PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO Nº 152/2018

Institui a Equipe e Processo de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO as boas práticas para seleção e implementação de controles de segurança da informação, especialmente a Norma ABNT NBR ISO/IEC 27002;

CONSIDERANDO a necessidade de disciplinar a criação da Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores (ETIR) no âmbito do Tribunal Regional do Trabalho da 7ª Região (TRT7);

CONSIDERANDO a necessidade de estabelecer as diretrizes e o processo de Gestão de Incidentes de Segurança da Informação relacionada ao ambiente tecnológico no âmbito do TRT7;

CONSIDERANDO que o Ato nº 229/2013 desta Corte Norma Complementar de Criação da Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores;

CONSIDERANDO que a Resolução nº 211/2015 do Conselho Nacional de Justiça, estabelece no art. 12 (inciso II, alínea "b") a necessidade de constituir e manter estruturas organizacionais adequadas e compatíveis para o macroprocesso de "incidentes de segurança";

CONSIDERANDO a necessidade de revisão periódica das normas de segurança, nos termos do art. 21 da Resolução TRT7 nº 278/2017,

RESOLVE:

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2571, 28 set. 2018.
Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 1.

Art. 1º Instituir a Norma 03/NC/POSIC para definir a Equipe e o Processo de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região, na forma do Anexo.

Art. 2º Revogar o Ato nº 229/2013.

Art. 3º Este ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
Fortaleza, 27 de setembro de 2018.
PLAUTO CARNEIRO PORTO
Presidente do Tribunal

Tribunal Regional do Trabalho da 7ª Região Secretaria de Tecnologia da Informação Seção de Segurança da Informação	Número da Norma Complementar	Revisão	Emissão	Folhas
	03/NC/POSIC	2	00/00/00	0
	Equipe e Processo de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região			

ORIGEM

NÚCLEO DE APOIO À GESTÃO DE TIC E SEGURANÇA DA INFORMAÇÃO

CAMPO DE APLICAÇÃO

Esta Norma Complementar se aplica ao âmbito do Tribunal Regional do Trabalho da 7ª Região.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2571, 28 set. 2018.
Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 1.

Tribunal Regional do Trabalho da 7ª Região Secretaria de Tecnologia da Informação Seção de Segurança da Informação	Número da Norma Complementar	Revisão	Emissão	Folhas
	03/NC/POSIC	2	00/00/00	0
	Equipe e Processo de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região			

1. OBJETIVOS

1.1. Disciplinar a criação da Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores (ETIR) no âmbito do Tribunal Regional do Trabalho da 7ª Região (TRT7).

1.2. Estabelecer as diretrizes e o processo de Gestão de Incidentes de Segurança da Informação relacionada ao ambiente tecnológico no âmbito do TRT7.

2. MOTIVAÇÕES

2.1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à Gestão de Incidentes de Segurança da Informação.

2.2. Necessidade de formalização da ETIR e seu funcionamento.

2.3. Garantir o cumprimento da missão institucional do TRT7 através da solução dos incidentes de segurança da informação na rede interna de computadores.

3. FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

3.1. **Norma ABNT NBR ISO/IEC 27001:2005,** que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização.

3.2. **Norma ABNT NBR ISO/IEC 27002:2005,** que trata de Código de Pratica para a gestão da Segurança da Informação.

3.3. **Decreto nº 3.505**, de 13 de junho de 2000, que "*Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal*";

3.4. **Resolução nº 211**, de 15 de dezembro de 2015, do Conselho Nacional de Justiça, estabelece no Art. 12 (inciso II, alínea "b") a necessidade de constituir e manter estruturas organizacionais adequadas e compatíveis para o macroprocesso de "incidentes de segurança";

3.5. **Instrução Normativa GSI/PR nº 01,** do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que estabelece "critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta";

3.6. **Norma Complementar 05/IN01/DSIC/GSIPR,** do Gabinete de Segurança Institucional da Presidência da República, de 17 de agosto de 2009, que "disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal";

3.7. **Norma Complementar 08/IN01/DSIC/GSIPR,** do Gabinete de Segurança Institucional da Presidência da República, de 24 de agosto de 2010, que "estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal";

3.8. **Norma Complementar 21/IN01/DSIC/GSIPR,** do Gabinete de Segurança Institucional da Presidência da República, de 10 de outubro de 2014, que "estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta".

