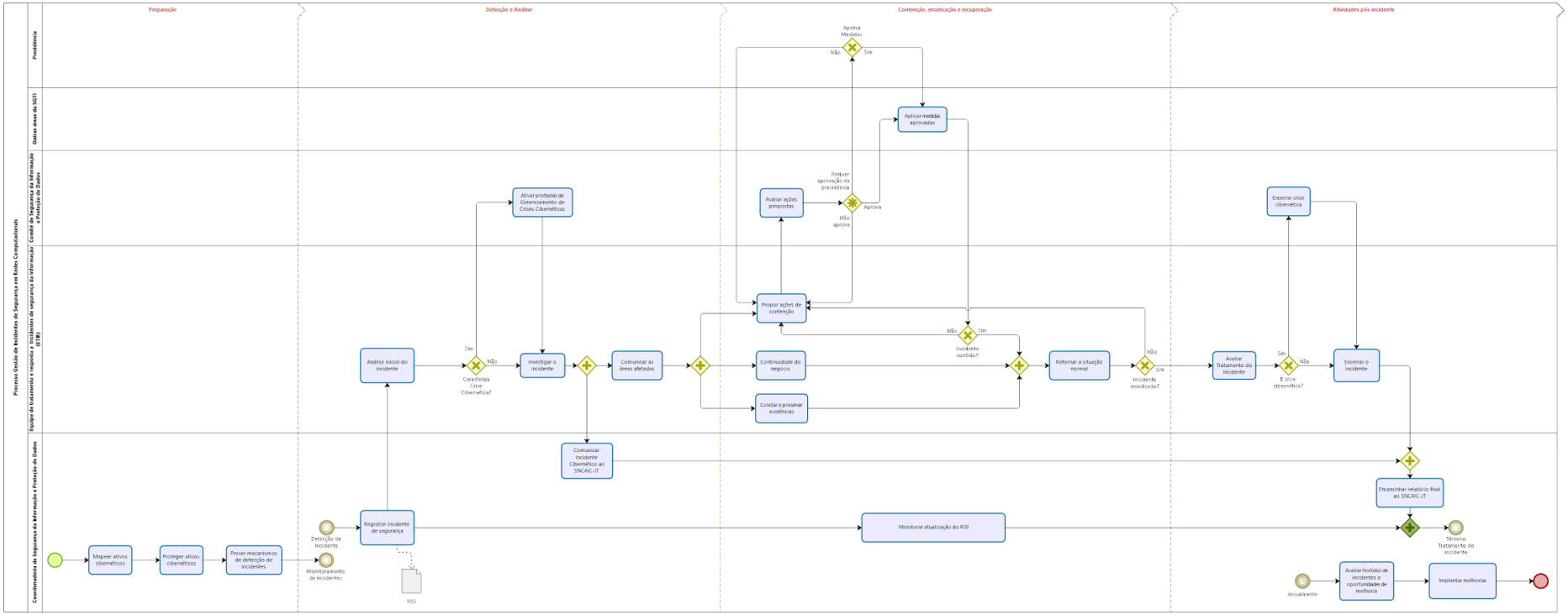
GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

DESENHO DO PROCESSO
DEFINIÇÕES
DESCRIÇÃO DAS TAREFAS

Versão set.2025

DESENHO DO PROCESSO



PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO
TRT DA 4ª REGIÃO

CONTROLE DE VERSÕES

Versão e data	Alterações
set.2025	Versão de controle inicial

DEFINIÇÕES

Objetivo do Processo
Detectar e responder a incidentes de segurança da informação de forma eficaz e eficiente, minimizando impactos adversos nas operações de negócio e assegurando que os níveis acordados de qualidade do serviço sejam mantidos.

