PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 19ª REGIÃO

ATO N.º 18/GP/TRT 19ª, DE 20 DE JANEIRO DE 2023

Aprova a Norma de Gestão de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 19ª Região.

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

CONSIDERANDO as boas práticas de Governança de TIC que visam a garantir a disponibilidade e integridade dos sistemas, aplicativos, dados e de documentos digitais do TRT da 19ª Região;

CONSIDERANDO o disposto no artigo 7º, inciso II, alínea "b", do Ato nº 45/2018 do TRT da 19ª Região, que instituiu a Política de Segurança da Informação;

CONSIDERANDO o disposto no artigo 21, inciso II, alínea "a", da Resolução nº 370/2021 do Conselho Nacional de Justiça, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO o disposto no artigo 11, inciso III, da Resolução nº 396/2021 do Conselho Nacional de Justiça, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o constante do Proad n.º 3971/2021,

RESOLV E:

Art. 1º Aprovar a Norma de Gestão de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 19ª Região, na forma do Anexo Único, e aprovar o Protocolo de Prevenção de Incidentes Cibernéticos (PPINC), o Protocolo de Gerenciamento de Crises Cibernéticas (PGCC) e o Protocolo de Investigação para Ilícitos Cibernéticos (PIILC) para observância e aplicação em todo o Regional.

Art. 2º Este Ato entrará em vigor na data da sua publicação.

Art. 3º Revoga-se o Ato GP n. 103, de 29 de outubro de 2019.

Dê-se ciência, cumpra-se e
Publique-se.

Original assinado
JOSÉ MARCELO VIEIRA DE ARAÚJO
Desembargador Presidente

Publicado no B.I., n.º 1, e no D.E.J.T. de 23/1/2023

ATO N.º 18/GP/TRT 19ª, DE 20 DE JANEIRO DE 2023

ANEXO ÚNICO
NSI002 - GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

1.1. Estabelecer as diretrizes e definir o Processo de Gestão de Incidentes de Segurança da Informação aplicáveis ao ambiente tecnológico do TRT19.

2. MOTIVAÇÕES

2.1. Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria;
2.2. Necessidade de prevenir e tratar os incidentes de segurança da informação com resposta rápida e eficiente;
2.3. Correto direcionamento e dimensionamento de recursos tecnológicos e humanos para prover uma Gestão de Incidentes de Segurança da Informação com menor custo e maior qualidade;
2.4. Formalização de um processo sistemático para gerenciamento dos incidentes de segurança da informação, provendo insumos para minimizar e/ou evitar eventos futuros.

3. REFERÊNCIAS NORMATIVAS

3.1. Decreto N° 9.637, de 26 de dezembro de 2018, que institui Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;
3.2. Decreto N° 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos;
3.3. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;
3.4. Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;
3.5. Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 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;

3.6. Norma Complementar nº 08/IN01/DSIC/GSIPR, de 23 de agosto de 2010, que estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais – Gestão de ETIR, nos órgãos e entidades da Administração Pública Federal;

3.7. Norma Complementar nº 21/IN01/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações da Presidência da República, 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;

3.8. Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

3.9. Portaria CNJ nº 162/2021, que Aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021;

3.10. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização;

3.11. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação.

4. CONCEITOS E DEFINIÇÕES

Para os efeitos deste documento são estabelecidos os seguintes conceitos e definições:

4.1. **Artefato malicioso**: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

4.2. **Central de serviços de TIC**: ponto único de contato entre o provedor de Serviço de TIC e os usuários;

4.3. **Medida de contenção**: controle e/ou ação tomada para evitar que danos causados por um determinado incidente continuem aumentando com o passar do tempo. Além disso, tais medidas visam o reestabelecimento do sistema/serviço afetado, mesmo eu não seja em sua capacidade total;

4.4. **Medida de solução**: controle e/ou ação tomada para sanar vulnerabilidades e problemas que sejam a causa-raiz de um ou mais incidentes de segurança da informação;

4.5. **Tratamento e resposta a incidentes de segurança cibernética**: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

Outras definições relevantes constam da Política de Segurança da Informação e do Anexo VIII da Portaria CNJ nº 162/2021.

