MANUAL DE PROCESSO DE TRABALHO 11

IDENTIFICAÇÃO DO PROCESSO

PROCESSO DE GERENCIAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO		
OBJETIVO	Receber, analisar e responder às notificações relacionadas a incidentes de segurança da informação.	
MANUAL	**NÚMERO**	11
	NOME	INCIDENTES DE SI
	VERSÃO	2

VISÃO SISTÊMICA

PROCESSO DE GERENCIAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	
ENTRADA(S)	Incidentes de segurança da informação
FORNECEDOR(ES)	Central de Serviços Processo de Gerenciamento de Eventos
SAÍDA(S)	Incidentes de segurança solucionados
CLIENTE(S)	Unidades de negócio
REGULAÇÃO	Resolução CNJ 23.501/2016 Resolução TRE-SE 180/2013 - Política de Segurança da Informação (PSI)
RECURSO(S)	Sistema de Helpdesk

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 11	Gestão da Informação
PROCESSO 11.7	Segurança da Informação
SUBPROCESSO 11.7.4	Gerenciamento de Incidentes de Segurança da Informação

GESTOR DO PROCESSO

GESTOR DO PROCESSO	
UNIDADE	A Assessoria de Planejamento e Gestão da STI (ASPLAN/ 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.

PARTICIPANTE(S) DO PROCESSO

PARTICIPANTE(S)	
GRUPO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO (GRISI)	Equipe multidisciplinar responsável por executar as atividades de avaliação, categorização, priorização e análise do incidente de segurança, bem como por responder aos incidentes identificados. A liderança do grupo cabe ao Gerente de Incidentes de SI, responsável por coordenar o trabalho diário do GRISI, decidindo como agir em situações problemáticas, verificando o cumprimento das tarefas, representando o GRISI dentro e fora da organização e escalando os incidentes caso necessário. No âmbito do TRE-SE, o papel é desempenhado pelo Coordenador de Infraestrutura.
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO (STI)	Unidade responsável por auxiliar na resolução de incidentes que ultrapassem a competência e a autoridade do GRISI.

TERMOS E DEFINIÇÕES

TERMO	DEFINIÇÃO
ATIVO	No contexto do processo refere-se ao recurso (sistema, equipamento, aplicação etc.) envolvido no incidente de segurança.
INCIDENTE DE SEGURANÇA DA INFORMAÇÃO	Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação, que cause a perda de um ou mais princípios de segurança (confidencialidade, integridade e disponibilidade).
MODELO DE INCIDENTE	Documento que define previamente o procedimento padrão (roteiro) a ser seguido pelos responsáveis pelo atendimento, durante a resolução de tipos particulares de incidentes, haja vista que nem todos os incidentes são novos.

INDICADOR(ES) DE DESEMPENHO

INDICADOR 1: ÍNDICE DE DESCUMPRIMENTO DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	
TIPO	Efetividade
O QUE MEDE	O quantitativo de incidentes de segurança da informação ocasionados por descumprimento das políticas de segurança da informação do TRE-SE.
PARA QUE MEDIR	Identificar a necessidade de se promover campanhas de esclarecimento sobre segurança da informação ou realização de ajustes nas políticas existentes.
QUEM MEDE	Seção de Segurança da Informação (SESIN)
QUANDO MEDIR	Anualmente
ONDE MEDIR	Sistema de Helpdesk
COMO MEDIR	Identificar o quantitativo de incidentes de segurança, constantes do sistema de Helpdesk, que violaram as políticas de segurança do Tribunal, seja de forma premeditada ou por desconhecimento das normas.
META	Menor que 10 ao ano

MATRIZ RACI

Definição e distribuição de papéis e responsabilidades que integram o Processo de Gerenciamento de Incidentes de Segurança da Informação.

