnica de Segurança Cibernética (ASSEC)

D2 - Planilha de Gerenciamento de Riscos/Guias Achados e Observações, Perfil dos Ativos e Controles de Segurança

DESCRIÇÃO
D2 - Planilha de Gerenciamento de Riscos/Guia Definição de Escopo
Planilha de Gerenciamento de Riscos
Guia Definição de Escopo
Guia Achados e Observações
Guia Perfil dos Ativos
Guia Controles de Segurança
Guia Cenários de Incidentes
Onde é encontrado ou unidade responsável: ASSEC/STI

2.3 FORNECER informações

DESCRIÇÃO
Fornecer as informações solicitadas, preferencialmente, em formato eletrônico (no caso de documentos), de acordo com o prazo estabelecido em conjunto com o ASSEC.

EXECUTANTE
Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)

☐2.4 CONSOLIDAR informações

DESCRIÇÃO

- Extrair as informações mais relevantes do material coletado (documentos ou respostas aos questionários) para auxiliar na tomada de decisão nas etapas posteriores.
- Exemplos de informações que podem ser extraídas dos documentos:

Análises de risco executadas anteriormente

Observações derivadas da análise de riscos, sobretudo aquelas relacionadas aos cenários de incidentes identificados e às recomendações dos especialistas;

Planos de ação ou recomendações derivadas da análise de riscos.

Relatórios de auditorias realizadas internamente ou por órgãos de controle, sobretudo o Tribunal de Contas da União (TCU) e o Conselho Nacional de Justiça (CNJ)

Observações derivadas da auditoria, principalmente aquelas relacionadas a segurança, operação de computadores, controle de acesso, controle de mudanças e recuperação de desastres;

Respostas dos gestores aos achados que foram identificados pelos auditores.

Questionários de avaliação de governança aplicados pelo TCU e CNJ

Lacunas (gaps) ou deficiências em relação às boas práticas de segurança cibernética, notadamente aquelas relacionadas aos ativos sob análise.

Políticas de segurança e procedimentos relacionados aos ativos sob análise

Lacunas (gaps) ou deficiências em relação às políticas e procedimentos em vigor no Tribunal.

Questionário de levantamento de informações elaborado pela ASSEC

Agentes, ameaças, vulnerabilidades e controles de segurança existentes;

Classificação das informações;

Nível de exposição dos ativos;

Alinhamento, no tocante à proteção dos ativos, entre as áreas técnica e de negócios;

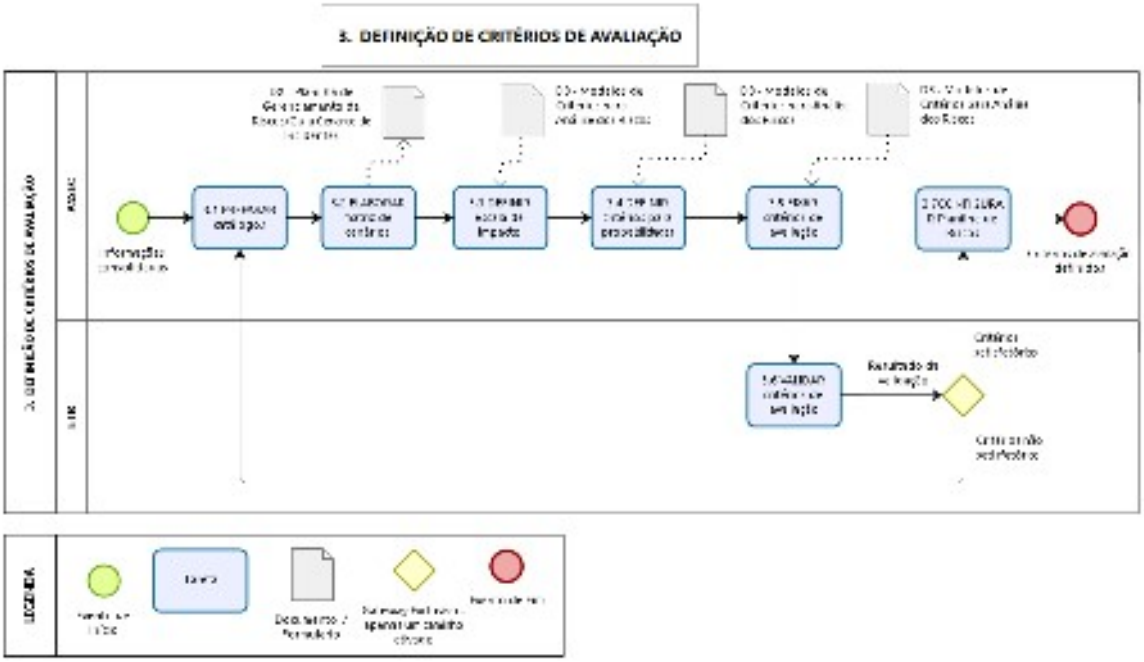
Incidentes de segurança e a frequência em que ocorrem;