3.9. **Resolução n. 278/2017,** da Presidência do TRT da 7ª Região, que institui a Política de Segurança da Informação e Comunicações (POSIC) no âmbito deste Tribunal, que determina no Art. 11 "Norma complementar definirá a composição e detalhamento das competências da ETIR".

4. CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições, em adição aos definidos na Resolução TRT7 n. 278/2017:

4.1. **Incidente de segurança:** é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de

computadores, tais como: divulgação não autorizada de dados ou informação sigilosa contida em sistema, arquivo ou base de dados deste Tribunal; invasão de dispositivo informático; interrupção de serviço essencial ao desempenho das atividades; inserção ou facilitação de inserção de dados falsos, alteração ou exclusão de dados corretos nos sistemas informatizados ou bancos de dados deste Tribunal e/ou prática de ato definido como crime ou infração administrativa.

4.2. **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR**: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores, como parte da estrutura de gestão da segurança da informação, prevista no Art. 8º, inciso V, da Resolução TRT7 n. 278/2017 (POSIC);

5. MODELO DE IMPLEMENTAÇÃO

5.1. Para a formação e implementação da ETIR, o modelo a ser utilizado é o que utiliza a própria equipe de Tecnologia da Informação (TI). A equipe será formada a partir dos membros das unidades vinculadas à Secretaria de Tecnologia da Informação e Comunicação (SETIC), que além de suas funções regulares passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes de segurança na rede de computadores interna do TRT7.

5.2. A Equipe desempenhará suas atividades, via de regra, de forma reativa. Porém, é desejável a atribuição de responsabilidades para que os seus membros exerçam atividades proativas.

5.3. O tratamento da informação deve ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.

5.4. O processo de Gestão de Incidentes de Segurança da Informação tem como principal objetivo identificar, registrar e avaliar tecnicamente em tempo hábil os

incidentes de segurança da informação, para que seja possível a tomada de medidas de contenção e/ou solução adequadas.

5.5. A Gestão de Incidentes de Segurança da Informação abrangida por essa norma está limitada aos eventos, confirmados ou suspeitos, relacionados à segurança de sistemas ou redes computacionais, que comprometam o ambiente tecnológico do TRT, seus ativos, informações e processos de negócio, bem como aqueles que contrariem a POSIC deste Tribunal.

6. ESTRUTURA ORGANIZACIONAL DA ETIR

6.1. A ETIR deve ser composta por servidores públicos ocupantes de cargo efetivo de carreira, com perfil técnico compatível, e deverá ser vinculada ao Núcleo de Apoio à Gestão de TIC e Segurança da Informação (NGTIC).

6.2. Recomenda-se que os membros da ETIR sejam: administradores de sistema ou de segurança, administradores de banco de dados, administradores de rede ou analistas de suporte.

6.3. A ETIR tem plena autonomia para tomada de decisão sobre quais medidas serão adotadas e poderá conduzir o público alvo para realizar ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança na rede interna de computadores. Durante um incidente de segurança, se justificável, a equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

6.4. A ETIR será composta por:

6.4.1. 1 (um) servidor da DITIC;

6.4.2. 1 (um) servidor da DSSUTIC;

6.4.3. 1 (um) servidor da DSTIC;

6.4.4. 1(um) servidor do NGTIC;

6.5. Para cada membro da Equipe deverá ser designado um substituto que deverá ser treinado e orientado para a realização das tarefas e atividades da ETIR.

6.6. Portaria da SETIC indicará o nome dos servidores titulares e substitutos que irão compor a ETIR.

7. RESPONSABILIDADES

7.1. Cabe à ETIR:

7.1.1. Executar o Processo de Gestão de Incidentes de Segurança da Informação do TRT7;

7.1.2. Guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de segurança em rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR GOV).