5. ESCOPO

5.1. A Gestão de Incidentes de Segurança da Informação, definida nesta norma, tem seu escopo limitado às situações relacionadas ao ambiente, ativos, projetos e processos de TIC.

6. DIRETRIZES

6.1. A Gestão de Incidentes de Segurança da Informação tem como principal objetivo assegurar que incidentes de segurança da informação sejam identificados, registrados e avaliados em tempo hábil, com a tomada de medidas de contenção e/ou solução adequadas;

6.2. Estão abrangidos por esta norma os eventos, confirmados ou suspeitos, que estejam relacionados à segurança de sistemas ou redes computacionais que:

6.2.1. Comprometam o ambiente tecnológico do TRT19, seus ativos, informações e processos de negócio;

6.2.2. Contrariem a Política de Segurança da Informação do TRT19;

6.2.3. Causem a interrupção ou indisponibilidade de serviço essencial ao desempenho das atividades;

6.2.4. Acarretem vulnerabilidades de segurança;

6.2.5. Provoquem a divulgação, alteração ou destruição de informações;

6.2.6. Impliquem em prática de ato definido como crime ou infração administrativa.

6.3. O TRT19 providenciará dispositivos de monitoramento, ferramentas de segurança e detecção de intrusão, a fim de subsidiar a Gestão de Incidentes de Segurança da Informação.

7. PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

7.1. O processo de Gestão de Incidentes de Segurança da Informação é contínuo e aplicado na implementação e operação do Sistema de Gestão de Segurança da Informação (SGSI);

7.2. O processo de Gestão de Incidentes de Segurança da Informação é composto pelas seguintes etapas:

7.2.1. Detecção: tem por objetivo receber a comunicação de eventos relacionados à segurança da informação;

7.2.2. Triagem: tem por objetivo selecionar quais eventos são caracterizadas como evento adverso, confirmado ou sob suspeita, relacionado à segurança e registrá-los;

7.2.3. Análise: tem por objetivo verificar todas as evidências coletadas, entender a dinâmica do incidente e propor ações de tratamento e resposta a incidentes;

7.2.4. Resposta: tem por objetivo comunicar as partes interessadas a respeito das ações de mitigação e tratamento dos incidentes identificados.

7.3. Os incidentes, notificados ou detectados, devem ser objeto de registro, com a finalidade de assegurar a manutenção do histórico e auxiliar na geração de indicadores;

7.4. A notificação de incidente poderá ser feita por qualquer usuário interno, sem necessidade de prévia autorização do gestor, através da central de serviços de TIC, que os reportarão ao Gestor de Segurança da Informação;

7.5. Os usuários devem notificar, o mais breve possível, os incidentes de segurança da informação e as vulnerabilidades de que tenham conhecimento (observados ou suspeitos);

7.6. Vulnerabilidades suspeitas não deverão ser objeto de teste ou prova pelos usuários, sob o risco de violar a Política de Segurança da Informação e/ou provocar danos aos serviços ou aos recursos tecnológicos;

7.7. As equipes da Setic responsáveis pelo monitoramento dos ativos, serviços e sistemas devem notificar os incidentes a eles relacionados ao Gestor de Segurança da Informação, por qualquer meio de comunicação que privilegie e garanta a maior celeridade possível na análise do ocorrido, para o devido registro e encaminhamento;

7.8. Os provedores contratados para a prestação de serviços em nuvem devem ser informados da existência deste processo no âmbito do TRT19 para que procedam com a comunicação de incidentes de segurança cibernética, quando estes ocorrerem;

7.9. O TRT19 poderá receber notificações externas sobre incidentes (ocorridos ou suspeitos) por e-mail (setic.seguranca@trt19.jus.br), que deverão ser remetidas ao Gestor de Segurança da Informação, para o devido encaminhamento;