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

Papéis		Responsabilidades
Presidência	Órgão diretivo do TRT	● Analisar e deliberar sobre ações a serem realizadas para o tratamento de incidentes de segurança da informação;
Comitê de Segurança da Informação e Proteção de Dados	Comitê multidisciplinar responsável pela coordenação das ações e deliberações relacionadas à área de segurança da TIC.	● Determinar e gerenciar situação de crise cibernética; ● Ativar e encerrar protocolo de Gerenciamento de Crises Cibernéticas quando necessário; ● Analisar e deliberar sobre ações a serem realizadas para o tratamento de incidentes de segurança da informação.
Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR)	Equipe responsável pelas atividades relacionadas ao tratamento e resposta a incidentes de segurança da informação.	● Monitorar o ambiente e recursos de TIC do TRT, a fim de identificar possíveis incidentes de segurança da informação. ● Realizar a investigação do incidente de segurança da informação, propondo medidas de contenção. ● Assessorar o Comitê de Segurança da Informação e Proteção de Dados e a SGTI na análise e tomada de decisões a respeito de situações resultantes de incidentes de segurança da informação. ● Realizar a análise do incidente de segurança da informação, de forma a propor medidas para eliminar ou solucionar problemas que causaram o incidente de segurança da informação.

		● Realizar a comunicação com o CTIR.BR.
Coordenadoria de Segurança da Informação e Proteção de Dados	Coordenadoria responsável pelas atividades que envolvam segurança da informação.	● Registrar e monitorar a atualização do incidente de segurança da informação (RISI); ● Acompanhar evolução da contenção do incidente e recuperação à situação normal;
Outras áreas da SGTI	Compreendem a Diretoria da SGTI, suas Coordenações e Seções. Atuam em conjunto na análise e resolução dos incidentes em redes quando acionados pela ETIR.	● Auxiliar a ETIR na proposição e execução de medidas para contenção e solução de incidentes de segurança da informação. ● Autorizar, quando necessário a execução das medidas propostas pela ETIR; ● Atualizar o RISI;

Termos/Artefatos	
RISI	Relatório de Incidentes de Segurança da Informação

Ferramentas	
Google Docs	RISI - Relatório de Incidentes de Segurança da Informação
PRIC-001 - Ransonware	Plano de resposta de incidentes cibernético - Ransomware
PRIC-002 - Dados Pessoais	Plano de resposta de incidentes cibernéticos envolvendo dados pessoais
Procedimento Operacional - 001 - Vazamento de Credenciais	Playbook para resposta de incidente cibernético com vazamento de credenciais de acesso

Referências técnicas, legais e normativas que fundamentam o Processo	
Ato Conjunto TST.CSJT.GP N.º 41/2025	Institui o Processo de Comunicação de Incidentes Cibernéticos na Justiça do Trabalho (PCIC)
NIST-SP 800-61	Guia de Tratamento de Incidentes de Segurança em Computadores

Indicador de benefício do processo		
Descrição do indicador	**Método de apuração / fórmula de cálculo**	**Frequência**
Registro correto de incidentes de Segurança da Informação	Percentual de RISIs preenchidos corretamente	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

DESCRIÇÃO DAS TAREFAS

Mapear ativos cibernéticos		
Descrição	Nesta tarefa deve-se mapear o conjunto de ativos cibernéticos (servidores, estações de trabalho, softwares e etc) utilizados pelo Tribunal para tratar informações.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Considerações importantes	O trabalho de mapeamento dos ativos cibernéticos é complementado no processo de Gestão de Riscos (PSI anexo 6 e Portaria 6.137/2014), onde é realizada a análise e avaliação dos riscos de exposição dos ativos cibernéticos, possibilitando a priorização de recursos humanos, tecnológicos e financeiros do Tribunal.	
Entradas	Gestão de riscos anterior e sistemas como, Oraculum, AD	
Saídas	Relação dos ativos cibernéticos do Tribunal	
Atividades	**Identificar Ativos**	Identificar quais são os ativos cibernéticos utilizados pelo Tribunal, seu responsável, etc.
	Registrar Ativos	Catalogar de forma organizada a relação dos ativos cibernéticos utilizados.
Ferramentas	Oraculum, AD, etc	