Nível de efetividade dos mecanismos de controle empregados;

Grau de impacto no negócio decorrente de um incidente de segurança.

EXECUTANTE

Assessoria Técnica de Segurança Cibernética (ASSEC)


3. DEFINIÇÃO DE CRITÉRIOS DE AVALIAÇÃO
ASSIC
SIM
LEGENDA

3. DEFINIÇÃO DE CRITÉRIOS DE AVALIAÇÃO

DESCRIÇÃO

- Será adotada a análise qualitativa de riscos, que utilizará escalas com atributos qualificadores para descrever o impacto no negócio decorrente da concretização de um cenário de incidente, a probabilidade de ocorrência desses incidentes, bem como o grau de risco para todos os cenários considerados relevantes.
- As atividades deste subprocesso deverão ser repetidas até que a Assessoria Técnica de Segurança Cibernética (ASSEC) e a Equipe de Prevenção, Tratamaneto e Resposta a Incidentes Cibernéticos (ETIR) considerem os critérios estabelecidos satisfatórios.
- As escalas sugeridas devem ser adaptadas ou ajustadas para se adequarem às circunstâncias.
- Para calcular o grau de risco, relacionado a cada cenário de incidente, será utilizada a seguinte fórmula:

RISCO = IMPACTO X PROBABILIDADE

- A variável "Impacto" será estimada a partir de uma escala de valores, conforme exibido no Documento D3 - Modelos de Critérios para Análise dos Riscos.
- Para cálculo da "Probabilidade" de uma ameaça explorar uma vulnerabilidade ou um conjunto de vulnerabilidades será utilizada a seguinte fórmula:

PROBABILIDADE = ((EXPOSIÇÃO + FREQUÊNCIA)/2) X (ÍNDICE DE INVERSÃO))

- As variáveis de "Exposição" e "Frequência", bem como o "Índice de Inversão" também serão estimados a partir de escalas customizadas de valores (vide Documento D3 - Modelos de Critérios para Análise dos Riscos).

☐ 3.1 PREPARAR catálogos

DESCRIÇÃO

- Preparar catálogos das ameaças e vulnerabilidades que sejam aplicáveis ao objeto sob análise.
- Utilizar como referência a experiência dos avaliadores, os anexos da norma NBR ISO/IEC 27005/2023 e os catálogos constantes do IT-Grundschutz Catalogues (GSK).

EXECUTANTE

Assessoria Técnica de Segurança Cibernética (ASSEC)

3.2 ELABORAR matriz de cenários

DESCRIÇÃO

- Elaborar uma matriz que relacione as ameaças identificadas com as vulnerabilidades (hipotéticas ou reais) que podem ser exploradas (cenário de incidentes).
- Registrar o produto da atividade na Guia Cenários de Incidentes da Planilha de Gerenciamento de Riscos.