7.10. O tratamento da informação deve ser realizado de forma a viabilizar e a assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, com retorno das operações à normalidade no menor prazo possível, bem como evitar futuras ocorrências, com a proposição de ações de solução, quando existentes;

7.11. A ETIR deve, em conjunto com as outras áreas da Setic, investigar o incidente e artefatos maliciosos, propondo e implementando as ações de contenção, comunicando as áreas afetadas e coletando os dados necessários;

7.12. A coleta de evidência dos incidentes de segurança da Informação deve ser realizada pela ETIR ou por pessoal competente e por ela autorizado, observando o Protocolo de Investigação de Ilícitos Cibernéticos para os casos penalmente relevantes;

7.13. 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;

7.14. A ETIR deverá acionar o Protocolo de Gerenciamento de Crises Cibernéticas nos casos de incidentes graves;

7.15. Quando ficar evidente que um incidente de segurança da informação não será mitigado rapidamente e poderá durar dias, semanas ou meses, ações responsivas devem ser tomadas paralelamente às ações para mitigar o incidente com objetivo de manter a continuidade dos serviços prestados. Caso seja necessário, o Plano de Continuidade de Serviços de TIC pode ser acionado;

7.16. Para melhor lidar com uma crise cibernética, é necessária preparação prévia e adequada, sendo fundamental que a ETIR, em conjunto com o Comitê de Crise Cibernética neste processo, defina um plano de atuação;

7.17. Após o retorno das operações à normalidade, a ETIR deverá realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada. Em seguida, deverá ser elaborado Relatório de Comunicação de Incidente de Segurança da Informação, que contenha as lições apreendidas, bem como o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados;

7.18. Quando houver indícios de ilícitos criminais durante o gerenciamento dos incidentes de segurança, deverá ser observado o Protocolo de Investigação de Ilícitos Cibernéticos;

7.19. O encerramento do incidente de segurança da informação será realizado pelo Gestor de Segurança da Informação, com comunicação ao CGSI e às demais áreas envolvidas;

7.20. A avaliação do processo de gestão de incidentes de segurança da informação ocorrerá através do histórico de incidentes, com verificação das oportunidades de melhoria;

7.21. O manual contendo o desenho do processo de Gestão de Incidentes de Segurança da Informação, a descrição das atividades, os respectivos papéis e responsabilidades dos envolvidos no processo, a serem utilizados nas etapas do processo, será publicado no Portal de Governança de TI, após aprovação pela Presidência;

7.22. O processo será revisto periodicamente e eventuais alterações propostas nos documentos acima indicados serão, após aprovação pela Presidência do TRT19, objeto de imediata divulgação na forma do item anterior.

8. ATUALIZAÇÃO DA NORMA

ATO N.º 18/GP/TRT 19ª, DE 20 DE JANEIRO DE 2023

8.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de Gestão de Incidentes de Segurança da Informação, observada a periodicidade prevista para a Política de Segurança da Informação.

Tribunal Regional do Trabalho
19ª Região | Alagoas

Manual de Processo

Processo Gestão de Incidentes de Segurança da Informação

Versão do documento: 1.0
Janeiro/2023

Sumário

Objetivo

O presente processo tem como principal objetivo detectar, selecionar, analisar e responder os incidentes relacionados à segurança da informação no Tribunal Regional do Trabalho da 19ª Região.

Propósito

Este processo tem como propósito garantir que incidentes de segurança da informação são avaliados e tratados de maneira específica e mais adequada possível, além de minimizar os efeitos adversos de incidentes de segurança da informação.

Escopo

O escopo do processo abrange a detecção, triagem, análise e resposta aos incidentes de segurança da informação, inclusive nos serviços disponibilizados em nuvem, no âmbito do TRT19, bem como a elaboração de relatórios.

