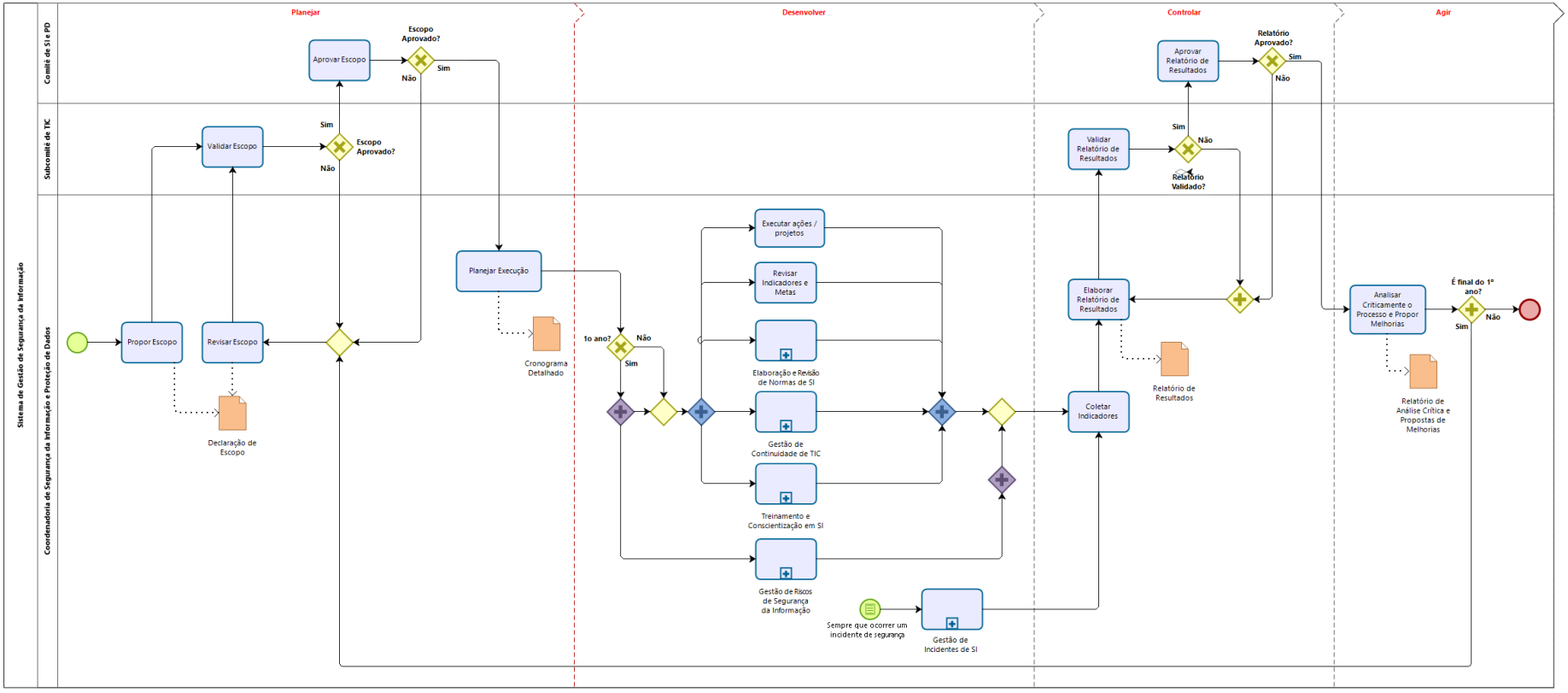
PROCESSO SGSI:
SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

DESENHO DO PROCESSO
DEFINIÇÕES
DESCRIÇÃO DAS TAREFAS

Versão set.2025

DESENHO DO PROCESSO



PROCESSO DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

CONTROLE DE VERSÕES

Versão e data	Alterações
set.2025	Versão de controle inicial

DEFINIÇÕES

Objetivo do Processo
Organizar e planejar as atividades com o objetivo de proteger as informações da organização contra ameaças, garantindo sua confidencialidade, integridade e disponibilidade, por meio de políticas, controles e práticas contínuas de gestão de riscos.