Proteger ativos cibernéticos		
Descrição	Consiste no desenvolvimento e implementação de soluções, controles, processos e planos que assegurem a proteção do ambiente tecnológico e da informação.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados Outras áreas da SGTI	
Considerações importantes	N/A	
Entradas	Relação dos ativos cibernéticos do Tribunal, Gestão de Riscos anterior	
Saídas	Planos de resposta a incidentes, planos de continuidade, implementação de controles de segurança, etc	
Atividades	**Desenvolver e implementar controles**	Criar e implementar (SGTI) controles que assegurem a proteção dos ativos cibernéticos e, por consequência, do ambiente tecnológico.
Ferramentas	Diversas	

Prover mecanismos de detecção de incidentes	
Descrição	Consiste em desenvolver e disponibilizar mecanismos que permitam a detecção de possíveis incidentes cibernéticos.
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados

	Outras áreas da SGTI	
Considerações importantes	Exemplos de mecanismos de proteção utilizados: antivírus, XDR, firewall, webproxy, SOC e etc.	
Entradas	Tráfego da rede; diversos tipos de logs, etc	
Saídas	Alertas gerados pelas ferramentas de proteção	
Atividades	**Prover mecanismos**	Prover mecanismos que detectem possíveis incidentes de segurança da informação.
Ferramentas	Antivírus, XDR, Firewall, Webproxy e etc. Planos de Resposta de Incidentes Cibernéticos; Playbooks para resposta de incidentes cibernéticos; Serviço gerenciado de SOC (XDR);	

Registrar incidente de segurança		
Descrição	Detectada a ocorrência ou suspeita de incidente, registrar de forma detalhada em formulário próprio no Google Drive - RISI (Relatório de Incidente de Segurança da Informação). Notificar a ETIR sobre o incidente suspeito.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados Equipe de Tratamento e Resposta de Incidentes de Segurança da Informação (ETIR)	
Considerações importantes	N/A	
Entradas	Detecção de possível incidente de segurança da informação	
Saídas	RISI preenchido com informações iniciais	
Atividades	**Detecção do Incidente**	CSIPD recebe alerta de detecção do incidente, que pode ser via sistema de monitoramento, a partir de telefonema ou chamado de usuário ou de outras áreas da SGTI.
	Buscar informações iniciais	A partir da detecção inicial, a CSIPD deve obter mais informações sobre o incidente. Caso o incidente tenha sido informado, deve entrar em contato para obter mais esclarecimentos para correto encaminhamento.
	Registrar o incidente	CSIPD registra o RISI no Google Drive, descrevendo e categorizando o incidente.
	Encaminhar incidente para análise inicial pela ETIR	CSIPD encaminha o registro do incidente para análise inicial da ETIR.
Ferramentas	RISI - Relatório de Incidente de Segurança da Informação	

	Planos de Resposta de Incidentes Cibernéticos Procedimentos operacionais para resposta de incidentes cibernéticos

Análise inicial do incidente		
Descrição	ETIR é notificada sobre o incidente suspeito para realizar análise inicial e, quando for o caso, encaminha ao Comitê de Segurança da Informação e Proteção de Dados para que se ative o protocolo de Gerenciamento de Crises Cibernéticas.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados Equipe de Tratamento e Resposta de Incidentes de Segurança da Informação (ETIR) Comitê de Segurança da Informação e Proteção de Dados Outras áreas da SGTI	
Considerações importantes	Neste primeiro momento, é importante que as devidas equipes sejam envolvidas para avaliar se o evento adverso é de fato um incidente de segurança da informação e, em caso positivo, analisar a extensão dos impactos e escopo do incidente, para que possa ser definido se trata-se crise cibernética.	
Entradas	RISI preenchido com informações iniciais	
Saídas	RISI preenchido com informações da análise inicial do incidente	
Atividades	**ETIR recebe notificação de incidente**	A ETIR recebe RISI registrado pela CSIPD para análise inicial do incidente.
	Análise inicial do incidente	A ETIR, com apoio de outras áreas da SGTI, verifica se o incidente possui as características para instauração do protocolo de Gerenciamento de Crises Cibernéticas.
	Encaminha para Comitê de Segurança da Informação e Proteção de Dados	Caso a ETIR julgue que o incidente possua as características para instauração do Protocolo de Gerenciamento de Crises Cibernéticas, comunicará o Comitê de Segurança da Informação e Proteção de Dados, que decidirá pela instauração ou não do protocolo.
	Encaminhar incidente para investigação	Caso a ETIR não encontre indícios da necessidade de instauração do Protocolo de Gerenciamento de Crises Cibernéticas, encaminha o incidente diretamente para investigação.
Ferramentas	RISI - Relatório de Incidente de Segurança da Informação Planos de Resposta de Incidentes Cibernéticos Playbooks para resposta de incidentes cibernéticos	