Definições e abreviações

- **Informação**: dados, processados ou não, que podem ser utilizados para a produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- **Incidente de segurança da informação**: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança da informação;
- **DSIPD**: Divisão de Segurança da Informação e Proteção de Dados, unidade do TRT19 responsável pela segurança da informação;
- **ETIR**: Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética;
- **CPTRIC-PJ**: Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos
- do Poder Judiciário;
- **TIC**: Tecnologia da Informação e Comunicação;
- **SI**: Segurança da Informação.

Benefícios esperados

Com a implementação deste processo no TRT da 19ª Região espera-se:
- Registro das vulnerabilidades de segurança da informação;
- Prevenção de futuras ocorrências relacionadas à segurança da informação.

Regras Gerais

- Os provedores contratados para a prestação de serviços em nuvem devem ser informados da existência deste processo no âmbito do TRT19 para que procedam com a comunicação de incidentes de segurança cibernética, quando estes ocorrerem.
- Em casos de incidentes graves, o CPTRIC-PJ deverá ser comunicado;
- O registro de eventos de segurança da informação e os relatórios do tratamento dos incidentes, incluindo as lições apreendidas, deverão ser anexados na ferramenta de

gestão de demandas utilizada pela Setic.

Interface com demais processos

A seguir estão descritas as principais interfaces deste processo com outros processos de gestão de Teconlogia da Informação e Comunicação do TRT19:

- **Gerenciamento de incidentes de TIC**: o processo pode ser iniciado através de um incidente que já estava em tratamento no processo de gerenciamento de incidentes de TIC;
- **Gerenciamento de crise cibernética**: em casos de crise cibernética este subprocesso será acionado para o gerenciamento da mesma;
- **Gerenciamento da central de serviços de TIC:** o atendimento à solicitação de resolução de incidentes é feito através desse processo.

Papéis e Responsabilidades

Papel	Executores	Responsabilidades
Dono do Processo	Diretor da Divisão de Segurança da Informação e Proteção de Dados.	● É formalmente designado e possui a autoridade máxima em relação ao processo, garantindo sua especificação e execução.
Gestor da Segurança da Informação	Diretor da Divisão de Segurança da Informação e Proteção de Dados.	● Realizar análise prévia; ● Registrar eventos; ● Convocar a ETIR.
ETIR	Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética	● Analisar, estabelecer ações e tratar incidentes de segurança da informação.
Comitê de Crise Cibernética	Alta administração e representantes executivos.	● Gerenciar crises.

Indicadores de Desempenho

Os indicadores descritos a seguir irão avaliar o desempenho do processo.