7.1.3. Registrar de forma detalhada a comunicação de ocorrência ou suspeita de incidente de segurança da informação na rede de computadores do TRT7;

7.1.4. Investigar, em conjunto com as demais áreas da SETIC, com base nas informações registradas, as possíveis causas, extensão e impacto do incidente;

7.1.5. Recolher evidências o quanto antes após a comunicação de ocorrência de um incidente de Segurança da Informação e Comunicações na rede interna de computadores;

7.1.6. Comunicar às partes interessadas sobre ocorrência, extensão, impacto, resultados do tratamento e encerramento do incidente;

7.1.7. Consolidar as ocorrências de incidentes comunicados pelos usuários por meio de relatórios de Incidentes de Segurança da Informação;

7.1.8. Propor e acompanhar a execução das ações de contenção do incidente;

7.1.9. Executar as ações de contenção do incidente, quando no âmbito da área técnica a que pertencem;

7.1.10. Executar uma análise crítica sobre os registros de falhas para assegurar que elas foram satisfatoriamente resolvidas;

7.1.11. Implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento;

7.1.12. Indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes.

7.1.13. A ETIR deverá comunicar de imediato a ocorrência de todos os incidentes de segurança, possíveis de serem notificados, ocorridos na sua área de atuação ao CTIR GOV, conforme padrão definido por esse Órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.

7.2. Cabe ao NGTIC:

7.2.1. No âmbito de suas atribuições, cabe ao Coordenador do NGTIC o papel de Agente Responsável pela ETIR, além de ser a interface com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR GOV).

7.2.2. Desenvolver, testar e implementar o processo de Gestão de Incidentes de Segurança da Informação e garantir sua efetividade;

7.2.3. Coordenar a instituição, capacitação, implementação e manutenção da infraestrutura necessária à ETIR.

7.2.4. Criar os procedimentos internos, gerenciar as atividades e distribuir tarefas para a ETIR.

7.2.5. Garantir que os incidentes de segurança na Rede de Computadores do TRT7 sejam monitorados;

7.2.6. Adotar procedimentos de *feedback* para assegurar que os usuários que comuniquem incidentes de segurança da informação e comunicações na rede interna de computadores sejam informados dos procedimentos adotados;

7.2.7. Apoiar o TRT7 nas atividades de capacitação e tratamento de incidentes de segurança em sua rede de computadores.

7.2.8. Disseminar cultura voltada para comunicação de incidentes de segurança da informação.

7.2.9. Atuar como instância consultiva da Administração do Tribunal nas questões relativas a incidentes de segurança da informação;

7.2.10. Subsidiar o Comitê Gestor de Segurança da Informação com informações pertinentes à estrutura de gestão de incidentes de segurança da informação;

7.3. Cabe às unidades vinculadas à SETIC:

7.3.1. Monitorar e comunicar os Incidentes de Segurança da Informação dos ativos sob sua responsabilidade;

7.3.2. Assegurar a implementação das ações e dos controles definidos para contenção e prevenção de incidentes de segurança da informação dos ativos sob sua responsabilidade.

7.4. Cabe ao Comitê Gestor de Segurança da Informação:

7.4.1. Deliberar sobre as principais diretrizes e temas relacionados à Gestão de Incidentes de Segurança da Informação;

7.4.2. Monitorar e avaliar periodicamente a estrutura de Gestão de Incidentes de Segurança da Informação e o sistema de controles internos, assim como propor melhorias consideradas necessárias;

7.4.3. Aprovar formalmente o processo de Gestão de Incidentes de Segurança da Informação e suas futuras revisões;

7.4.4. Deliberar sobre ações de contenção ou prevenção de incidentes de segurança da informação;

7.4.5. Aprovar os critérios de encaminhamento do RISI para aprovação superior;

7.4.6. Monitorar e analisar periodicamente a implementação do Plano juntamente com a ETRI.

7.5. Cabe à Presidência:

7.5.1. Analisar as deliberações do Comitê Gestor de Segurança da Informação sobre Gestão de Incidentes de Segurança da Informação e decidir sobre possíveis providências;

7.5.2. Formalizar a aceitação da execução das ações propostas para conter ou prevenir incidentes de segurança da informação.

8. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O processo de Gestão de Incidentes de Segurança da Informação é contínuo e integra o Sistema de Gestão de Segurança da Informação (SGSI).

8.1. O processo de Gestão de Incidentes de Segurança da Informação é abordado no **Anexo A** desta Norma e composto pelas seguintes etapas:

8.1.1. Detecção e registro: inclui desde o recebimento e registro do incidente de segurança da informação até a obtenção das autorizações necessárias para o prosseguimento das investigações;

8.1.2. Investigação e contenção: inclui atividades de investigação, coleta de evidências, proposições de ações de contenção e/ou solução, comunicação às áreas afetadas, além da obtenção das autorizações

para o prosseguimento da aplicação das ações propostas, quando necessárias;

8.1.3. Encerramento: compreende a análise do incidente com o objetivo de verificar a necessidade de propor outras providências necessárias ao encerramento do incidente;

8.1.4. Avaliação: compreende a avaliação do histórico de incidentes, além da verificação e implantação de melhorias no processo.