Comunicar incidente cibernético ao SNCAIC-JT		
Descrição	O Gestor de Segurança Cibernética do Tribunal comunicará o incidente ao SNCAIC-JT.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Considerações importantes	Conforme processo estabelecido no Ato Conjunto TST.CSJT.GP N.º 41, de 25 de julho de 2025, encaminhar relatório contendo informações preliminares acerca do incidente cibernético.	
Entradas	RISI preenchido com informações da análise inicial do incidente	
Saídas	Comunicação ao SNCAIC-JT	
Atividades	**Comunicar incidente ao SNCAIC-JT**	A CSIPD comunicará a SNCAIC-JT do incidente, contemplando ao menos as seguintes informações: I - descrição sucinta do incidente cibernético; II - data e hora da ocorrência ou da detecção; III - produtos ou ativos afetados; IV - classificação da gravidade do incidente cibernético; V - impactos observados; VI - providências iniciais adotadas; VII - Tipo de incidente (p. ex: malware, phishing, DDoS, acesso não autorizado); e VIII - Evidências coletadas (e.g. logs, screenshots).
Ferramentas	RISI - Relatório de Incidente de Segurança da Informação	

Ativar o Protocolo de Gerenciamento de Crises Cibernéticas		
Descrição	O Comitê de Segurança da Informação e Proteção de Dados se reunirá para ativar o Protocolo de Gerenciamento de Crises Cibernéticas observando as definições da Portaria GP.TRT nº 4.347/2022.	
Papéis	Comitê de Segurança da Informação e Proteção de Dados	
Considerações importantes	Os critérios para definição de Crise Cibernéticas encontram-se descritas no item 4 do Protocolo de Gerenciamento de Crises Cibernéticas.	
Entradas	RISI	
Saídas	Ativação ou não do Protocolo de Gerenciamento de Crises Cibernéticas	
Atividades	**Recebe informações sobre incidente**	O Comitê recebe as informações sobre o incidente.
	Analisa	A partir das informações recebidas o comitê analisa se deve ser

	informações	ativado o Protocolo de Gerenciamento de Crises Cibernéticas.
	Ativa Protocolo	Julgando tratar-se de crise ativa formalmente o protocolo. Após encaminha o incidente para investigações aprofundadas.
Ferramentas	RISI - Relatório de Incidente de Segurança da Informação Protocolo de Gerenciamento de Crises Cibernéticas (PGCC-TRT4)	

Investigar o incidente		
Descrição	A ETIR, com base nas informações registradas no RISI, deverá investigar as possíveis causas, extensão e impacto do incidente, a fim de subsidiar as decisões e ações para sua contenção e erradicação.	
Papéis	ETIR	
Considerações importantes	Para esta atividade a ETIR poderá solicitar informações às áreas técnicas responsáveis, a fim de elucidar a extensão e o impacto do problema, quais ativos e sistemas estão sendo afetados e começar a definir uma ação para conter o incidente. A identificação do tipo e impacto do incidente é muito importante nesta etapa, pois ela definirá o encaminhamento a ser dado quanto à necessidade de ações de contenção, de comunicação a outras áreas sobre a ocorrência do incidente e de realização de investigação de acessos. Quando ativado, o Protocolo de Gerenciamento de Crises Cibernéticas incorrerá no acompanhamento das atividades do ETIR pelo Comitê de Segurança da Informação e Proteção de Dados.	
Entradas	RISI	
Saídas	RISI	
Atividades	**Verificar o tipo de incidente**	Verificar se é uma investigação de acesso indevido, descumprimento da PSI, indisponibilidade de um serviço ou sistema por falha de segurança, invasão, propagação de vírus, vazamento de dados etc.
	Analisar a extensão e o impacto causado pelo incidente	Analisar quais serviços, sistemas e ativos foram afetados e qual foi o dano causado pelo impacto. Se necessário, envolver outras equipes.
Ferramentas	RISI Planos de Resposta de Incidentes Cibernéticos Procedimentos operacionais para resposta de incidentes cibernéticos	