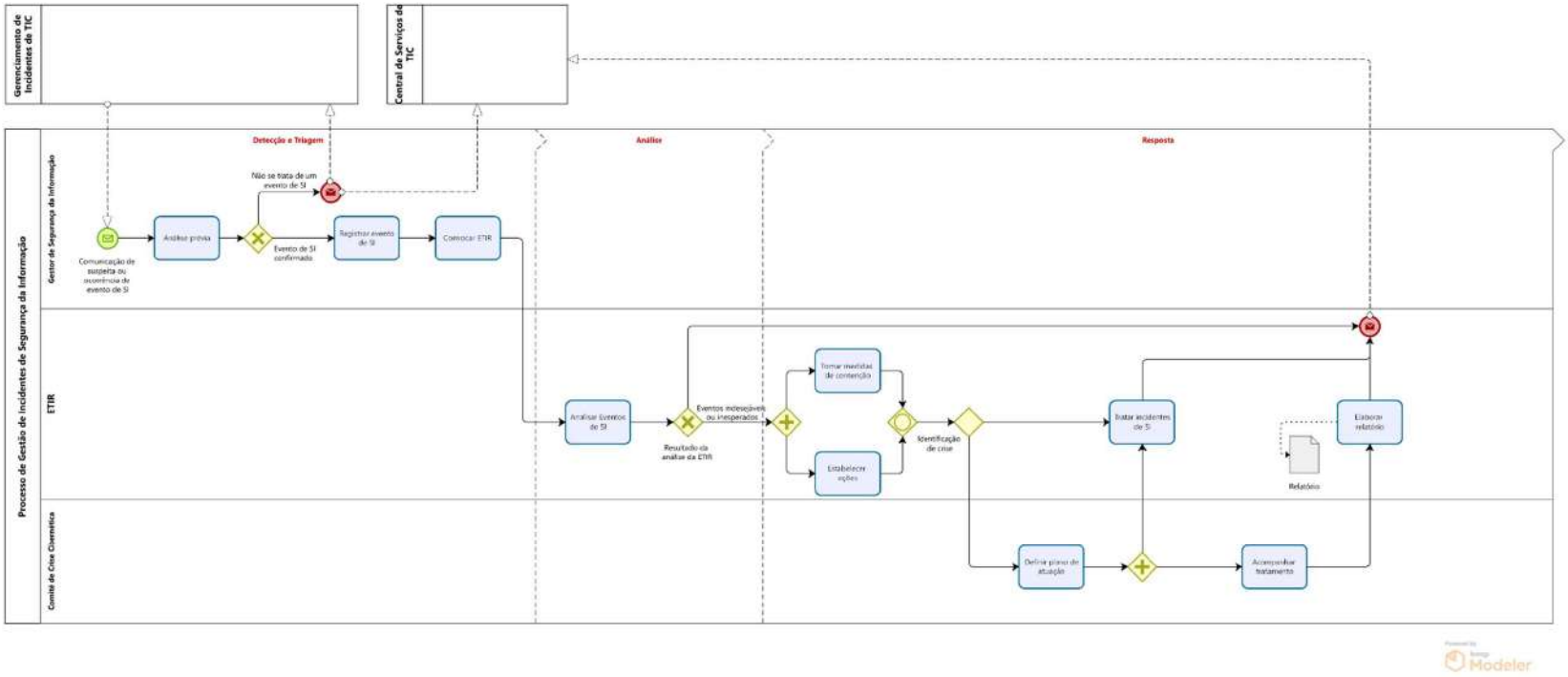
Descrição do	Método de apuração / fórmula de cálculo	Frequência

Indicador		
Número de incidentes de segurança da informação identificados	nº de incidentes de segurança da informação registrados na ferrramenta de gestão de demandas de TIC	anual

Controles de execução

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

Fluxograma


Gerenciamento de Incidentes de TIC
Central de Serviços de TIC
Processo de Gestão de Incidentes de Segurança da Informação
Gestor de Segurança da Informação
ETIR
Comitê de Crise Cibernética
Detecção e Triagem
Análise
Resposta
Não se trata de um evento de SI
Comunicação de suspeita ou ocorrência de evento de SI
Análise prévia
Evento de SI confirmado
Registrar evento de SI
Convocar ETIR
Analisar Eventos de SI
Resultado da análise da ETIR
Eventos indesejáveis ou inesperados
Tomar medidas de contenção
Estabelecer ações
Identificação de crise
Tratar incidentes de SI
Relatório
Elaborar relatório
Definir plano de atuação
Acompanhar tratamento

Descrição das Tarefas

Análise Prévia		
Descrição	O Gestor de Segurança da Informação realiza a análise preliminar dos eventos comunicados à Divisão de Segurança da Informação e Proteção de Dados. O objetivo é detectar incidentes de segurança da informação e fazer triagem nos eventos relatados.	
Papéis	Gestor de Segurança da Informação	
Considerações importantes	A comunicação corresponde a qualquer indício de fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar a segurança da informação.	
Entradas	Comunicação de Evento	
Saídas	Resultado da Triagem do Evento	
Atividades	Receber comunicação	A comunicação pode ser feita através da Central de Serviços de TIC, por Provedor de Serviço em Nuvem ou por qualquer outro meio de comunicação que privilegie e garanta a maior celeridade possível na análise do ocorrido.
	Analisar evento e realizar triagem	Caso os eventos não correspondam a um incidente de Segurança da Informação, o processo é finalizado e comunicado ao processo de Gerenciamento de Incidentes de TIC e / ou às partes interessadas através do Processo de Gerenciamento da Central de Seviços.
Ferramentas	Sistema de atendimento ao usuário de TIC	