Responsável pelo Processo
Coordenadoria de Segurança da Informação e Proteção de Dados

Papéis e responsabilidades	
Coordenadoria de Segurança da Informação e Proteção de Dados (CSIPD)	Responsável pela gestão do processo e acompanhamento da execução das atividades relacionadas ao SGSI.
Subcomitê de TIC	Subcomitê responsável pela aprovação em primeiro nível de alguns documentos gerados no processo.
Comitê de Segurança da Informação e Proteção de Dados	Responsável pela avaliação das proposições e documentos produzidos no processo.

Termos/Artefatos	
	São exemplos de produtos do SGSI: ● Política de Segurança da Informação (PSI); ● Protocolos de Segurança Cibernética; ● Processos de Segurança da Informação;

	● Planos de Continuidade de Negócio (PCNs): ○ Planos de Continuidade Operacional (PCOs); ○ Planos de Recuperação de Desastres (PRDs); ● Relatórios de Incidentes de Segurança da Informação (RISIs); ● Relatório de Gestão de Riscos de Segurança da Informação; ● Plano de Tratamento de Riscos de Segurança da Informação; ● Treinamentos de Conscientização em Segurança da Informação; ● Análises de aderência com: ○ ABNT NBR ISO/IEC 27002:2022 ○ Guia de Infraestrutura Crítica - CNJ ● Definição e medição de indicadores de Segurança da Informação.

Ferramentas	
Suíte SA - Módulo de Risk Manager	Sistema utilizado para o registro e monitoramento da Gestão de Riscos
PROAD	Sistema de processo administrativo eletrônico.

Referências técnicas, legais e normativas que fundamentam o Processo	
Resolução CNJ 396/2021	Instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)
Norma ABNT NBR ISO/IEC 27001:2022	estabelece os requisitos para um Sistema de Gestão da Segurança da Informação
Norma ABNT NBR ISO/IEC 27002:2022	Fornece um conjunto de referências de controles de segurança da informação.

Indicador de benefício do processo		
Descrição do indicador	**Método de apuração / fórmula de cálculo**	**Frequência**
Conformidade com a ABNT NBR 27002	(Controles da ISO 27002 aplicados) / (Controles ISO 27002 aplicáveis)	Anual
Aderência ao Guia de Proteção de Infraestrutura Crítica - CNJ	Percentual de controles do CIS Controls 7.1 implementados	Anual

Controle de execução do processo		
Controle	**Método de execução**	**Frequência**
Auditoria	Realizar uma reunião com as equipes executoras do processo, para avaliar a aderência, os benefícios gerados e oportunidades de melhoria do processo. Essa reunião deve identificar se o processo necessita de revisão.	Anual

Propor Escopo		
Descrição	O processo do SGSI representa a gestão do Macroprocesso de Gestão de Segurança da Informação, englobando todas as atividades realizadas pela Coordenadoria de Segurança da Informação e Proteção de Dados. Dessa forma, a proposição do escopo compreende a definição das atividades a serem realizadas bem como os objetivos a serem alcançados na execução do SGSI para o biênio que se segue.	
Considerações importantes	Embora o processo seja dimensionado para execução bianual, há determinadas atividades que são executadas anualmente ou até mesmo pontualmente. Portanto, o escopo deve definir quais são tais atividades, os objetivos e resultados esperados. No segundo ano do biênio, há uma atividade cujo objetivo é a revisão do escopo, permitindo eventuais ajustes.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Entradas	PDTIC, SGSI anterior, fontes diversas.	
Saídas	Declaração de Escopo	
Atividades	**Definir o Escopo**	Com base em diferentes entradas, definir o escopo e seus limites para a execução do SGSI, que abrange não somente avaliação de riscos bianual, mas também as demais atividades relacionadas à Coordenadoria de Segurança da Informação e Proteção de Dados.
	Formalizar a Proposição do Escopo	Redigir a proposta de escopo para o biênio que se segue.
	Encaminhar ao Subcomitê de TIC	Compete à Coordenadoria de Segurança da Informação e Proteção de Dados remeter o documento de “Declaração de Escopo” para validação do Subcomitê de TIC, a quem caberá solicitar ajustes ou, após avaliação, encaminhar para consideração superior.
Templates	Declaração de Escopo	