Comunicar as áreas afetadas		
Descrição	Se o incidente de segurança afetar um ou mais grupos de serviço/sistemas ou usuários (p.ex. investigação de acesso por descumprimento da PSI), a ETIR, de posse da extensão e do impacto do incidente, deverá comunicar as áreas da SGTI sobre a ocorrência e deliberar se é necessário informar outras áreas do TRT sobre o incidente.	
Papéis	ETIR	
Considerações importantes	É de suma importância informar outras áreas da SGTI para que estas possam agir para ajudar na proposição de medidas para conter e erradicar o incidente. Além disso, a área de Serviços de TIC deve ser informada principalmente quando o incidente afetar sistemas e serviços utilizados diretamente pelos usuários, de forma a repassar orientações e informações sobre o incidente e seu tratamento, prazo de retorno do serviço, etc. Se necessário, uma comunicação ostensiva pode ser divulgada em conjunto com a SECOM, informando que a SGTI está ciente do problema e está trabalhando para resolvê-lo, informando, se possível, uma estimativa de tempo para tratá-lo.	
Entradas	RISI preenchido com as informações sobre o incidente investigado	
Saídas	Comunicado com as informações necessárias + RISI preenchido com as informações sobre o plano de comunicações	
Atividades	**Informar a extensão do impacto e quais sistemas/serviços foram afetados**	De posse dessas informações, será possível avaliar a quem e como a comunicação será realizada, bem como o teor da mensagem.
Ferramentas	RISI - Relatório de Incidente de Segurança da Informação Planos de Resposta de Incidentes Cibernéticos Playbooks para resposta de incidentes cibernéticos	

Propor ações de contenção	
Descrição	Com base nas informações levantadas na investigação do incidente, a ETIR deverá propor ações para conter o incidente, que podem ser soluções de contorno ou de resolução do problema.
Papéis	ETIR
Considerações importantes	Dependendo do tipo de incidente e de sua extensão, a ETIR poderá envolver outras áreas da SGTI para definir as ações de contenção. Dependendo da proposição (tirar um sistema crítico do ar, por exemplo), poderá ser necessária a aprovação superior. Se as medidas não forem autorizadas, novas medidas deverão ser propostas. Da mesma forma, se o incidente não for contido, novas medidas deverão ser propostas.

Entradas	RISI preenchido com as informações sobre o incidente/ ou não aprovação das medidas anteriores/ ou informação de que as medidas não foram suficientes a conter o incidente	
Saídas	RISI preenchido com as ações de contenção propostas	
Atividades	**Propor ações de contenção**	A ETIR deverá propor ações para contenção do incidente, de forma a evitar que os danos e impactos aumentem com o passar do tempo. Além disso, a ação de contenção deve restabelecer o sistema ou serviço, ainda que parcialmente, via solução de contorno ou resolução da causa do incidente.
	Encaminhar solução para aprovação	Dependendo do teor da ação proposta e da gravidade do incidente, será necessária a aprovação da chefia/coordenadoria das áreas afetadas e/ou envolvidas no incidente e na sua resolução, do Comitê de Segurança da Informação e Proteção de Dados ou da Presidência do TRT.
	Proposição de novas medidas, caso o incidente não seja contido	Se o incidente não for contido pelas medidas inicialmente propostas, novas medidas deverão ser estudadas e aplicadas.
Ferramentas	RISI - Relatório de Incidente de Segurança da Informação Planos de Resposta de Incidentes Cibernéticos Procedimentos operacionais para resposta de incidentes cibernéticos	