Registrar Evento de SI		
Descrição	Uma vez detectado que trata-se de um incidente de segurança da informação, este deve ser registrado de maneira a garantir documentação e, consequentemente, rastreabilidade.	
Papéis	Gestor de Segurança da Informação	
Considerações importantes	O Gestor de Segurança da Informação deve anexar documentos adicionais à Ferramenta de Gestão de Demandas de TIC e envolver as partes interessadas.	
Entradas	Incidente de Segurança da Informação	
Saídas	Registro do Incidente de Segurança da Informação	
Atividades	Registrar	Registrar o incidente
	Comunicar	Comunicar Partes Interessadas
Ferramentas	Ferramenta de Gestão de Demandas de TIC	

Convovar ETIR		
Descrição	O Gestor de Segunrança da Informação deve convocar a ETIR da forma que decidir mais eficaz.	
Papéis	Gestor de Segurança da Informação	
Considerações importantes	É recomendado o registro da convocação na Ferramenta de Gestão de Demandas de TIC.	
Entradas	Incidente de Segurança da Informação	
Saídas	Convocação da ETIR	
Atividades	Convocar	Atualizar solicitação com os requisitos necessários.
	Registrar	Registrar convocação
Ferramentas	Ferramenta de Gestão de Demandas de TIC.	

Analisar Eventos de SI	
Descrição	A ETIR deve reunir-se para fins de cumprimento de sua missão, mais especificamente no que tange a análise dos eventos que caracterizam o incidente de segurança da informação. Outra importante análise a ser feita é a identificação de crise cibernética.
Papéis	Equipe de Tratamento e Resposta a Incidentes
Considerações importantes	A crise cibernética acontecerá nos casos de incidentes graves que: a) ficar caracterizado grave dano material ou de imagem; b) restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses; c) o incidente impactar a atividade finalística ou o serviço crítico mantido pela organização; ou d) incidente atrair grande atenção da mídia e da população em geral.
Entradas	Incidente de Segurança da Informação
Saídas	Resultado da análise da ETIR
Atividades	
Ferramentas	Ferramenta de Gestão de Demandas de TIC.

Tomar Medidas de Conteção	
Descrição	Quando ficar evidente que um incidente de segurança da informação não será mitigado rapidamente e poderá durar dias, semanas ou meses, ações responsivas devem ser tomadas paralelamente às ações para mitigar o incidente com objetivo de manter a continuidade dos serviços prestados. Caso seja necessário, o Processo de Gestão de Continuidade de TIC pode ser acionado.
Papéis	Equipe de Tratamento e Resposta a Incidentes
Considerações importantes	
Entradas	Incidente de Segurança da Informação
Saídas	Medidas de contenção tomadas

Atividades		
Ferramentas	Ferramenta de Gestão de Demandas de TIC.	

Estabelecer Ações		
Descrição	A ETIR deve estabelecer quais serão os procedimentos a serem executados. Em geral, principalmente quando não se tratar de crise cibernética ou incidente que possa ser resolvido brevemente, apenas ações de contenção devem ser tomadas.	
Papéis	Equipe de Tratamento e Resposta a Incidentes	
Considerações importantes	Em caso de crise cibernética, o Comitê de Crise Cibernética deverá ser acionado. Nos casos de incidentes graves, o CPTRIC-PJ deverá ser comunicado.	
Entradas	Incidente de Segurança da Informação	
Saídas	Ações para tratamento do incidente	
Atividades		
Ferramentas	Ferramenta de Gestão de Demandas de TIC.	

