PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO TRT7.GP Nº 144, DE 24 DE SETEMBRO DE 2021

Institui o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário no âmbito do Tribunal Regional do Trabalho da 7ª Região (TRT7).

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

CONSIDERANDO a Resolução nº 396, de 07 de junho de 2021, do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o anexo I da Portaria nº 162, de 10 de junho de 2021, do Conselho Nacional de Justiça, que constitui o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ);

CONSIDERANDO os anexos IV, V e VI da Portaria nº 162/2021, do Conselho Nacional de Justiça, que contêm os manuais referentes à Proteção de Infraestruturas Críticas de TIC, Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, e, ainda, Gestão de Identidades;

CONSIDERANDO a Resolução Normativa nº 14, de 22 de junho de 2020 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 Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR)”;

CONSIDERANDO a 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";

CONSIDERANDO a 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";

CONSIDERANDO a 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;

CONSIDERANDO a Norma ABNT NBR ISO/IEC 27002:2005, que trata de Código de Prática para a Gestão da Segurança da Informação;

CONSIDERANDO o Decreto nº 9.637, de 26 de dezembro de 2018, que "Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação",

RESOLVE:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Adotar o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ), no âmbito do TRT7, com os seguintes objetivos:

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

II - promover alinhamento às normas, regulamentações e às melhores práticas, relacionadas à Gestão de Incidentes de Segurança da Informação;

III - promover ações que contribuam para a resiliência dos serviços de Tecnologia da Informação e Comunicação (TIC) aos ataques cibernéticos.

Art. 2º Os Protocolos de Investigação para Ilícitos Cibernéticos e para Gerenciamento de Crises Cibernéticas são complementares e harmonizam-se com este protocolo de Prevenção a Incidentes Cibernéticos.

Parágrafo único. Para os efeitos deste normativo, são estabelecidas as seguintes definições:

I - Incidente cibernético ou 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 de 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;

II - 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.

Art. 3º Para implementação desta norma, deverão ser observados pelas áreas envolvidas os princípios críticos definidos no PPINC-PJ, que são:

I - uso de base de conhecimento de defesa;

II - priorização da segurança da informação;

III - definição e estabelecimento de métricas;

IV - diagnóstico contínuo;

V - formação e capacitação;

VI - busca de soluções automatizadas de segurança cibernética;

VII - resiliência.

Art. 4º Fica instituída a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) do TRT da 7ª Região, com a missão, ação e as competências de acordo com o Anexo A.

Art. 5º Cabe ao Comitê Gestor de Segurança da Informação:

I - deliberar sobre as principais diretrizes e temas relacionados à Gestão de Incidentes de Segurança da Informação;

II - 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;

III - aprovar formalmente o processo de Gestão de Incidentes de Segurança da Informação e suas futuras revisões;

IV - deliberar sobre ações de contenção ou prevenção de incidentes de segurança da informação.

Art. 6º Cabe à Presidência:

I - analisar as deliberações do Comitê Gestor de Segurança da Informação sobre Gestão de Incidentes de Segurança da Informação e decidir sobre possíveis providências;

II - formalizar a aceitação da execução das ações propostas para conter ou prevenir incidentes de segurança da informação;

III - comunicar ao órgão de polícia judiciária com atribuição para apurar os fatos, na ocorrência de incidentes penalmente relevantes;

IV - acionar o Comitê de Crises Cibernéticas, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas, quando necessário.

Art. 7º Cabe às unidades vinculadas à Secretaria de Tecnologia da Informação e Comunicação (SETIC):

I - monitorar e comunicar à ETIR os Incidentes de segurança da informação dos ativos sob sua responsabilidade;

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

Art. 8º Cabe ao Gabinete de Segurança da Informação (GSI):

I - desenvolver, testar e implementar o processo de Gestão de Incidentes de Segurança da Informação e garantir sua efetividade;

II - coordenar a instituição, capacitação, implementação e manutenção da infraestrutura necessária à ETIR;

III - gerenciar as atividades e distribuir tarefas para a ETIR;

IV - garantir que os incidentes de segurança na Rede de Computadores do TRT7 sejam devidamente tratados;

V - 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;

VI - disseminar cultura voltada para comunicação de incidentes de segurança da informação;

VII - atuar como instância consultiva da Administração do Tribunal nas questões relativas a incidentes de segurança da informação;

VIII - subsidiar o Comitê Gestor de Segurança da Informação com informações pertinentes à estrutura de gestão de incidentes de segurança da informação.

Parágrafo único. Cabe ao Chefe do GSI 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).