Validar Escopo	
Descrição	Compreende a validação da proposta de Declaração de Escopo e eventual devolução da proposta para ajustes ou encaminhamento para consideração superior.
Considerações	A validação poderá ocorrer em reunião presencial, via e-mail ou via sistema e

importantes	posteriormente documentada em PROAD criado para tal fim.	
Papéis	Subcomitê de TIC	
Entradas	Declaração de Escopo	
Saídas	Declaração de Escopo Validada / Proposta de ajustes na Declaração de Escopo	
Atividades	**Validar "Declaração de Escopo"**	Realizar validação da proposta, verificando se há necessidade de ajustes ou correções.
	Solicitar Ajustes	Devolver à Coordenadoria de Segurança da Informação e Proteção de Dados com proposições de alteração e ajustes.
	Encaminhar para aprovação superior	Após validada a Declaração de Escopo, encaminhar ao Comitê de Segurança da Informação e Proteção de Dados para aprovação quando se tratar de proposta de escopo (1º ano do ciclo) ou quando for uma revisão de escopo (2º ano do ciclo), com vistas a aprovar alterações no escopo original do SGSI.
Templates	N/A	

Aprovar Escopo		
Descrição	Consiste na apreciação para aprovação ou reprovação da proposta de escopo recebida.	
Considerações importantes	Realiza a análise com o objetivo de aprovação ou reprovação da proposta de escopo do SGSI recebida, podendo solicitar eventuais ajustes também. A apreciação poderá ocorrer em reunião presencial ou via e-mail e posteriormente documentada em PROAD criado para tal fim.	
Papéis	Comitê de Segurança da Informação e Proteção de Dados	
Entradas	Declaração de Escopo	
Saídas	Declaração de Escopo Aprovada ou Rejeitada	
Atividades	**Análise da Proposta de Escopo**	Realizar análise crítica da proposta de escopo apresentada, contendo o detalhamento das atividades vinculadas ao SGSI para o biênio que se inicia, ou para a revisão do escopo, realizada no segundo ano do ciclo.
	Aprovação da Proposta de Escopo	Sinalizar à Coordenadoria de Segurança da Informação e Proteção de Dados a aprovação da Declaração de Escopo.
	Reprovação da	Caso o Comitê de Segurança da Informação e Proteção de

	Proposta de Escopo	Dados não aprove integralmente ou parcialmente a proposta de escopo, ele poderá encaminhar a avaliação indicando eventuais pontos a serem alterados, para adequação da proposta de escopo.
Templates	N/A	

Revisar Escopo		
Descrição	Compreende a revisão do escopo.	
Considerações importantes	Essa revisão poderá ocorrer em dois momentos: durante a proposta do escopo, para ajustes indicados pelos colegiados, ou no início do segundo ano do ciclo, quando se propõe a revisão integral do escopo e sua adequação a eventuais mudanças que possam ter ocorrido ao longo do primeiro ano, mantendo a Gestão de Segurança da Informação atualizada. Caso tais mudanças resultem em necessidade de alterações na Gestão de Riscos, que estará em andamento, é importante analisar o impacto que elas poderão representar na análise de riscos desenvolvida, e avaliar se a melhor estratégia é a mudança do escopo do SGSI ou a realização de uma Gestão de Riscos extraordinária e externa ao escopo inicialmente proposto para SGSI.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Entradas	Declaração de Escopo Vigente, PETIC, SGSI anterior, fontes diversas	
Saídas	Declaração de Escopo (revisada)	
Atividades	**Revisar o Escopo**	Se devolvida para revisão durante aprovação da proposta de escopo, adequar de acordo com as indicações propostas. No caso da revisão periódica proposta para o início do segundo ano, com base em diferentes entradas, revisar o escopo inicialmente definido e seus limites para a execução do SGSI, que abrange não somente a avaliação de riscos bianual, mas também as demais atividades relacionadas à Coordenadoria de Segurança da Informação e Proteção de Dados.
	Formalizar Revisão do Escopo	Gerar versão revisada da Declaração de Escopo do SGSI, indicando as alterações, se efetuadas.
	Encaminhar ao Subcomitê de TIC	Compete à Coordenadoria de Segurança da Informação e Proteção de Dados remeter a revisão da “Declaração de Escopo” para validação do Subcomitê de TIC, na existência