8.2. Quando o incidente de segurança da informação decorrer de suspeita de descumprimento da Política de Segurança da Informação, será observado o sigilo durante todo o processo, ficando as evidências, informações e demais registros restritos aos envolvidos na investigação.

8.3. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, o Comitê Gestor de Segurança da Informação e a Administração do TRT deverão ser comunicados, para avaliação das providências cabíveis.

9. VIGÊNCIA E REVISÃO

9.1. Esta norma deverá ser revisada e atualizada periodicamente, no máximo, a cada três anos.

9.2. Esta Norma Complementar entra em vigor na data de sua publicação.

ANEXO A

PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2571, 28 set. 2018.
Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 1.

Índice

1. INTRODUÇÃO

A informação constantemente tratada no âmbito do TRT7 é um ativo de fundamental importância. Por ser valiosa, é também ameaçada e deve ser protegida.

Quando se suspeita ou confirma que uma informação ou ativo de informação teve sua integridade, confidencialidade ou disponibilidade comprometida, temos um incidente de segurança da informação.

São exemplos de incidentes de segurança da informação: qualquer tipo de indício de fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar a segurança da informação.

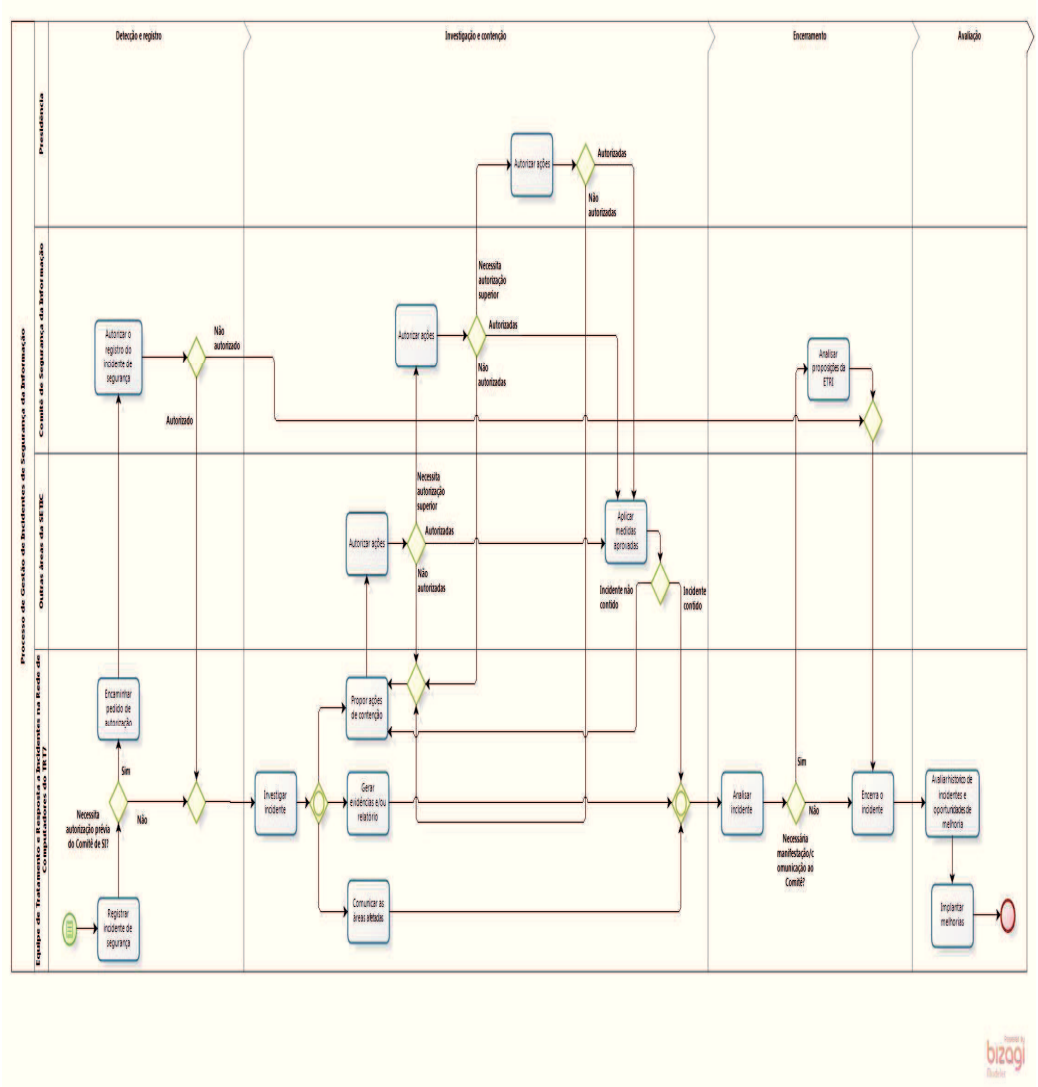
Desse modo, a Gestão de Incidentes de Segurança da Informação, que é um dos processos do Sistema de Gestão de Segurança da Informação(SGSI), objetiva-se a dotar o Tribunal de ferramenta eficaz no intuito de assegurar que fragilidades e incidentes em segurança da informação sejam identificados, para permitir a tomada de ação corretiva em tempo hábil.

2. PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O processo do TRT7 está baseado nas definições constantes nas normas técnicas ABNT NBR ISO/IEC 27002:2005, Norma Complementar 08/IN01/DSIC/GSIPR, Norma Complementar 21/IN01/DSIC/GSIPR, NSI008 - Gestão de Incidentes de Segurança da Informação do TRT da 4ª Região e consiste nas seguintes etapas:

- Detecção e registro;
- Investigação e contenção;
- Encerramento;
- Avaliação;

Tribunal Regional do Trabalho da 7ª Região Secretaria de Tecnologia da Informação e Comunicação	Número da Norma Complementar	Revisão	Emissão	Folhas
	03/NC/POSIC	2	00/00/00	0
	ANEXO A Processo de Gestão de Incidentes de Segurança da Informação			



2.1. Registrar incidente de segurança

A comunicação de ocorrência ou suspeita de incidente de segurança da informação pode ser feita por qualquer magistrado, servidor, estagiário ou colaborador por meios dos seguintes canais:

a) Registro na Central de Serviços de TIC, disponível na intranet (https://centraldeservicos.trt7.jus.br) ou;

b) Diretamente ao Gabinete da SETIC: pelo e-mail setic@trt7.jus.br, telefone ou pessoalmente, ou ainda;

c) Diretamente à equipe responsável pelo tratamento de incidentes de segurança: pelo e-mail etir@trt7.jus.br;

O processo é iniciado com o registro de forma detalhada, feito pela ETIR em formulário próprio, da comunicação de ocorrência ou suspeita de incidente de segurança da informação na rede de computadores do TRT7.

Feito isso, a ETIR verifica a necessidade de autorização prévia do Comitê Gestor de Segurança da Informação para prosseguimento.

Registrar incidente de segurança	
Objetivo:	Registrar de forma detalhada, em formulário próprio disponível na intranet, a comunicação de ocorrência ou suspeita de incidente de segurança da informação na rede de computadores do TRT7. Além disso, verifica a necessidade de autorização prévia do Comitê Gestor de Segurança da Informação para prosseguimento.
Responsável:	ETIR
Entrada:	Comunicação da suspeita ou ocorrência de incidente de segurança da informação.
Ação:	• Receber comunicação sobre o incidente; • Entrar em contato com os usuários para solicitar esclarecimentos, quando necessário; • Registrar o incidente (preencher o formulário);

	• Verificar necessidade de autorização prévia do Comitê Gestor de SI.
Saída:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações iniciais.

2.2. Encaminhar pedido de autorização

A ETIR tem plena autonomia para decidir pela continuidade da análise ou não do possível incidente de segurança, porém caso entenda necessário poderá comunicar ou solicitar autorização ao Comitê Gestor de Segurança da Informação para o prosseguimento da investigação

Investigar incidente	
Objetivo:	Solicitar autorização ao Comitê Gestor de Segurança da Informação para o prosseguimento da investigação (opcional)
Responsável:	ETIR
Entrada:	Comunicação da suspeita ou ocorrência de incidente de segurança da informação.
Ação:	• Coletar as informações necessárias ao encaminhamento do pedido de autorização; • Encaminhar pedido de autorização ao Comitê Gestor de SI; • Prestar esclarecimentos, quando necessário.
Saída:	• Pedido de autorização ao Comitê Gestor de Segurança da Informação; • Relatório de Incidente de Segurança da Informação (RISI) preenchido com as informações iniciais.