EXECUTANTE

Assessoria Técnica de Segurança Cibernética (ASSEC)

D2 - Planilha de Gerenciamento de Riscos/Guia Cenários de Incidentes

DESCRIÇÃO

D2 - Planilha de Gerenciamento de Riscos/Guia Definição de Escopo
Planilha de Gerenciamento de Riscos
Guia Definição de Escopo
Guia Achados e Observações
Guia Perfil dos Ativos
Guia Controles de Segurança
Guia Cenários de Incidentes
Onde é encontrado ou unidade responsável: ASSEC/STI

3.3 DEFINIR escala de impacto

DESCRIÇÃO

- Definir os critérios que serão adotados para estimar o impacto no negócio decorrente de um incidente de segurança.
- Entre os fatores que podem ser utilizados para estimar o impacto de um incidente podemos citar:

O valor financeiro de reposição do ativo perdido (ou parte dele);
O custo de aquisição, configuração e instalação do novo ativo;
Violação de leis e normas;
Dano à imagem do TRE-SE;
Número de usuários afetados etc.

- Um modelo de escala de impacto pode ser visto no Documento D3 - Modelos de Critérios para Análise dos Riscos.

EXECUTANTE

Assessoria Técnica de Segurança Cibernética (ASSEC)

D3 - Modelos de Critérios para Análise dos Riscos

DESCRIÇÃO

D3 - Modelos de Critérios para Análise dos Riscos
Onde é encontrado ou unidade responsável: ASSEC/STI

3.4 DEFINIR critérios para probabilidades

DESCRIÇÃO

Os elementos necessários para se calcular a probabilidade de uma ameaça explorar as vulnerabilidades de um ativo são os seguintes:

Nível de efetividade dos **controles** de segurança em uso

Controles de segurança são mecanismos (procedimentos, técnicas, ferramentas, políticas, práticas, estruturas organizacionais etc.) utilizados para modificar os riscos, fornecendo os seguintes tipos de proteção: correção, eliminação, prevenção, minimização do impacto, dissuasão, detecção, recuperação, monitoramento e conscientização.
No entanto, o grau de efetividade dos controles pode variar significativamente, de forma que controles ineficientes (não testados periodicamente, sujeitos a falhas, ultrapassados etc.) podem aumentar a probabilidade de uma ameaça explorar uma vulnerabilidade. Controles efetivos, por outro lado, diminuem a probabilidade de incidentes de segurança.
Em suma, há uma relação inversa entre a efetividade do controle e a probabilidade de uma ameaça explorar uma vulnerabilidade.
Deste modo, é necessário definir o grau de efetividade dos controles de segurança adotados, utilizando como base o modelo de escala disponível no Documento D3 - Modelos de Critérios para Análise dos Riscos.

Grau de **exposição** do ativo

Quanto mais exposto a fatores ambientais um ativo estiver, maior a probabilidade de uma ameaça explorar uma vulnerabilidade ou um grupo de vulnerabilidades.
Exemplos de fatores que podem afetar o valor de exposição de um ativo estão relacionados a seguir:
Acessibilidade do ativo: disponível na Internet, remotamente via VPN ou acessível apenas na rede local. Um sistema de informação acessível via Internet, por exemplo, está mais exposto a tentativas de invasão por hackers do que outro acessível apenas na rede local do TRE-SE;

Localização: se um equipamento servidor estiver localizado dentro de um Datacenter, por exemplo, ele estará menos exposto do que outro instalado sobre uma mesa de escritório;
Fluxo dos dados: se as informações são transferidas para outras entidades ou apenas dentro do Tribunal;
Número de usuários: normalmente, quanto maior o número de usuários, mais exposto encontra-se o ativo a ameaças relacionadas à confidencialidade, integridade e disponibilidade;
Perfil de usuários: sistemas com uma grande quantidade de usuários externos estão mais expostos a ameaças relacionadas à confidencialidade, integridade e disponibilidade do que sistemas acessíveis apenas a usuários internos;
Ocorrência de incidentes: a ocorrência de incidentes de segurança anteriores ou eventos de segurança relacionados a uma ameaça em particular, podem ser indicativo de um problema sistêmico. Tal fato pode aumentar a probabilidade ocorrência de eventos semelhantes no futuro.
Um modelo de determinação do grau de exposição dos ativos pode ser visto no Documento D3 - Modelos de Critérios para Análise dos Riscos.