Avaliar ações propostas		
Descrição	Avaliar as ações propostas pela ETIR: aprovando para que sejam executadas, rejeitando para que sejam realizadas novas proposições ou encaminhando à análise da presidência quando as ações necessitarem desse nível de aprovação	
Papéis	Comitê de Segurança da Informação e Proteção de Dados	
Considerações importantes	N/A	
Entradas	Proposição da ETIR	
Saídas	Deliberação do Comitê	
Atividades	**Avaliar soluções propostas**	Ao Comitê cabe deliberar sobre a proposição de novas ações pela ETIR, sempre que necessária sua intervenção
	Emitir avaliação	Aprovar ou rejeitar as ações propostas pela ETIR

	Consultar a presidência para avaliação	Quando as ações propostas ensejarem temas que requerem o aval da Presidência para a realização, caberá ao Comitê realizar tal consulta, para obtenção da aprovação ou rejeição das ações propostas
Ferramentas	N/A	

Continuidade do negócio		
Descrição	Ativar os planos de continuidade do negócio (PCOs e PRDs), conforme Processo de Gestão de Continuidade de TIC	
Papéis	ETIR Outras áreas da SGTI	
Considerações importantes	N/A	
Entradas	RISI preenchido com as informações sobre o incidente investigado	
Saídas	RISI preenchido com registro de aplicação do plano de continuidade utilizado	
Atividades	**Ativar os planos de continuidade de negócio**	ETIR deve, com apoio das outras áreas da SGTI, disparar a execução dos planos de continuidade de negócio necessários de modo a manter a operação.
Ferramentas	RISI - Relatório de Incidente de Segurança da Informação Planos de Resposta de Incidentes Cibernéticos Playbooks para resposta de incidentes cibernéticos Planos de Continuidade Operacional (PCO) Plano de Recuperação de Desastres (PRD)	

Coletar e preservar evidências	
Descrição	Durante a investigação e resposta ao incidente é importante que sejam coletadas e preservadas as evidências do incidente, conforme Protocolo de Investigação para Ilícitos Cibernéticos (PIILC-TRT4)
Papéis	ETIR Outras áreas da SGTI
Considerações importantes	A coleta e preservação de evidências deverá observar o Protocolo de Investigação de Ilícitos Cibernéticos, de forma a atender às práticas forenses. Poderá ocorrer a realização de coletas pelos órgãos competentes, como Polícia Federal, Polícia Civil, etc.
Entradas	RISI
Saídas	Evidências ou relatórios

Atividades	**Identificação dos dados necessários à elucidação do incidente**	De acordo com as informações recebidas, os dados podem ser coletados de sistemas de monitoramento diversos. Assim, é importante que sejam identificados quais os dados que melhor podem elucidar a questão noticiada.
	Realizar a coleta, compilação e preservação de evidências	Realizar a coleta e a compilação de dados necessários à elaboração de relatório. Estes dados deverão ser protegidos contra alteração e armazenados em local de acesso restrito ao Comitê de Segurança da Informação e Proteção de Dados, a ETIR e à CSIPD Deverão ser seguidos procedimentos para garantir a integridade das evidências coletadas.
Ferramentas	RISI - Relatório de Incidente de Segurança da Informação Planos de Resposta de Incidentes Cibernéticos Protocolo de Investigação para Ilícitos Cibernéticos (PIILC-TRT4) Procedimentos operacionais para resposta de incidentes cibernéticos	

Aplicar medidas aprovadas		
Descrição	Executar as ações propostas na fase anterior, visando conter e erradicar o incidente, e verificar se o resultado esperado foi alcançado.	
Papéis	Outras áreas da SGTI	
Considerações importantes	Após aplicar as medidas, a equipe deverá avaliar se o incidente foi contido e, em caso negativo, deverá propor à ETIR novas ações que contenham o incidente. Após conter com sucesso, a equipe deverá trabalhar na erradicação do incidente, eliminando os impactos causados pela atividade maliciosa.	
Entradas	RISI com autorização da aplicação da medida de contenção proposta, quando necessária.	
Saídas	RISI com resultados das medidas aplicadas	
Atividades	**Aplicar as medidas necessárias**	Realizar as configurações e/ou modificações necessárias para conter e erradicar o incidente.
	Avaliar medidas aplicadas	Verificar se medidas aplicadas obtiveram o resultado esperado e, em caso negativo, propor à ETIR novas medidas de contenção e erradicação.
Ferramentas	RISI - Relatório de Incidente de Segurança da Informação Planos de Resposta de Incidentes Cibernéticos	