2.3. Autorizar o registro de incidente de segurança

O Comitê Gestor de Segurança da Informação analisa o pedido de autorização para prosseguimento da investigação do provável incidente de segurança.

Autorizar o registro de incidente de segurança	
Objetivo:	Analisar o pedido de autorização para prosseguimento da investigação do provável incidente de segurança.
Responsável:	Comitê Gestor de Segurança da Informação.
Entrada:	• Pedido de autorização ao Comitê Gestor de Segurança da Informação; • Relatório de Incidente de Segurança da Informação (RISI) preenchido com as informações iniciais.
Ação:	• Analisar informações fornecidas no RISI; • Pedir esclarecimentos à Equipe de Tratamento e Resposta à Incidentes, quando necessário; • Autorizar e encaminhar para investigação ou negar e encaminhar para encerramento.
Saída:	Autorização para prosseguimento da investigação.

2.4. Investigar incidente

A Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI), com base nas informações registradas, investiga as possíveis causas, extensão e impacto do incidente, a fim de subsidiar as decisões e ações para sua contenção ou encaminhamento.

Investigar incidente	
Objetivo:	Investigar, com base nas informações registradas, as possíveis causas, extensão e impacto do incidente, a fim de subsidiar as decisões e ações para sua contenção ou encaminhamento.
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações iniciais ou autorização do Comitê Gestor de Segurança da Informação.
Ação:	• Verificar o tipo de incidente, tal como: acesso indevido, descumprimento da Política de Segurança da Informação, indisponibilidade de serviços ou sistemas por falha de segurança, invasão, propagação de vírus, vazamento de dados, etc.;

	• Solicitar informações às áreas técnicas responsáveis; Analisar a extensão e o impacto causado pelo incidente.
Saída:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações do incidente investigado.

2.5. Propor ações de contenção

A Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI), com base nas informações levantadas durante a fase de investigação, propõe ações para conter o incidente. Essas ações podem ser soluções de contorno ou de resolução do problema. Além disso, devem evitar que os danos e impactos aumentem com o passar do tempo.

Autorizar o registro de incidente de segurança	
Objetivo:	Propor, com base nas informações levantadas durante a fase de investigação, ações para conter o incidente. Essas ações podem ser soluções de contorno ou de resolução do problema. Além disso, devem evitar que os danos e impactos aumentem com o passar do tempo.
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações do incidente investigado.
Ação:	• Propor ações de contenção; • Encaminhar solução para aprovação da chefia; • Propor novas medidas de contenção, caso o incidente não seja contido pelas medidas propostas inicialmente.
Saída:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção propostas.

2.6. Coletar evidências e/ou gerar relatório

Quando necessário, a Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) realiza auditoria em sistemas e serviços com o objetivo de coletar evidências e/ou gerar relatórios, tais como relatórios de logs de acesso.

Coletar evidências e/ou gerar relatório	
Objetivo:	Realizar, quando necessário, auditoria em sistemas e serviços com o objetivo de coletar evidências e/ou gerar relatórios, tais como relatórios de logs de acesso.
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações do incidente investigado.
Ação:	• Identificar dados necessários para elucidação do incidente; • Realizar a coleta e compilação dos dados.
Saída:	Evidências e/ou relatório.

2.7. Comunicar as áreas afetadas

Quando necessário, a Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) comunica às áreas da SETIC sobre a ocorrência, extensão e impacto do incidente e, em conjunto com o NGTIC, delibera se é necessário informar outras áreas do TRT sobre o incidente.

Comunicar as áreas afetadas

Objetivo:	Comunicar, quando necessário, as áreas da SETIC sobre a ocorrência, extensão e impacto do incidente e, em conjunto com o NGTIC, delibera se é necessário informar outras áreas do TRT sobre o incidente.
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações do incidente investigado.
Ação:	• Informar a ocorrência, extensão e impacto, além de quais sistemas/serviços foram afetados; • Definir como e a quem a comunicação será realizada.
Saída:	• Comunicação interna; • Pedido à Direção da SETIC para realização de comunicação externa (áreas afetadas), quando necessário; • Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações sobre o plano de comunicações.