Frequência de ocorrência de eventos de segurança

Frequência é o valor que designamos para medir com que regularidade um evento de segurança ocorre (a cada cinco anos, anualmente, diariamente etc.).
Incidentes de segurança frequentes contribuem para concretização de um cenário de incidentes.
Assim como nos demais modelos de escala utilizados neste processo, há necessidade de customização dos valores pela ASSEC (vide Documento D3 - Modelos de Critérios para Análise dos Riscos).

EXECUTANTE
Assessoria Técnica de Segurança Cibernética da STI (ASSEC/STI)

D3 - Modelos de Critérios para Análise dos Riscos
DESCRIÇÃO
D3 - Modelos de Critérios para Análise dos Riscos
Onde é encontrado ou unidade responsável: ASSEC/STI

3.5 FIXAR critérios de avaliação

DESCRIÇÃO

- Definir os critérios para tratamento e aceitação dos riscos, considerando-se os seguintes aspectos:
Definição dos valores associados a cada nível de risco;
Definição da postura que será adotada em relação a cada nível de risco.

- Modelo contendo os critérios para tratamento e aceitação de riscos pode ser visto no Documento D3 - Modelos de Critérios para Análise dos Riscos.

EXECUTANTE

Assessoria Técnica de Segurança Cibernética da STI (ASSEC/STI)

D3 - Modelos de Critérios para Análise dos Riscos

DESCRIÇÃO

D3 - Modelos de Critérios para Análise dos Riscos
Onde é encontrado ou unidade responsável: ASSEC/STI

3.6 VALIDAR critérios de avaliação

DESCRIÇÃO

- Validar os critérios estabelecidos pela ASSEC.
- Caso a definição dos critérios não tenha sido considerada satisfatória, executar novamente o subprocesso (ou apenas as atividades consideradas deficientes).

EXECUTANTE

Equipe de Prevenção, Tratamaneto e Resposta a Incidentes Cibernéticos (ETIR)