CAPÍTULO II
DAS FUNÇÕES DO PROTOCOLO DE PREVENÇÃO A INCIDENTES CIBERNÉTICOS

Art. 9º São funções básicas do Protocolo de Prevenção a Incidentes Cibernéticos, conforme definição do PPINC-PJ, identificar, detectar, responder o incidente, proteger e recuperar a informação.

Seção I
Da Função Identificar

Art. 10. A função "Identificar" consiste na análise dos riscos a que os recursos de TIC estão expostos, incluindo a elaboração e a execução do plano de tratamento dos riscos.

§ 1º A função identificar é executada dentro do escopo do processo de Gestão de Riscos de Segurança da Informação, instituído em ato próprio, e está limitada aos ativos incluídos no respectivo ciclo de análise de riscos no âmbito do TRT7.

§ 2º O mesmo tratamento previsto no parágrafo § 1º deste artigo deve ser dispensado a ativos considerados relevantes, mesmo que não estejam diretamente relacionados à sustentação dos serviços críticos, que poderiam ser ponto de entrada para a exploração de falhas.

§ 3º O rol de atividades de TIC consideradas essenciais, para fins deste normativo, é o mesmo constante no ciclo de análise de riscos vigente.

Seção II
Da Função Proteger

Art. 11. A função "Proteger" consiste no desenvolvimento e na implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, ativos de informação e a prestação de serviços.

§ 1º A função "Proteger" deve ser implementada pelo conjunto mínimo de ações elencadas a seguir:

I - aprimoramento contínuo do Sistema de Gestão de Segurança da Informação (SGSI) do TRT7;

II - controle de acesso e de utilização de recursos de TIC;

III - cópia de segurança e de restauração de sistemas, aplicativos, dados e de documentos;

IV - plano de contingência dos serviços essenciais;

V - gestão de capacidade e disponibilidade de TIC dos serviços essenciais;

VI - processo de gerenciamento de mudanças para todos os ativos de TIC;

VII - gestão de vulnerabilidades técnicas dos serviços essenciais;

VIII - utilização de ferramenta de segurança para estações de trabalho, contendo, no mínimo, as funções de antivírus, automação de políticas de segurança de endpoint, proteção contra criptografia (ransomware), controle de aplicativos e de dispositivos removíveis;

IX - controle de acesso a conteúdo na *internet* (filtragem web);

X - utilização de ferramentas de segurança de rede (firewall), para filtragem e bloqueio de tráfego de rede, prevenção de ameaças e implementação de redes privadas virtuais (VPN);

XI - integridade da rede protegida por meio da segmentação e segregação de ambientes, de maneira a estabelecer barreiras de contenção de danos em caso de comprometimento (sub-redes distintas por serviços) e para garantia de recursos para serviços prioritários (missão crítica, em detrimento de ambientes de laboratório/desenvolvimento/homologação);

XII - anualmente promover campanha e/ou treinamento sobre segurança da informação para magistrados e servidores;

XIII - atualização tecnológica constante;

XIV - implementação gradual dos controles de segurança da informação presentes na Norma NBR 27002;

XV - implementação gradual dos controles mínimos recomendados no Manual de Referência para Proteção de Infraestruturas Críticas de TIC, editado pelo Conselho Nacional de Justiça, considerando a escala de aplicabilidade de cada controle em relação ao porte e maturidade do TRT7 em segurança da informação;

XVI - implementação gradual dos requisitos de resiliência cibernética recomendados no Manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital, editado pelo Conselho Nacional de Justiça, considerando a aplicabilidade dos requisitos em relação ao porte e maturidade do TRT7 em segurança da informação.

§ 2º As salvaguardas elencadas no § 1º deste artigo devem ser implementadas para todos os ativos de TIC, no que couber, considerados essenciais ou não ao negócio, permitindo variar quanto ao nível de implementação, de acordo com a natureza e criticidade do ativo.

§ 3º As atualizações dos ativos de TIC (pacotes de segurança, firmware, entre outros) devem ser aplicadas, sempre que possível, tão logo liberadas, mas considerando:

I - os riscos decorrentes da atualização;

II - os riscos decorrentes da não aplicação (ou postergação);

III - a criticidade do ativo;

IV - a estabilidade dos serviços.

Seção III
Das Funções Detectar, Responder e Recuperar

Art. 12. As atividades decorrentes das funções "Detectar", "Responder" e "Recuperar" do PPINC-PJ estão cobertas pelo Processo de Gestão de Incidentes de Segurança da Informação, detalhado no Anexo B deste ato.