2.8. Referendar ações

O Diretor da SETIC analisa as ações de contenção propostas pela Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) para decidir se dá prosseguimento aos esforços de execução das ações. Em alguns casos, pode ser necessário o envio do Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção para análise do Comitê Gestor de Segurança da Informação.

Referendar ações	
Objetivo:	Analisar as ações de contenção propostas pela Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) para decidir se dá prosseguimento aos esforços de execução das ações. Em alguns casos, pode ser necessário o envio do Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção para análise do Comitê

	de Segurança da Informação.
Responsável:	Diretor da Secretaria de Tecnologia da Informação e Comunicação (SETIC).
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção propostas.
Ação:	• Analisar informações fornecidas no Formulário de registro de incidentes; • Pedir esclarecimentos à Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI), quando necessário; Autorizar a execução e encaminhar para o setor responsável ou encaminhar para aprovação superior ou negar a execução e encaminhar para encerramento do incidente.
Saída:	Autorização de execução ou encaminhamento para aprovação superior ou encaminhamento para encerramento do incidente.

2.9. Analisar ações

O Comitê de Segurança da Informação analisa as ações de contenção propostas pela Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) para decidir se dá prosseguimento aos esforços de execução das ações. Em alguns casos, pode ser necessário o envio do formulário de registro de incidentes para análise da Presidência do Tribunal.

Analisar ações	
Objetivo:	Analisar as ações de contenção propostas pela Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) para decidir se dá prosseguimento aos esforços de execução das ações. Em alguns casos, pode ser necessário o envio do formulário de registro de incidentes para análise da Presidência do Tribunal.
Responsável:	Comitê Gestor de Segurança da Informação.

Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção propostas.
Ação:	• Analisar informações fornecidas no Formulário de registro de incidentes; • Pedir esclarecimentos ao Diretor da SETIC e/ou à Equipe de Tratamento e Resposta à Incidentes, quando necessário; • Autorizar a execução e encaminhar para o setor responsável ou encaminhar para aprovação superior ou negar a execução e encaminhar para encerramento do incidente.
Saída:	Autorização de execução ou encaminhamento para aprovação superior ou encaminhamento para encerramento do incidente.

2.10. Autorizar ações

A Presidência do TRT7 analisa as ações de contenção propostas pela Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) para decidir se dá prosseguimento aos esforços de execução das ações.

Autorizar ações	
Objetivo:	Analisar as ações de contenção propostas pela Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) para decidir se dá prosseguimento aos esforços de execução das ações.
Responsável:	Presidência do TRT7.
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção propostas.
Ação:	• Analisar informações fornecidas no Formulário de registro de incidentes; • Pedir esclarecimentos ao Diretor da SETIC (representante do Comitê de Segurança da Informação), quando necessário; • Autorizar a execução e encaminhar para o setor responsável ou negar a

	execução e encaminhar para encerramento do incidente.
Saída:	Autorização de execução ou encaminhamento para encerramento do incidente.

2.11. Aplicar medidas aprovadas

O setor da SETIC responsável executa as ações propostas na fase anterior visando conter o incidente. Após aplicar as medidas, avalia se o resultado esperado foi alcançado e, em caso negativo, encaminha o RISI preenchido com os resultados nas medidas aplicadas para a ETRI.

Aplicar medidas aprovadas	
Objetivo:	Executar as ações propostas na fase anterior visando conter o incidente. Após aplicar as medidas, avalia se o resultado esperado foi alcançado e, em caso negativo, encaminha o RISI preenchido com os resultados nas medidas aplicadas para a ETRI.
Responsável:	Outras áreas da SETC.
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com ações de contenção propostas.
Ação:	• Aplicar medidas necessárias; • Avaliar medidas aplicadas; • Encaminhar resultados para ETRI ou encaminhar para encerramento do incidente.
Saída:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com resultado das medidas aplicadas.