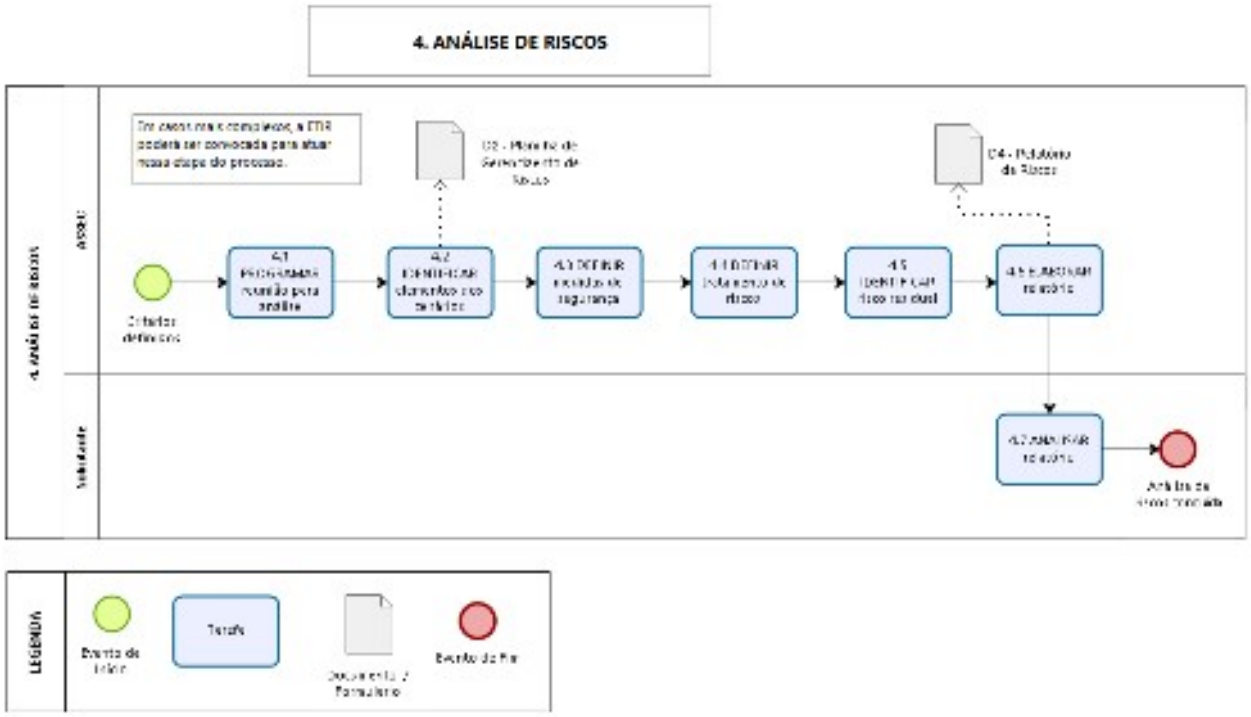
3.7 CONFIGURAR Planilha de Riscos

DESCRIÇÃO

Adequar a Planilha de Gerenciamento de Riscos aos critérios de análise e avaliação de riscos estabelecidos.

EXECUTANTE

Assessoria Técnica de Segurança Cibernética da STI (ASSEC/STI)


4. ANÁLISE DE RISCOS
ETIR
Solicitante
4.1
4.2
4.3 OBTER
4.4 OBTER
4.5
4.6 ELABORAR
4.7 ANALISAR
LEGENDA
Tarefa

4. ANÁLISE DE RISCOS

DESCRIÇÃO

A Assessoria Técnica de Segurança Cibernética da STI (ASSEC/STI) fará a análise e avaliação dos riscos relacionados a cada cenário de incidentes. Caso julgue necessário, fará reunião com a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

☐ 4.1 PROGRAMAR reunião para análise

DESCRIÇÃO

- Sugere-se que a reunião dure, no máximo, 1h30 (uma hora e trinta minutos) e que seja conduzida por um facilitador (membro da ASSEC) com conhecimento no processo de gerenciamento de riscos e no objeto avaliado (sistema, serviço etc.).
- Propõe-se a adoção da seguinte agenda:

Apresentações e breve explanação sobre o gerenciamento de riscos: 5 min;
Papéis e responsabilidades dos envolvidos: 5 min;
Análise e avaliação dos riscos: 1h20 (uma hora e vinte minutos).

- Caso o tempo da reunião não tenha sido suficiente para execução dos trabalhos, ou ainda, se os resultados obtidos não forem considerados satisfatórios, novas sessões de análise e avaliação de riscos devem ser programadas.

EXECUTANTE

Assessoria Técnica de Segurança Cibernética da STI (ASSEC/STI)

☐ 4.2 IDENTIFICAR elementos dos cenários

DESCRIÇÃO

- Identificar os seguintes elementos para cada um dos cenários de incidentes:

Impacto no negócio;
O grau de exposição do ativo;
A frequência de ocorrência de eventos de segurança;
O nível de efetividade dos controles de segurança em uso.

- Lançar as informações coletadas na Planilha de Gerenciamento de Riscos que efetuará o cálculo do "Nível de Riscos" automaticamente.

Observação: A Planilha de Gerenciamento de Riscos contém, neste momento, as informações coletadas nas fases anteriores do processo.

EXECUTANTE
Assessoria Técnica de Segurança Cibernética da STI (ASSEC/STI)

D2 - Planilha de Gerenciaento de Riscos
DESCRIÇÃO
D2 - Planilha de Gerenciamento de Riscos/Guia Definição de Escopo
Planilha de Gerenciamento de Riscos
Guia Definição de Escopo
Guia Achados e Observações
Guia Perfil dos Ativos
Guia Controles de Segurança
Guia Cenários de Incidentes
Onde é encontrado ou unidade responsável: ASSEC/STI

4.3 DEFINIR medidas de segurança
DESCRIÇÃO
Discutir sobre as possíveis medidas de segurança a serem adotadas, os custos envolvidos, o trabalho necessário e o grau de dificuldade de implementação.

