Macroprocesso de Segurança da Informação e Proteção de Dados

TRT-14ª REGIÃO
Rondônia e Acre

JOENIR JOSE DELLA FLORA
18/06/2024 13:47

WAINNER BRUM CAETANO
20/06/2024 08:08

SETIC - Secretaria de Tecnologia da Informação e Comunicação

Gestor do Processo: Chefe da Divisão de Segurança da Informação
Área responsável: Divisão de Segurança da Informação

OBJETIVO

Este Macroprocesso descreve as atividades e procedimentos adotados para a gestão da Segurança da Informação no Tribunal Regional da 14ª Região.

DEFINIÇÕES GERAIS PARA A ADEQUADA EXECUÇÃO DESTE PROCESSO

Este MOP é compreendido por um Macroprocesso de Segurança da Informação e Proteção de Dados, o qual define procedimentos e atividades relacionadas à execução de ações e subprocessos relacionados à Segurança da Informação.

Através de sua execução, poderão ser realizados os procedimentos necessários para a elaboração, revisão, execução e acompanhamento de artefatos relacionados à área de Segurança da Informação e seus subprocessos associados.

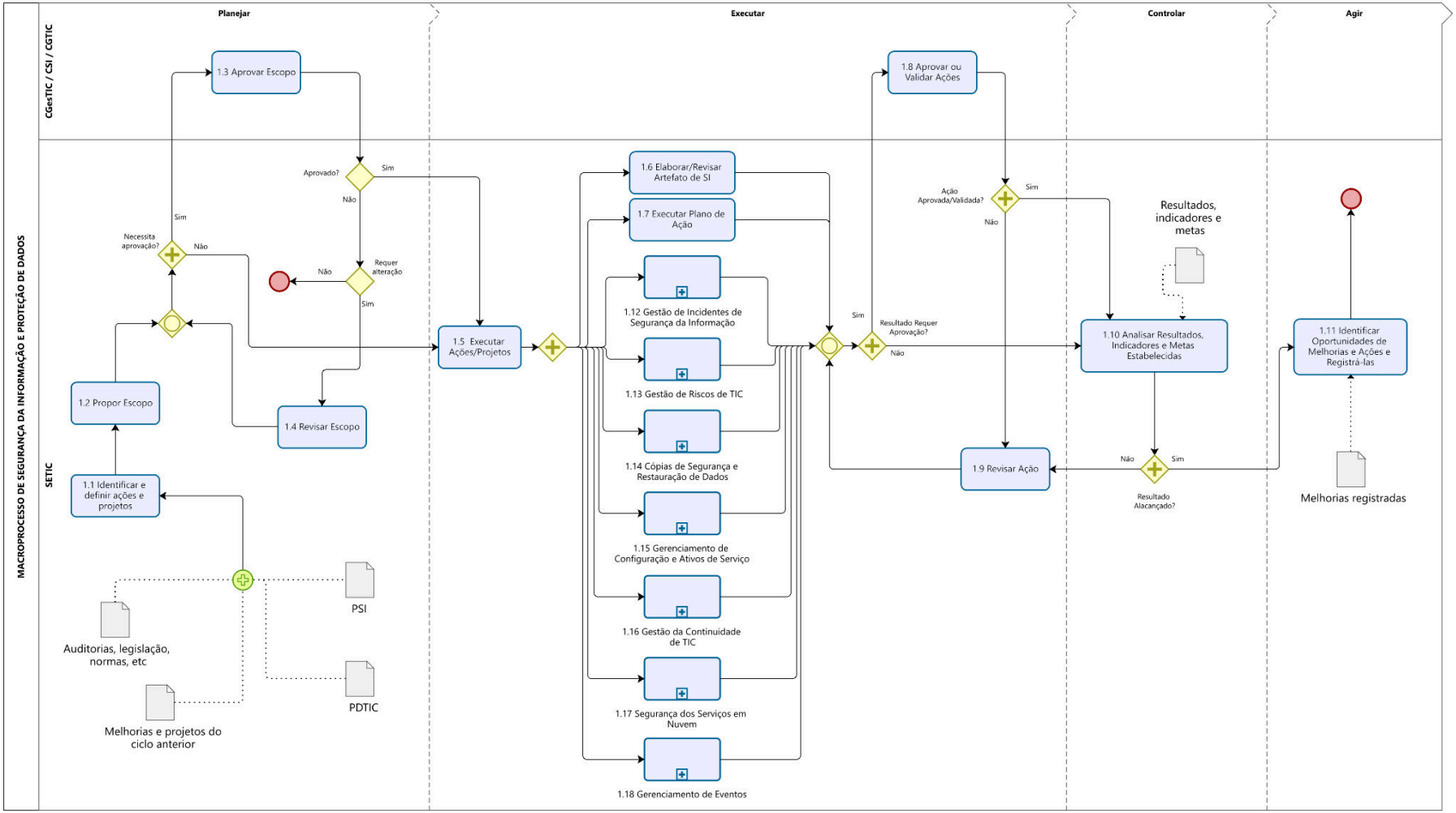
INTERFACE COM DEMAIS PROCESSOS

- **Gerenciamento de Configuração e Ativos de Serviço:** interação para assegurar que os ativos requeridos para a entrega de um serviço sejam adequadamente controlados, com informações seguras;
- **Gerenciamento de incidentes de TIC:** o processo pode ser iniciado através de um incidente que já estava em tratamento no processo de gerenciamento de incidentes.
- **Gestão de Incidentes de Segurança da Informação:** o processo pode ser iniciado para realizar procedimentos a serem adotados no tratamento de incidentes de segurança da informação e detalhes de comunicação.
- **Gestão de Riscos de TIC:** procedimentos a serem adotados para o gerenciamento dos riscos de TIC.
- **Cópias de Segurança e Restauração de Dados:** interação com o processo visando garantir a disponibilidade contínua da informação em tempo hábil para a tomada das decisões do Regional, por meio da gestão de cópias de segurança (backup) e de restauração (restore).

- **Gestão da Continuidade de TIC:** o processo pode ser iniciado para realizar procedimentos que visem estabelecer a continuidade dos serviços essenciais de TIC.
- **Segurança dos Serviços em Nuvem:** procedimentos a serem executados em relação à segurança dos serviços em nuvem.