2.12. Analisar incidente

A ETIR analisa o incidente como um todo (causa raiz, ações de contenção aplicadas, danos, por exemplo), a fim de propor outras providências necessárias ao encerramento do incidente (medidas de solução). Se for o caso de uma investigação (suspeita de violação da Política de Segurança da Informação), a ETIR deverá elaborar relatórios de acesso com base na análise de ferramentas e logs disponíveis a fim de elucidar a suspeita, apresentando suas conclusões ao Comitê Gestor de Segurança da Informação.

Analisar incidente	
Objetivo:	Analisar o incidente como um todo (causa raiz, ações de contenção aplicadas, resultados dos relatórios elaborados etc), a fim de propor outras providências necessárias ao encerramento do incidente (medidas de solução). Se for o caso de uma investigação (suspeita de violação da Política de Segurança da Informação), a ETRI deverá elaborar relatórios de acesso com base na análise de ferramentas e logs disponíveis a fim de elucidar a suspeita, apresentando suas conclusões ao Comitê de Segurança da Informação.
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com resultado das medidas aplicadas.
Ação:	• Analisar causa-raiz do incidente; • Propor melhorias no cenário investigado para evitar que o incidente volte a acontecer; • No caso de uma investigação de acessos, analisar logs e utilizar ferramentas de auditoria para elucidar a suspeita e encaminhar o relatório à apreciação do Comitê de Segurança da Informação.
Saída:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com propostas de ações para encerramento do incidente.

2.13. Analisar proposições da ETIR

O Comitê de Segurança da Informação avalia as soluções propostas ou o relatório de auditoria enviado pela ETRI e encaminha o incidente para encerramento.

Analisar proposições da ETRI	
Objetivo:	Avaliar as soluções propostas ou o relatório de auditoria enviado pela ETRI e encaminha o incidente para encerramento.
Responsável:	Comitê Gestor de Segurança da Informação
Entrada:	Formulário de registro de incidentes preenchido com providências necessárias ao encerramento do incidente ou relatório de auditoria encaminhado pela ETIR.
Ação:	• Tomar ciência do incidente e medidas aplicadas • Avaliar soluções propostas • Analisar relatório de auditoria
Saída:	Encaminhamento do Comitê de Segurança da Informação.

2.14. Encerrar o incidente

A ETIR verifica providências ou determinações pendentes e promove sua execução, além de comunicar os resultados do tratamento e encerramento para o usuário que informou o incidente. Feito isso, o incidente de segurança da informação será considerado encerrado. Quando necessário, a ETIR deve notificar o incidente ao CTIR.BR, utilizando-se os procedimentos definidos pelo CTIR Gov.

Encerrar o incidente

Objetivo:	Verificar providências ou determinações pendentes e promove sua execução, além de comunicar os resultados do tratamento e encerramento para o usuário que informou o incidente. Feito isso, o incidente de segurança da informação será considerado encerrado.
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com propostas de ações para encerramento do incidente e, quando couber, deliberação do Comitê de Segurança da Informação.
Ação:	• Cumprir providências e determinações; • Encerrar o incidente; • Quando necessário, notificar o incidente ao CTIR.BR, utilizando-se os procedimentos definidos pelo CTIR Gov.
Saída:	Relatório de Incidente de Segurança da Informação (RISI) preenchido e encerrado.

2.15. Avaliar histórico de incidentes e oportunidades de melhoria

A Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) analisa o histórico de incidentes de forma a perceber alguma oportunidade de melhoria no processo de gestão de incidentes de segurança da informação, bem como sistema ou serviço afetado por um ou mais incidentes.

Avaliar histórico de incidentes e oportunidades de melhoria	
Objetivo:	Analisar o histórico de incidentes de forma a perceber alguma oportunidade de melhoria no processo de gestão de incidentes de segurança da informação, bem como sistema ou serviço afetado por um ou mais incidentes.
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido e encerrado.

Ação:	• Avaliar histórico de incidentes; • Alimentar indicadores estabelecidos, se houver; • Identificar oportunidade de melhoria.
Saída:	Registro de indicadores/histórico de incidentes.

2.16. Implantar melhorias

A Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores do TRT7 (ETRI) planeja e implanta as propostas de melhorias identificadas na atividade anterior.

Implantar melhorias	
Objetivo:	Planejar e implantar as propostas de melhorias identificadas na atividade anterior.
Responsável:	ETIR
Entrada:	Registro de indicadores/histórico de incidentes.
Ação:	• Implantar melhorias.
Saída:	Ações de melhorias.