Art. 13. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, deverá, ainda, ser seguido o Protocolo de Investigação para Ilícitos Cibernéticos.

Parágrafo único. Na ocorrência da hipótese prevista no caput deste artigo, o Comitê Gestor de Segurança da Informação e a Presidência do TRT7 deverão ser comunicados.

Art. 14. 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.

Art. 15. Este ato deverá ser revisado e atualizado pelo menos a cada três anos, mediante provocação da Secretaria de Tecnologia da Informação e Comunicação.

Art. 16. Revogar o Ato TRT7 nº 152, de 27 de setembro de 2018.

Art. 17. Este Ato entra em vigor na data de sua publicação.

Fortaleza, 24 de setembro de 2021.
REGINA GLÁUCIA CAVALCANTE NEPOMUCENO
Presidente do Tribunal

Anexo A

1 - DA EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS – ETIR

1.1 - MISSÃO

Planejar, coordenar e executar atividades de tratamento e resposta a incidentes de segurança da informação, confirmado ou sob suspeita, relacionado às redes de computadores, preservando os dados, as informações e a infraestrutura de TIC do TRT da 7ª Região.

1.2 - PÚBLICO ALVO

Usuários da rede corporativa de computadores e sistemas de informação do TRT da 7ª Região.

1.3 - MODELO DE IMPLEMENTAÇÃO

1.3.1 A ETIR será formada por 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.

1.3.2 - 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.

1.4 - NÍVEL DE AUTONOMIA

1.4.1 - 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.

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 3317, 27 set. 2021. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 3.

1.4.2 A ETIR poderá solicitar apoio multidisciplinar abrangendo as áreas de tecnologia da informação, jurídica, pesquisas judiciárias, comunicação, controle interno, segurança institucional, dentre outras necessárias para responder aos incidentes de segurança de maneira adequada e tempestiva.

1.5 - DESIGNAÇÃO DE INTEGRANTES

1.5.1 - A ETIR deve ser composta por servidores públicos ocupantes de cargo efetivo de carreira, com perfil técnico compatível, e deverá ser gerida pelo Gabinete de Segurança da Informação (GSI).

1.5.2 - Recomenda-se que os membros da ETIR sejam: administradores de sistemas ou de segurança, administradores de banco de dados, administradores de redes ou analistas de suporte.

1.5.3 - A ETIR será composta por:

a) 2 (dois) servidores da Divisão de Infraestrutura de TIC;
b) 1 (um) servidor da Divisão de Serviços e Suporte aos Usuários de TIC;
c) 1 (um) servidor da Divisão de Sistemas de TIC;
d) 1(um) servidor do Gabinete de Segurança da Informação;

1.5.4 - 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.

1.5.5 - Portaria da SETIC indicará os servidores titulares e substitutos que irão compor a ETIR.

1.6 - CANAL DE COMUNICAÇÃO

Os canais de comunicação com a ETIR e/ou para informar incidentes de segurança da informação estão publicados na página “Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do TRT da 7ª Região” disponível no site institucional, dentro da seção “Institucional - Governança de TIC - Segurança da Informação”.

1.7 - SERVIÇOS QUE SERÃO PRESTADOS PELA ETIR (COMPETÊNCIAS)

1.7.1 - Execução do Processo de Gestão de Incidentes de Segurança da Informação do TRT7;

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 3317, 27 set. 2021. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 3.

1.7.2 - Aplicar 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);

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

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

1.7.5 - Coletar e preservar as evidências, durante o processo de tratamento do incidente penalmente relevante, nos termos do Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário;

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

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

1.7.8 - Propor e acompanhar a execução das ações de contenção do incidente;

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

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

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

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

1.7.13 - 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.

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 3317, 27 set. 2021. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 3.

1.7.14 - Realizar reuniões regulares para avaliar o progresso até que seja possível retornar à condição de normalidade.

1.7.15 - A ETIR, sob a supervisão do Gabinete de Segurança da Informação do TR7, durante o processo de tratamento do incidente, quando constatado crise cibernética, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas, deverá, de imediato, comunicar o Comitê de Crises Cibernéticas e o Comitê Gestor de Segurança da Informação.

1.7.16 - Elaborar Relatório de Incidente de Segurança da Informação, também chamado de Relatório de Comunicação de Incidente de Segurança em Redes Computacionais, descrevendo detalhadamente os eventos verificados, nos termos do Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário, quando se tratar de incidente penalmente relevante.

ANEXO B

PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

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 os incidentes em segurança da informação sejam **detectados, respondidos e recuperados**, em tempo hábil.