- **Gerenciamento de Eventos:** desenvolvimento e implementação de atividades adequadas à descoberta oportuna de eventos ou à detecção de incidentes de segurança cibernética. Estão contempladas ações de monitoramento contínuo de segurança, processos de detecção de anomalias e eventos;

FLUXOGRAMAS DESTE PROCESSO

FLUXOGRAMA: Macroprocesso de Segurança da Informação e Proteção de Dados



DESCRIÇÃO DAS ATIVIDADES DO FLUXOGRAMA			
Nome da atividade	**Objetivo**	**Responsável**	**Tarefas / Ações**
1.1 – Identificar e definir ações e projetos	Avaliar as demandas relacionadas à Segurança da Informação e definir ações.	SETIC	**Entrada:** PDTIC, PSI, auditorias, legislação, normas, resultado do ciclo de melhoria dos processos, etc. **Tarefas:** ● **Identificar ações e projetos** - Identificar as demandas relacionadas à Segurança da Informação provenientes de achados (recomendações ou determinações) de auditorias, projetos ou demandas do PDTIC, normas, legislação vigente que demande implantação, elaboração ou revisão de algum artefato (PSI e seus anexos, protocolos da ENSEC-PJ e seus anexos), revisão dos processos associados a este macroprocesso; - Propostas de melhoria contínua decorrente de ações anteriormente realizadas. ● **Definir ações e projetos** - Identificar ações/projetos, definindo quais serão os objetos de implementação e definir período. **Saída:** Ações/Projetos a serem executadas.
1.2 – Propor Escopo	Definir as atividades, os objetivos, os resultados esperados com a execução da ação ou projeto.	SETIC	**Entrada:** Ações/Projetos a serem executadas. **Tarefas:** ● Definir o escopo da ações/projetos que serão executadas; ● Documentar a proposta e enviar para validação ao Comitê Responsável. **Saída:** Escopo das Ações/Projetos.
1.3 – Aprovar Escopo	Realizar análise da proposta e formalizar aprovação da ação ou projeto que será executada.	CGesTIC; CSI; ou CGTIC	**Entrada:** Escopo das Ações/Projetos; Escopo das Ações/Projetos Revisado. **Tarefas:** ● Analisar o escopo das Ações/Projetos e manifestar-se quanto à aprovação ou necessidade de ajustes; ● Caso necessário, solicitar ajustes ao documento; ● Encaminhar para a unidade responsável por executar as Ações/Projetos. **Saída:** Escopo das Ações/Projetos aprovado; Solicitação de ajustes no escopo; ou Escopo não aprovado.
1.4 – Revisar Escopo	Adequar o escopo com as alterações sugeridas pelo	SETIC	**Entrada:** Solicitação de ajustes no escopo. **Tarefas:**