		de alterações. Mesmo que não haja alterações, a revisão do escopo será encaminhada ao Subcomitê de TIC para validação.
Templates	Declaração de Escopo (revisada)	

Planejar Execução		
Descrição	Compreende a organização da execução do SGSI, elaboração de cronograma, formalização de projetos, identificação de todos os PROADs que poderão ser impactados, bem como o que cada um conduzirá. Por fim, iniciar a execução do SGSI.	
Considerações importantes	O cronograma do SGSI deve abranger, de modo macro, os cronogramas dos subprocessos que serão executados durante o ciclo, detalhando a dependência entre as atividades. A formalização contempla a criação dos projetos necessários, tanto para o SGSI, como para subprocessos que os exijam. Subprocessos que se repetem ao longo do SGSI, pois ocorrem anualmente, devem ter cronogramas para ambas as execuções previstas. Quando a atividade ocorrer ao longo do segundo ano do ciclo, caberão apenas ajustes, pois o SGSI já contará com cronogramas, projetos formalizados e etc.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Entradas	Declaração de Escopo Aprovada	
Saídas	Cronograma detalhado, Mapeamento dos PROADs impactados, etc	
Atividades	**Elaborar/Ajustar Cronograma**	Elaborar/Ajustar cronograma detalhado do SGSI e suas etapas, bem como cronograma macro, com as fases dos subprojetos que serão executados durante o ciclo do SGSI.
	Identificar PROADs Impactados	Gerar/Atualizar documento contendo detalhadamente todos os PROADs envolvidos no SGSI, ou seus subprocessos, apontando a finalidade e o que deverá ser registrado em cada um.
	Iniciar a execução do SGSI	Disparar o início da execução do cronograma planejado, ou, quando já em andamento (2º ano do ciclo), dar sequência ao andamento das atividades, seguindo a revisão realizada.
Templates	N/A	

Executar ações / projetos

Descrição	Realizar as ações/projetos, propostos durante o ciclo bianual do SGSI, e que não se enquadram nos fluxos de processos definidos.	
Considerações importantes	Essas ações e projetos contemplarão atividades pontuais, tais como aquisições e contratações de serviços, software ou soluções, análise de riscos específicas, dentre outras.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Entradas	Cronograma e planejamento SGSI	
Saídas	Resultados dos projetos/ações	
Atividades	**Executar ações/projetos**	Executar ações e projetos que poderão ser propostos no escopo do SGSI ou que eventualmente venham a surgir durante o biênio e que não se enquadram nos processos de SI executados anualmente.
Templates	N/A	

Revisar Indicadores e Metas		
Descrição	Realizar estudo revisando os indicadores de Segurança da Informação, analisando a necessidade de criação, exclusão ou alteração. Executar, também, a revisão das metas estabelecidas para os indicadores.	
Considerações importantes	Todas as modificações propostas devem ser validadas pelo Subcomitê de TIC.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados, Subcomitê de TIC	
Entradas	Metas e indicadores estabelecidos no ciclo anterior	
Saídas	Metas e indicadores revisados	
Atividades	**Analisar Indicadores Atuais**	Verificar se os indicadores existentes estão adequados, medindo o desempenho dos processos de forma correta ou se é necessária sua adequação, criação de novos indicadores ou exclusão de indicadores existentes.
	Revisar Metas Estabelecidas	Revisar as metas estabelecidas para os indicadores e, caso necessário, alterá-las.
	Propor Modificações dos Indicadores e das Metas	Formalizar a revisão e as alterações, caso existentes, para posterior validação pelo Subcomitê de TIC.