EXECUTANTE
Assessoria Técnica de Segurança Cibernética da STI (ASSEC/STI)

4.4 DEFINIR tratamento de riscos
DESCRIÇÃO
- O Tratamento de riscos é a fase do processo de Gestão de Riscos de Segurança Cibernética onde a organização decide e implementa ações para modificar os riscos inaceitáveis para que se tornem aceitáveis.
- Após a avaliação de riscos (que classifica os riscos como Baixo, Médio, Alto ou Crítico), a organização deve focar nos riscos classificados acima do seu nível de aceitação (ou "apetite de risco") e escolher uma das quatro estratégias de tratamento, baseadas nas diretrizes da ISO/IEC 27005:

Mitigar: implementar controles, tratar o risco para reduzir sua probabilidade e/ou seu impacto nos objetivos;
Evitar: não se expor a uma situação de risco (atentar-se para o fato de que a consequência desta medida pode ser a não exploração de oportunidades associadas ao risco);

Transferir: transferir ou compartilhar o risco com terceiros. Isto pode ser feito através de seguros ou contratualmente, por meio de cláusulas específicas e garantias;
Aceitar: o proprietário do ativo pode escolher pela aceitação do risco (sempre de forma consciente), caso não seja possível evitar o risco, tratá-lo ou transferi-lo. O custo de tomar uma ação, por exemplo, pode ser desproporcional ao benefício potencial gerado.

Observação: A implementação de ações para responder aos riscos identificados não faz parte do escopo deste processo.

EXECUTANTE
Assessoria Técnica de Segurança Cibernética da STI (ASSEC/STI)

4.5 IDENTIFICAR risco residual

DESCRIÇÃO
- O Risco residual é o resultado da reavaliação do risco, considerando a eficácia dos controles já implementados. Trata-se do nível de risco que a alta administração do Tribunal decide aceitar (apetite ao risco).
- O ponto de partida para a identificação do risco residual é o chamado risco inerente (risco sem qualquer controle).
- Identificado o risco inerente, a organização define e implementa controles de segurança (técnicos, administrativos e físicos).
- O risco residual deve ser documentado, incluindo sua probabilidade e impacto, para garantir que as decisões de aceitação sejam informadas e que o risco seja compreendido pelos proprietários do negócio.
- O tratamento do risco residual também deverá seguir as estratégias de tratamento baseadas nas diretrizes da ISO/IEC 27005, já descritas na tarefa 4.4.

EXECUTANTE
Assessoria Técnica de Segurança Cibernética da STI (ASSEC/STI)

4.6 ELABORAR relatório

DESCRIÇÃO
- Elaborar Relatório de Riscos apresentando respostas aos riscos, visando trazê-los para patamares aceitáveis, de forma que os gestores e os proprietários dos ativos possam decidir seguramente a respeito.
- Do Relatório de Riscos devem constar os seguintes elementos (quando aplicável):

Introdução
Objetivo
Escopo
Metodologia adotada
Participantes
Técnicas utilizadas
Modelo de Risco
DESCRIÇÃO do sistema/serviço
Componentes tecnológicos
Localização física
Dados utilizados pelo sistema
Usuários
Diagrama do sistema
Achados e recomendações
Principais vulnerabilidades
Principais ameaças
Resultados da análise de risco
Recomendações de controles de segurança

- As diretrizes para a elaboração do Relatório de Riscos são informadas pela ASSEC/STI.

EXECUTANTE
Assessoria Técnica de Segurança Cibernética da STI (ASSEC/STI)

 **D4 - Relatório de Riscos**
DESCRIÇÃO
D4 - Relatório de Riscos
Onde é encontrado ou unidade responsável: ASSEC/STI

 **4.7 ANALISAR relatório**
DESCRIÇÃO
- Analisar o relatório de riscos e decidir acerca das medidas que entender cabíveis. Após essa tarefa, caberá ao solicitante concluir o processo no SEI.

EXECUTANTE
Solicitante