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.

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 3317, 27 set. 2021. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 3.

2. PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A gestão de incidentes de segurança cibernética é realizada por meio deste processo, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.

2.1. Detecção

Detectar incidente de segurança	
Objetivo:	Desenvolvimento e à implementação de atividades adequadas à descoberta oportuna de eventos para a detecção de incidentes de segurança cibernética.
Responsável:	Divisão de Infraestrutura de TIC
Entrada:	- Alertas de Rede; - Alerta de eventos; - Informações de vulnerabilidades e incidentes divulgados por fornecedores ou mídia especializada;
Ação:	● Coletar e/ou observar os eventos gerados pelo ativos computacionais; ● Analisar vulnerabilidades e incidentes divulgados; ● Fornecer informações relacionadas a incidentes ou vulnerabilidades ao Gabinete de Segurança da Informação
Saída:	- Aviso sobre vulnerabilidades e/ou risco de incidentes; - Comunicação de suspeita ou ocorrência de incidente;

2.2. Triagem

Triagem	
Objetivo:	Realizar análise superficial da suspeita ou ocorrência de incidente
Responsável:	ETIR
Entrada:	- Aviso sobre vulnerabilidades e/ou risco de incidentes; - Comunicação de suspeita ou ocorrência de incidente (email, sistema de gestão de serviços, telefone, chat);
Ação:	● Receber comunicação sobre o incidente; ● Entrar em contato com os usuários para solicitar esclarecimentos, quando necessário; ● Classificar e priorizar o incidente; ● Registrar o incidente (preencher o formulário); ● Estabelecer a relação com outros incidentes/eventos; ● Dar ciência ao Comitê Gestor de Segurança da Informação (CGSI) do registro da suspeita ou ocorrência de incidente ● Atribuir o incidente a um responsável para análise aprofundada
Saída:	- Relatório de Incidente de Segurança da Informação (RISI) preenchido com informações iniciais.

2.3. Resposta

É a fase de tratamento do incidente, incluindo atividades de investigação, contenção e/ou solução, comunicação às áreas afetadas, coleta de evidências, além da

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 3317, 27 set. 2021. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 3.

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

2.3.1. Investigar incidente

A ETIR, 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.

2.3.2. Propor ações de contenção

A ETIR, 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.

Propor ações de contenção	
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.

2.3.3. Coletar evidências e/ou gerar relatório

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 3317, 27 set. 2021. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 3.

Quando necessário, a ETIR 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.

Caso o Incidente de Segurança seja considerado penalmente relevante, a ETIR deverá realizar os procedimentos para coleta e preservação das evidências e comunicar o incidente de segurança, de acordo com o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário.

2.3.4. Comunicar as áreas afetadas

Quando necessário, a ETIR 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 comunicação.

2.3.5. Referendar ações

O diretor da SETIC analisa as ações de contenção propostas pela ETIR 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

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 3317, 27 set. 2021.
Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 3.

Objetivo:	Analisar as ações de contenção propostas pela ETIR 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 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 ETIR, 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.

2.3.6. Analisar ações

O Comitê de Segurança da Informação analisa as ações de contenção propostas pela ETIR 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 ETIR 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.

2.3.7. Autorizar ações

A Presidência do TRT7 analisa as ações de contenção propostas pela ETIR para decidir se dá prosseguimento aos esforços de execução das ações.

Autorizar ações	
Objetivo:	Analisar as ações de contenção ETIR 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 Gestor 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.

2.3.8. 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 ETIR.

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 ETIR.
Responsável:	Unidades vinculadas à SETIC.
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 ETIR ou encaminhar para encerramento do incidente.
Saída:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com resultado das medidas aplicadas.

2.4. Encerramento

2.4.1 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).
Responsável:	ETIR
Entrada:	Relatório de Incidente de Segurança da Informação (RISI) preenchido com resultado das medidas aplicadas.

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 3317, 27 set. 2021. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 3.

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.

2.4.2. Analisar proposições da ETIR

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

Analisar proposições da ETIR	
Objetivo:	Avaliar as soluções propostas ou o relatório de auditoria enviado pela ETIR 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.

2.4.3 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 promover 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.

2.5. Avaliar

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 3317, 27 set. 2021. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 3.

2.5.1 Avaliar histórico de incidentes e oportunidades de melhoria

A ETIR 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 oportunidades de melhoria.
Saída:	Registro de indicadores/histórico de incidentes.

2.5.2 Implantar melhorias

A ETIR 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.