Templates	N/A

Executar Processo: Elaboração e Revisão de Normas de SI	
Descrição	Subprocesso “Elaboração e Revisão de Normas de SI”
Considerações importantes	Conforme estabelecido na Política de Segurança da Informação e nos Protocolos de Segurança Cibernética, a documentação deve ser revisada pelo menos uma vez ao ano ou quando houver alterações significativas no ambiente tecnológico.
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados, Comitê de Governança de TIC, Comitê de Segurança da Informação e Proteção de Dados, Presidência e Outras áreas da SGTI.
Entradas	N/A
Saídas	N/A
Atividades	Conforme descrito no processo
Templates	N/A

Executar Processo: Gestão de Continuidade de TIC	
Descrição	Subprocesso “Gestão de Continuidade de TIC”
Considerações importantes	Conforme estabelecido na Política de Segurança da Informação, os Planos de Continuidade de Negócio devem ser revisados pelo menos uma vez ao ano ou quando houver alterações significativas no ambiente tecnológico.
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados, Subcomitê de TIC, Comitê de Segurança da Informação e Proteção de Dados, Presidência e Outras áreas da SGTI.
Entradas	N/A
Saídas	N/A
Atividades	Conforme descrito no processo
Templates	N/A

Executar Processo: Treinamento e Conscientização em SI	
Descrição	Subprocesso “Treinamento e Conscientização em SI”.

Considerações importantes	O processo deve ser executado anualmente, uma vez que há indicador com coleta anual acerca da quantidade de usuários treinados anualmente.
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados, Comitê de Segurança da Informação e Proteção de Dados e Outras áreas do TRT4
Entradas	N/A
Saídas	N/A
Atividades	Conforme descrito no processo.
Templates	N/A

Executar Processo: Gestão de Riscos de Segurança da Informação	
Descrição	Subprocesso “Gestão de Riscos de Segurança da Informação”
Considerações importantes	Este subprocesso é executado ao longo do biênio do SGSI ao qual está vinculado. Isso possibilita a realização de uma análise de riscos mais elaborada e criteriosa, aproveitando o prazo maior para a execução das atividades. O escopo de tal análise de riscos é definido na proposição de escopo do ciclo do SGSI. No entanto, cabe frisar que outras análises de riscos pontuais, com escopos específicos, também poderão ser executadas dentro do biênio, seguindo o fluxo estabelecido neste subprocesso.
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados, Comitê de Segurança da Informação e Proteção de Dados, Presidência, Subcomitê de TIC e Outras áreas da SGTI.
Entradas	N/A
Saídas	N/A
Atividades	Conforme descrito no processo.
Templates	N/A

Executar Processo: Gestão de Incidentes de SI	
Descrição	Subprocesso “Gestão de Incidentes de SI”
Considerações importantes	Este subprocesso é executado sob demanda quando ocorrem incidentes de SI.
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados, ETIR, Comitê de

	Segurança da Informação e Proteção de Dados, Presidência, Subcomitê de TIC e Outras áreas da SGTI
Entradas	N/A
Saídas	N/A
Atividades	Conforme descrito no processo.
Templates	N/A

Coletar Indicadores		
Descrição	Realizar coleta dos indicadores de SI.	
Considerações importantes	Há indicadores que devem ser coletados anualmente ou mensalmente. No entanto, o indicador referente à Gestão de Riscos de SI é bianual, devendo ser coletado apenas no final do ciclo (segundo ano do biênio).	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Entradas	Resultado dos processos de SI	
Saídas	Levantamento de indicadores	
Atividades	**Declaração de Aplicabilidade**	Realizar análise de aplicabilidade dos controles propostos da ABNT NBR 27002:2022.
	Aderência ao Guia de Proteção de Infraestrutura Crítica	Realizar análise de Aderência ao Guia de Proteção de Infraestrutura Crítica - CNJ
	Coletar Indicadores	Realizar a coleta dos indicadores anuais.
	Publicar Indicadores	Realizar a publicação dos indicadores coletados.
Template	Planilha de indicadores	