	Procedimentos operacionais para resposta de incidentes cibernéticos

Retornar à Situação Normal		
Descrição	Após a contenção e erradicação do incidente deve-se retornar à situação de funcionamento normal do ambiente tecnológico do TRT.	
Papéis	ETIR Coordenadoria de Segurança da Informação e Proteção de Dados Outras áreas da SGTI	
Considerações importantes	A restauração às condições normais só é possível após a total contenção e erradicação do incidente. Compete à ETIR, com apoio da CSIPD, avaliar se a recuperação normal pode ser instaurada e as ações para se alcançar essa situação. Demais áreas da SGTI serão envolvidas nas atividades de recuperação do ambiente tecnológico.	
Entradas	RISI	
Saídas	RISI com resultados das medidas aplicadas	
Atividades	**Avaliar a contenção e erradicação do incidente**	Avaliar se ocorreu a completa contenção e erradicação do incidente de segurança; caso ainda não tenha ocorrido devem ser encaminhadas propostas de novas ações para atingir esse objetivo
	Retornar ao estado normal de operação	Executar ações para que o ambiente tecnológico do Tribunal retorne ao seu estado normal de operação e de monitoramento.
Ferramentas	RISI - Relatório de Incidente de Segurança da Informação Planos de Resposta de Incidentes Cibernéticos Procedimentos operacionais para resposta de incidentes cibernéticos Planos de Recuperação de Desastres (PRD)	

Monitorar atualização do RISI	
Descrição	Durante todo o processo de contenção, erradicação e recuperação é necessário que o RISI seja mantido atualizado com informações do que é realizado e respectivos resultados. Compete à CSIPD o monitoramento para que essa atualização seja realizada pelas diferentes partes envolvidas neste processo.
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados
Considerações importantes	Não compete à CSIPD o preenchimento total do RISI com as informações, pois muitas vezes são de conhecimento de outras áreas da SGTI, mas cabe à CSIPD o constante

	monitoramento do relatório e a solicitação para que as informações sejam reportadas no relatório.	
Entradas	RISI	
Saídas	RISI	
Atividades	**Controlar e cobrar o correto preenchimento do RISI**	A CSIPD deve monitorar o preenchimento do relatório para que seja sempre preciso e atualizado, solicitando às áreas envolvidas o preenchimento adequado.
Ferramentas	RISI - Relatório de Incidente de Segurança da Informação	

Avaliar Tratamento do Incidente		
Descrição	Esta atividade tem por objetivo analisar o incidente como um todo (causa raiz identificada, ações de contenção e erradicação aplicadas, resultados dos relatórios elaborados etc), a fim de propor outras providências necessárias ao encerramento do incidente (medidas de solução).	
Papéis	ETIR	
Considerações importantes	O estudo poderá ser realizado em conjunto com outras áreas dependendo do tipo de incidente. De acordo com o teor da proposição, poderá ser necessário o encaminhamento para deliberação por parte do Comitê de Segurança da Informação e Proteção de Dados ou comunicação a outras áreas (internas e externas).	
Entradas	RISI preenchido com todas as informações	
Saídas	RISI com análise crítica do tratamento do incidente	
Atividades	**Analisar causa-raiz do incidente**	Analisar o cenário do incidente, identificando a causa-raiz, quais as vulnerabilidades exploradas, quais as ameaças envolvidas, etc;
	Propor melhorias no cenário investigado	De posse da análise realizada, propor ações de melhoria para o cenário analisado, de forma a evitar, ou diminuir o risco de, que o incidente volte a ocorrer.
Ferramentas	RISI - Relatório de Incidente de Segurança da Informação	