	comitê responsável.		• Revisar o escopo de acordo com as solicitações impostas. • Formalizar a revisão do escopo: elaborar versão atualizada. • Reencaminhar ao Comitê que solicitou a revisão. **Saída:** Escopo das Ações/Projetos Revisado.
1.5 – Executar Ações e Projetos	Encaminhar as ações ou projetos às atividades correspondentes.	SETIC	**Entrada:** Escopo das Ações/Projetos; ou Escopo das Ações/Projetos aprovado **Tarefas:** • Direcionar ao processo ou à atividade adequada ao escopo da ação ou do projeto. **Saída:** Ação a executar.
1.6 – Elaborar/Revisar Artefatos de SI	Elaborar ou revisar artefatos relacionados à Segurança da Informação.	SETIC	**Entrada:** Ação a executar. **Tarefas:** • Elaborar artefatos relacionados à segurança da informação; • Revisar artefatos de acordo com sua necessidade ou programação. **Saída:** Artefato elaborado/revisado.
1.7 – Executar Plano de Ação	Executar o Plano de Ação previsto no escopo.	SETIC	**Entrada:** Ação a executar. **Tarefas:** • Identificar as ações prioritárias. • Estabelecer o cronograma de execução. • Distribuir as tarefas. • Executar as ações. **Saída:** Plano de ação executado.
1.8 – Aprovar ou Validar Ações	Aprovar ou validar as ações e/ou resultados.	CGesTIC; CSI; ou CGTIC	**Entrada:** Artefato elaborado/revisado; Plano de ação executado; Processo executado; Ação reexecutada. **Tarefas:** • Analisar a execução das Ações/Projetos e manifestar-se quanto à aprovação ou necessidade de ajustes; • Caso necessário, solicitar ajustes e/ou reexecução da ação; • Encaminhar para a unidade responsável por executar as Ações/Projetos. **Saída:** Artefato elaborado/revisado - Aprovado; Plano de ação executado - Aprovado; ou Processo executado - Aprovado. Artefato elaborado/revisado - Não Aprovado; Plano de ação executado - Não Aprovado;
1.9 – Revisar Ação	Revisar a ação ou projeto caso não obtenha o resultado esperado.	SETIC	**Entrada:** Artefato elaborado/revisado - Não Aprovado; Plano de ação executado/Não Aprovado; Relatório de execução. **Tarefas:** • Reexecutar a ação buscando atender os resultados esperados.

			Saída: Ação reexecutada;
1.10 – Analisar Resultados, Indicadores e Metas Estabelecidas	Apurar os resultados das ações em comparação com o planejado e o realizado.	SETIC	**Entrada:** Artefato elaborado ou revisado - Aprovado; Plano de ação executado - Aprovado; ou Processo executado. **Tarefas:** ● Compilar as informações. ● Executar a análise comparativa entre o planejado e o realizado. ● Confeccionar relatório. **Saída:** Relatório de execução.
1.11 – Identificar Oportunidades de Melhorias e Ações e Registrá-las	Identificar as oportunidades de melhorias encontradas com base no relatório de execução e registrá-las.	SETIC	**Entrada:** Relatório de execução. **Tarefas:** ● Implementar o plano de ação de melhorias; ● Criar o cronograma de execução; ● Controlar e acompanhar a execução do plano de ação de melhorias; ● Registrar as melhorias. **Saída:** Plano de ação de melhorias; ou Registro de melhorias.
1.12 Executar processo: Gestão de Incidentes de Segurança da Informação	Executar o processo de acordo com sua metodologia aplicável.	SETIC	**Entrada:** Ação a executar **Tarefas:** ● Executar tarefas conforme descrito no processo. **Saída:** Processo executado
1.13 Executar processo: Gestão de Riscos de TIC	Executar o processo de acordo com sua metodologia aplicável.	SETIC	**Entrada:** Ação a executar **Tarefas:** ● Executar tarefas conforme descrito no processo. **Saída:** Processo executado
1.14 Executar processo: Cópias de Segurança e Restauração de Dados	Executar o processo de acordo com sua metodologia aplicável.	SETIC	**Entrada:** Ação a executar **Tarefas:** ● Executar tarefas conforme descrito no processo. **Saída:** Processo executado
1.15 Executar processo: Gerenciamento de Configuração e Ativos de Serviço	Executar o processo de acordo com sua metodologia aplicável.	SETIC	**Entrada:** Ação a executar **Tarefas:** ● Executar tarefas conforme descrito no processo. **Saída:** Processo executado
1.16 Executar processo: Gestão da	Executar o processo de acordo com sua	SETIC	**Entrada:** Ação a executar **Tarefas:**