Elaborar Relatório de Resultados	
Descrição	Elaborar relatório contendo resultado do SGSI.
Considerações importantes	O relatório trará, quando executado ao final do primeiro ano, os resultados das ações realizadas até o momento. Quando executado ao final do SGSI (segundo ano), contemplará todas as ações executadas ao longo do ciclo completo do SGSI.
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados

Entradas	Atividades executadas durante os ciclos	
Saídas	Relatório de Resultados	
Atividades	**Elaborar Relatório**	Confeccionar o relatório.
	Encaminhar para Validação e Aprovação	Encaminhar para aprovação em instâncias superiores
Templates	Relatório da implementação do Sistema de Gestão de Segurança da Informação (sem a parte de análise crítica) e relatórios produzidos pelos subprocessos, se existirem.	

Validar Relatório de Resultados		
Descrição	Validar o Relatório de Resultados elaborado pela CSIPD.	
Considerações importantes	N/A	
Papéis	Subcomitê de TIC	
Entradas	Relatório de Resultados	
Saídas	Validação do Relatório	
Atividades	**Validar Relatório**	Verificar e validar o relatório elaborado pela Coordenadoria de Segurança da Informação e Proteção de Dados.
	Encaminhar para Aprovação Superior	Encaminhar o relatório validado ao Comitê de Segurança da Informação e Proteção de Dados para aprovação.
	Devolver para ajustes	Devolver à Coordenadoria de Segurança da Informação e Proteção de Dados o para eventuais ajustes.
Templates	N/A	

Aprovar Relatório de Resultados	
Descrição	Apreciar e aprovar ou apontar eventuais questões no relatório elaborado.
Considerações importantes	O Comitê de Segurança da Informação e Proteção de Dados analisará os resultados obtidos até o presente momento, podendo eventualmente solicitar maiores informações, correções, ajustes, etc.
Papéis	Comitê de Segurança da Informação e Proteção de Dados
Entradas	Relatório de resultados validado pelo Subcomitê de TIC
Saídas	Aprovação do Relatório

Atividades	**Aprovar Relatório**	Realizar aprovação ou reprovação do relatório
	Encaminhar para prosseguimento	Encaminhar para a Coordenadoria de Segurança da Informação e Proteção de Dados para ajustes (em caso de rejeição) ou para dar prosseguimento no SGSI em caso de aprovação.
Templates	N/A	

Analisar Criticamente o Processo e Propor Melhorias		
Descrição	Realizar análise crítica do SGSI executado.	
Considerações importantes	Verificar pontos de sucesso e pontos que necessitam ajustes para o próximo ciclo, elaborar relação de melhorias para implementar na próxima execução com base no processo do SGSI e nos demais processos aplicados durante o período. Quando a análise ocorrer no meio do ciclo (ao final do primeiro ano) acrescenta-se o estudo de oportunidades que possam ser aplicadas imediatamente, já no segundo ano do ciclo do SGSI. Ao final do ciclo, avalia-se a análise crítica do primeiro ano do ciclo e atualiza o documento, complementando com as informações geradas no segundo ano do ciclo.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Entradas	Relatório de Resultados do SGSI	
Saídas	Análise Crítica e proposta de Melhorias	
Atividades	**Elencar pontos de sucesso e pontos de atenção**	Elencar pontos que foram sucesso durante a execução do SGSI, até o momento, e pontos que indicam necessidade de melhoria.
	Analisar outros processos e SGSIs anteriores	Analisar a saída de outros processos de SI executados verificando a possibilidade de ajustes no SGSI; analisar os SGSI anteriores de forma a verificar se há possibilidade de melhorias a serem implantadas na segunda parte do SGSI, ou em um próximo ciclo de execução.
	Redigir Documento	Elaborar relatório com melhorias a serem implantadas no próximo ciclo do SGSI.
Templates	Relatório da Implementação do Sistema de Gestão de Segurança da Informação (com análise crítica)	