Encerrar Crise Cibernética		
Descrição	Caberá ao Comitê de Segurança da Informação e Proteção de Dados definir o encerramento da atividade do Protocolo de Gerenciamento de Crises Cibernéticas quando esse houver sido instaurado no tratamento do incidente.	
Papéis	Comitê de Segurança da informação e Proteção de Dados	
Considerações importantes	N/A	
Entradas	RISI e propostas de melhorias do ETIR	
Saídas	RISI e parecer	
Atividades	**Avaliar as propostas**	Avaliar e emitir parecer sobre as propostas de melhorias emitidas pela ETIR.
	Encerrar a Crise Cibernética	Realizar o encerramento do estado de Crise Cibernética, conforme Protocolo de Gerenciamento de Crises Cibernéticas
Ferramentas	N/A	

Encerrar o incidente		
Descrição	Nesta atividade devem ser encerradas todas as atividades relacionadas ao incidente específico, desde que sanadas quaisquer pendências.	
Papéis	ETIR	
Considerações importantes	N/A	
Entradas	RISI e deliberação do comitê	
Saídas	RISI preenchido e encerrado Notificação ao CTIR.BR, quando necessário	
Atividades	**Cumprir providências**	Dar prosseguimento nas deliberações e ações definidas pelo Comitê de Segurança da Informação e Proteção de Dados ou pela ETIR.
	Encerrar o incidente	Inexistindo pendências, o incidente deve ser encerrado.
	Notificar o incidente ao CTIR.BR	Quando necessário, o incidente deverá ser informado ao CTIR.BR, utilizando-se os procedimentos definidos pelo CTIR.BR (ver documento NOTIFICAÇÃO CTIR-Procedimentos)
Ferramentas	N/A	

Encaminhar relatório final ao SNCAIC-JT		
Descrição	Após o encerramento do incidente cibernético, o Tribunal encaminhará relatório final ao CSJT contendo a descrição completa do incidente cibernético e as medidas aplicadas para tratá-lo.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Considerações importantes	Conforme processo estabelecido no Ato Conjunto TST.CSJT.GP N.º 41, de 25 de julho de 2025.	
Entradas	RISI preenchido e encerrado	
Saídas	Relatório encaminhado ao CSJT	
Atividades	**Encaminhar relatório ao CSJT**	A CSIPD encaminhará ao CSJT relatório final do incidente,contendo, ao menos, as seguintes informações: I - tratamento realizado; II - medidas preventivas recomendadas; III - lições aprendidas; IV - Análise de causa raiz do incidente; V - Recomendações para prevenção de incidentes futuros.
Ferramentas	RISI - Relatório de Incidente de Segurança da Informação	

Avaliar histórico de incidentes e oportunidades de melhoria		
Descrição	Analisar o tipo e histórico de incidentes, com o intuito de estudar o cenário "macro", de forma a perceber alguma oportunidade de melhoria no processo de gestão de incidentes de SI, bem como sistema ou serviço afetado por um ou mais incidentes.	
Papéis	Coordenadoria de Segurança da Informação e Proteção de Dados	
Considerações importantes	É importante que os RISIs sejam preenchidos de forma mais completa e precisa possível, pois serão utilizados para alimentar os indicadores do processo de gestão de incidentes de SI.	
Entradas	RISI encerrado	
Saídas	Registro de indicadores Ações de melhoria	
Atividades	**Avaliar histórico de incidentes**	Verificar os RISIs anteriores e outras bases (Sistemas de registro de atendimentos, por exemplo) a fim de fazer alguma correlação de incidentes e verificar possíveis gaps em algum processo, sistema ou infraestrutura.
	Alimentar indicadores estabelecidos	Atualizar as informações dos indicadores definidos para o processo.

	Identificar oportunidade de melhoria	Com base na avaliação detectar quais ações poderiam ser executadas a fim de melhorar o processo de gestão de incidentes de SI.
Ferramentas	Diversas	

Implantar melhorias		
Descrição	Planejar e implementar as propostas de melhoria identificadas.	
Papéis	CSIPD Outras áreas da SGTI	
Considerações importantes	N/A	
Entradas	Ações de melhorias	
Saídas	Ações de melhorias	
Atividades	**Implantar melhorias**	Planejar e implementar as melhorias identificadas.
Ferramentas	N/A	