Continuidade de TIC	metodologia aplicável.		• Executar tarefas conforme descrito no processo. **Saída:** Processo executado
1.17 Executar processo: Segurança dos Serviços em Nuvem	Executar o processo de acordo com sua metodologia aplicável.	SETIC	**Entrada:** Ação a executar **Tarefas:** • Executar tarefas conforme descrito no processo. **Saída:** Processo executado
1.18 Executar processo: Gerenciamento de Eventos	Executar o processo de acordo com sua metodologia aplicável.	SETIC	**Entrada:** Ação a executar **Tarefas:** • Executar tarefas conforme descrito no processo. **Saída:** Processo executado

IDENTIFICAÇÃO DOS RISCOS

Os principais riscos e ameaças que afetam a Segurança da Informação devem ser identificados e gerenciados, de forma a mitigar o impacto da sua ocorrência no âmbito do armazenamento ou transmissão de dados. A relação de eventos evidenciados na Matriz de Gerenciamento de Riscos de Segurança da Informação, não pretende esgotar todas as possibilidades de acontecimentos danosos, porém contempla de forma macro um mapeamento inicial que deve ser aperfeiçoado ao longo do tempo, de acordo com as revisões previstas neste macroprocesso.

GLOSSÁRIO

Ataque Cibernético: tentativa de ataque a captura de dados ou invasão à rede computacional do Tribunal.

Atividades Críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de forma que permitam atingir os objetivos mais importantes e sensíveis ao tempo.

Backup: processo de cópia e armazenamento dos dados sob a guarda da Secretaria de Tecnologia da Informação e Comunicação, visando garantir a segurança, integridade e disponibilidade.

Crise Cibernética: decorre de incidentes em dispositivos, serviços e redes de computadores, que causam dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;

CSI: Comitê de Segurança da Informação.

Evento de segurança da informação: Ocorrência identificada que pode afetar um ativo de informação associada a possível violação da política de segurança da informação ou falha de controles de segurança da informação, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

ETIR: Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação - Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança da informação.

Evidência: Dados que apoiam a existência ou a veracidade de algo.

Malware: É um programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não).

Incidente de Segurança da Informação: Ocorrência identificada e confirmada que afeta um ativo de informação com indicação de violação da política de segurança da informação ou falha de controles de segurança da informação, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Integridade: Propriedade de salvaguarda da exatidão e completeza de ativos de informação.

Parte Interessada: Pessoa ou grupo que tem um interesse no desempenho ou no sucesso de uma organização.

RISI: Relatório de Incidente de Segurança da Informação.

Vulnerabilidade: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

REFERÊNCIAS

PDTIC 2023-2024 Ed.2023-2

Res CNJ Nº 370/2021 - ENTIC-JUD

Res CNJ nº 396/2021 - ENSEC-PJ

Processos de Tecnologia da Informação e Comunicação do TRT14

Política de Segurança da Informação do TRT14

DESTINAÇÃO DO PROCESSO

Servidores da Secretaria de Tecnologia da Informação e Comunicação, ETIR e CSI.

OUTRAS INFORMAÇÕES DESTE PROCESSO

Histórico de Revisões			
Data	**Versão**	**Descrição**	**Responsável**
21/11/2022	1.0	Versão inicial do documento	Wainner Brum Caetano
18/06/2024	1.1	Revisão do processo	Wainner Brum Caetano