LEGENDA

R **Responsável**, quem deve executar a atividade
A **Autoridade**, quem deve responder pela atividade
C **Consultado**, quem deve ou pode ser consultado no momento da execução da atividade
I **Informado**, quem deve receber a informação de que uma atividade foi executada

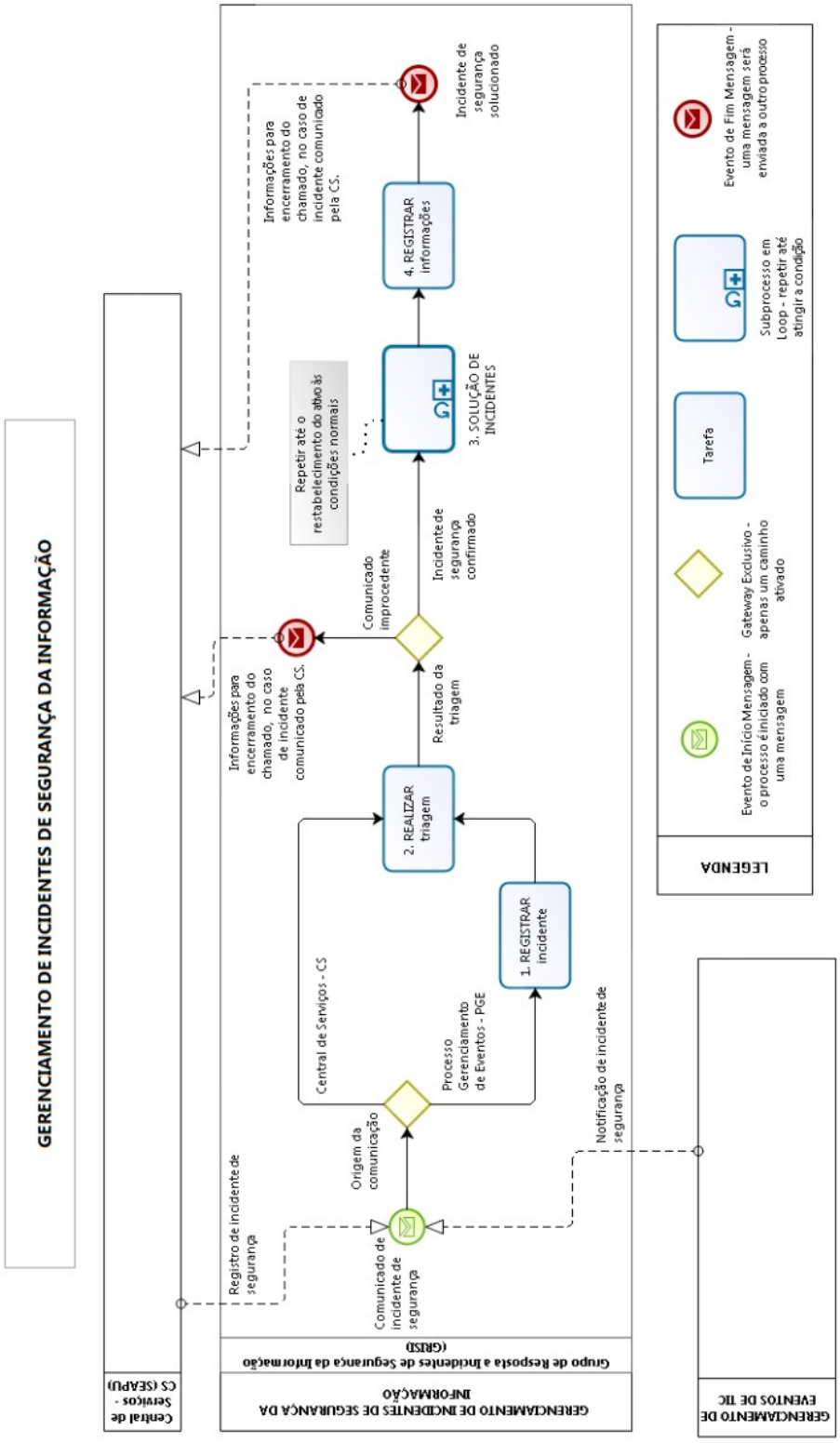
ATIVIDADE	STI	GRISI
1. REGISTRAR incidente	-	R/A
2. REALIZAR triagem	R/A	R/A
3. SOLUÇÃO DE INCIDENTES		
3.1. EXECUTAR medidas de contenção	-	R/A
3.2 COLETAR informações	-	R/A
3.3. ANALISAR informações	-	R/A
3.4 TOMAR providências	R/A	-
3.5 SOLUCIONAR Incidente	-	R/A
4. REGISTRAR informações	-	R/A

AUTORES DO MANUAL

MANUAL ELABORADO POR	
UNIDADES	STI - Secretaria de Tecnologia da Informação
	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


GERENCIAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO
Central de Serviços - CS (SEAPU)
GERENCIAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO
Grupo de Resposta a Incidentes de Segurança da Informação (GRSI)
GERENCIAMENTO DE EVENTOS DE TIC
Comunicado de incidente de segurança
Origem da comunicação
Central de Serviços - CS
Processo Gerenciamento de Eventos - PGE
1. REGISTRAR incidente
2. REALIZAR triagem
Registro de incidente de segurança
Notificação de incidente de segurança
Resultado da triagem
Comunicado improcedente
Incidente de segurança confirmado
Informações para encerramento do chamado, no caso de incidente comunicado pela CS.
Repetir até o restabelecimento do atvo às condições normais
3. SOLUÇÃO DE INCIDENTES
4. REGISTRAR informações
Incidente de segurança solucionado
Informações para encerramento do chamado, no caso de incidente comunicado pela CS.
LEGENDA
Evento de Início Mensagem - o processo é iniciado com uma mensagem
Gateway Exclusivo - apenas um caminho ativado
Tarefa
Subprocesso em Loop - repetir até atingir a condição
Evento de Fim Mensagem - uma mensagem será enviada a outro processo

PROCESSOS/ENTIDADES RELACIONADOS

GERENCIAMENTO DE EVENTOS DE TIC
DESCRIÇÃO
Dispõe sobre o gerenciamento de eventos gerados pelos itens de configuração ou serviços de TIC, sendo responsável por determinar e analisar, de forma proativa, as ocorrências dos mesmos, garantindo o funcionamento normal dos serviços com o menor impacto para os usuários.

CENTRAL DE SERVIÇOS - CS (SEAPU)
DESCRIÇÃO
Unidade de gerenciamento de incidentes, de requisições de serviços e também de comunicação com os usuários, constituindo-se no único ponto de contato entre estes e o provedor de serviços. É responsável, no contexto do processo de gerenciamento de incidentes de segurança da informação, pelo registro, encaminhamento e fechamento dos incidentes reportados.
No TRE-SE, as funções da Central de Serviços são exercidas pela Seção de Apoio ao Usuário (SEAPU).

1. REGISTRAR incidente
DESCRIÇÃO
Registrar o incidente de segurança da informação para posterior análise e solução.

EXECUTANTE
Grupo de Resposta a Incidentes de Segurança da Informação (GRISI)

2. REALIZAR triagem
DESCRIÇÃO
- Verificar se, realmente, trata-se de incidente de segurança da informação.
- Classificar o incidente de segurança de acordo com a seguinte tabela:

Categorias de Incidentes de Segurança da Informação		
Classe	**Tipo**	**Descrição**
Conteúdo Abusivo	Spam	Recebimento/envio de e-mail não solicitado para grande número de pessoas.
	Assédio	Recebimento/postagem de mensagem com conteúdo discriminatório.
	Sexual/Violência	Recebimento/postagem/armazenamento de material com conteúdo pornográfico ou incentivando a violência.
Código Malicioso (Malware)	Virus	Software incluído intencionalmente em um sistema com a intenção de executar ações maliciosas (alterar ou excluir informações, monitorar atividade do sistema, etc.)
	Bot	
	Worm	
	Cavalo de Tróia (Trojan)	
	Spyware	
Coleta de Informações	Varredura (scan)	Técnica que consiste em efetuar buscas minuciosas em redes com objetivo a identificação de sistemas e a coleta de informações para utilização posterior.
	Sniffing	Interceptação de tráfego.
	Engenharia Social	Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações ou fornecer informações.
Tentativa de intrusão	Exploração de vulnerabilidade conhecida	Tentativa de comprometer um sistema ou indisponibilizar um serviço mediante a exploração de vulnerabilidade conhecida (buffer overflow, backdoors, cross side scripting, etc.).
	Tentativa de login	Múltiplas tentativas de efetuar login em sistema (guessing, cracking de senhas, força bruta).
	Nova assinatura de ataque	Tentativa de explorar vulnerabilidade desconhecida (zero-day attack)
Intrusão	Comprometimento de conta privilegiada	Comprometimento bem-sucedido de sistema ou aplicação. Pode ter sido realizado remotamente (vulnerabilidade conhecida ou não) ou localmente via acesso não autorizado.
	Comprometimento de conta não privilegiada	
	Comprometimento de aplicação ou sistema	

Categorias de Incidentes de Segurança da Informação		
Disponibilidade	DoS	Ataques que comprometam a disponibilidade de sistemas ou serviços (PING flooding, e-mail bomba, interrupção do fornecimento de refrigeração ou de fornecimento de energia, etc.)
	DDoS	
	Sabotagem	
Fraude	Uso não autorizado de recursos	Utilizar recursos de TIC para propósitos não autorizados (ex: uso de conta de e-mail corporativo para participar de esquemas de pirâmide ou enviar spam).
	Pirataria	Uso de software não licenciado.
Outros	Todos os incidentes de segurança da informação que não se enquadrem nas categorias anteriores.	OBS: O crescimento do número de incidentes nesta categoria é um indicativo de que o esquema de classificação deve ser revisado.

- Priorizar o incidente de segurança de acordo com os seguintes critérios:

Nível de prioridade	Impacto	Critérios
3	Alto	• Muitas Secretarias e Cartórios Eleitorais foram afetados; • Usuários chave do Tribunal foram afetados; • Usuários externos (parceiros, eleitores, etc.) foram afetados; • Usuário incapaz de desempenhar suas atividades, podendo acarretar consequências graves (perda de prazo, comprometimento de um procedimento licitatório, etc.); • Serviços/sistemas críticos foram afetados: ELO, SEI, sistemas/equipamentos que atendem ao plenário, durante a sessão plenária; sistemas/equipamentos relacionados às eleições, em dia de eleição, etc).
2	Moderado	• Uma ou mais Secretarias e Cartórios Eleitorais foram impactados; • O usuário desempenha suas atividades de forma

Nível de prioridade	Impacto	Critérios
		precária, podendo acarretar consequências graves com o passar do tempo; • Degradação no desempenho/qualidade de sistemas ou equipamentos, podendo se agravar com o passar do tempo.
1	Baixo	• Poucos usuários foram impactados; • Usuário executa suas atividades de forma precária, mas a urgência para execução das tarefas é baixa.

- Atribuir o incidente a um indivíduo ou a um grupo.

EXECUTANTE
Grupo de Resposta a Incidentes de Segurança da Informação (GRISI)

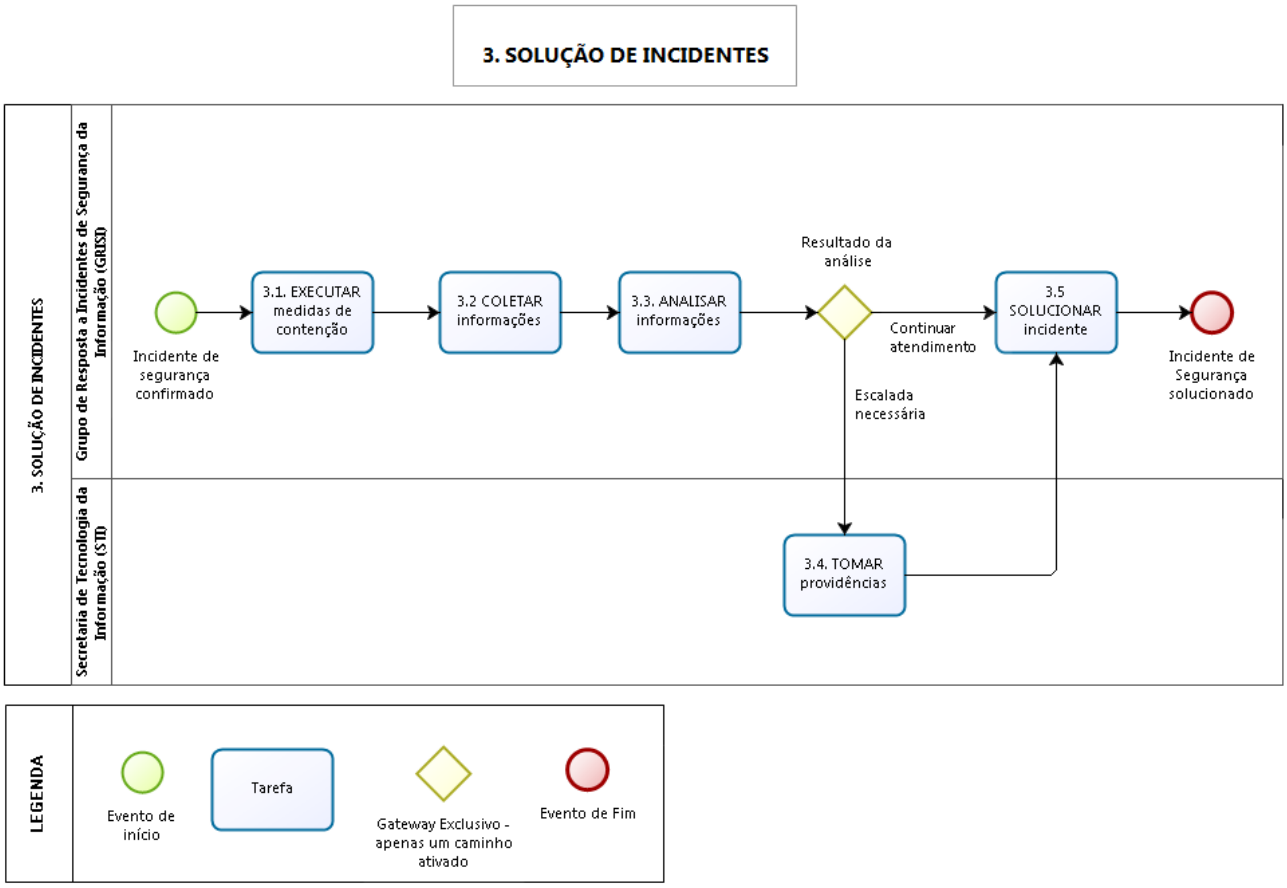
3. SOLUÇÃO DE INCIDENTES

DESCRIÇÃO
Subprocesso

4. REGISTRAR informações

DESCRIÇÃO
Registrar as medidas que foram adotadas para a resolução do incidente e submeter o chamado para encerramento na Central de Serviços.

EXECUTANTE
Grupo de Resposta a Incidentes de Segurança da Informação (GRISI)


3. SOLUÇÃO DE INCIDENTES
3. SOLUÇÃO DE INCIDENTES
Grupo de Resposta a Incidentes de Segurança da Informação (GRISI)
Secretaria de Tecnologia da Informação (STI)
Incidente de segurança confirmado
3.1. EXECUTAR medidas de contenção
3.2 COLETAR informações
3.3. ANALISAR informações
Resultado da análise
Continuar atendimento
Escalada necessária
3.5 SOLUCIONAR incidente
Incidente de Segurança solucionado
3.4. TOMAR providências

LEGENDA
Evento de início
Tarefa
Gateway Exclusivo - apenas um caminho ativado
Evento de Fim

3. SOLUÇÃO DE INCIDENTES

3.1. EXECUTAR medidas de contenção

DESCRIÇÃO

Executar medida de contenção imediata, a exemplo do bloqueio de conta, remoção da rede de computador suspeito, suspensão de acesso à Internet, dentre outros.

EXECUTANTE

Grupo de Resposta a Incidentes de Segurança da Informação (GRISI)

3.2 COLETAR informações

DESCRIÇÃO

Notificar as partes interessadas e coletar informações a respeito do incidente (sistemas e usuários afetados, logs de eventos, hora do incidente, histórico de ocorrências, ou seja, todas as evidências aplicadas ao caso concreto).

EXECUTANTE

Grupo de Resposta a Incidentes de Segurança da Informação (GRISI)

3.3. ANALISAR informações

DESCRIÇÃO

- Filtrar os dados mais relevantes;
- Confrontar as evidências encontradas com o comportamento considerado normal para o sistema/aplicação/rede;
- Efetuar a correlação entre os diversos eventos coletados na atividade anterior;
- Pesquisar bases de conhecimento e efetuar pesquisas na internet para identificação das possíveis causas do incidente ou os métodos utilizados;
- Solicitar o auxílio de técnicos mais experientes de outros Tribunais ou de fornecedores, caso necessário;
- Propor ações para solução do incidente;
- Caso as ações necessárias para solucionar o incidente extrapolem a competência da GRISI, escalar o chamado para a STI.

EXECUTANTE

Grupo de Resposta a Incidentes de Segurança da Informação (GRISI)

3.4. TOMAR providências

DESCRIÇÃO

Dar o encaminhamento necessário, de acordo com a sensibilidade da situação.

EXECUTANTE

Secretaria de Tecnologia da Informação (STI)

3.5 SOLUCIONAR incidente

DESCRIÇÃO

- Solucionar o incidente e restabelecer o ativo às condições normais.
- Sempre que possível, deve-se seguir os passos de um "modelo de incidente" para resolução do problema.

EXECUTANTE

Grupo de Resposta a Incidentes de Segurança da Informação (GRISI)