Definir Plano de Atuação	
Descrição	Para melhor lidar com uma crise cibernética, é necessário prévia e adequada preparação, sendo fundamental que a ETIR, em conjunto com o Comitê de Crise Cibernética), defina um plano de atuação.
Papéis	Comitê de Crise Cibernética
Considerações importantes	Para elaboração do plano, é necessário: a) entender claramente o incidente que gerou a crise, sua gravidade e os impactos negativos; b) levantar todas as informações relevantes, verificando fatos e descartando boatos; c) levantar soluções alternativas para a crise, avaliando sua viabilidade e consequências; d) avaliar a necessidade de suspender serviços e/ou sistemas informatizados; e) centralizar a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas;

	f) realizar comunicação tempestiva e eficiente, de forma a evidenciar o trabalho diligente das equipes e a enfraquecer boatos ou investigações paralelas que alimentem notícias falsas; g) definir estratégias de comunicação com a imprensa e/ou redes sociais e estabelecer qual a mídia mais adequada para se utilizar em cada caso; h) aplicar o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário; i) solicitar a colaboração de especialistas ou de centros de resposta a incidentes de segurança; j) apoiar equipes de resposta e de recuperação com gerentes de crise experientes; k) avaliar a necessidade de recursos adicionais extraordinários a fim de apoiar as equipes de resposta; l) orientar sobre as prioridades e estratégias da organização para recuperação rápida e eficaz; m) definir os procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações com base nas informações colhidas sobre o incidente; e n) elaborar plano de retorno à normalidade.
Entradas	Ações para tratamento do incidente
Saídas	Plano de Retorno à Normalidade
Atividades	
Ferramentas	

Tratar Incidentes de SI	
Descrição	A ETIR deve mobilizar as competências necessárias coordenando as atividades de tratamento e resposta aos incidentes de segurança da informação.
Papéis	Equipe de Tratamento e Resposta a Incidentes
Considerações importantes	Caso seja necessária a coleta de evidências, ela deverá ser realizada de acordo com a prática forense digital, de forma a garantir a devida confidencialidade, integridade e autenticidade das informações coletadas.
Entradas	Ações para tratamento do incidente
Saídas	Incidente tratado

Atividades		
Ferramentas		

Acompanhar tratamento		
Descrição	As etapas e os procedimentos de resposta são diferentes a depender do tipo de crise. Dessa forma, são necessárias reuniões regulares do Comitê de Crise Cibernética para avaliar o progresso até que seja possível retornar à condição de normalidade.	
Papéis	Comitê de Crise Cibernética	
Considerações importantes		
Entradas	Ações para tratamento do incidente	
Saídas	Plano de Retorno à Normalidade	
Atividades		
Ferramentas		

Elaborar relatório	
Descrição	Após o retorno das operações à normalidade, a ETIR deverá realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada. Em seguida, deverá ser elaborado Relatório de Comunicação de Incidente de Segurança da Informação, que contenha as lições apreendidas, bem como o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.
Papéis	Equipe de Tratamento e Resposta a Incidentes
Considerações importantes	Para a identificação das lições aprendidas e a elaboração de relatório, devem ser objeto de avaliação: a) a identificação e análise da causa-raiz do incidente; b) a linha do tempo das ações realizadas; c) a escala do impacto nos dados, sistemas e operações de negócios importantes; d) os mecanismos e processos de detecção e

	proteção existentes e as necessidades de melhoria identificadas; e) o escalonamento da crise (quando for o caso); f) a investigação e preservação de evidências; g) a efetividade das ações de contenção; h) a coordenação da crise (quando for o caso), liderança das equipes e gerenciamento de informações; e i) a tomada de decisão e as estratégias de recuperação.	
Entradas	Ações para tratamento do incidente	
Saídas	Incidente tratado / retorno das operações à normalidade	
Atividades	Comunicar as partes interessadas	Comunicar resultado da ocorrência do evento de SI.
Ferramentas	Ferramenta de Gestão de Demandas de TIC.	

PROTOCOLO DE PREVENÇÃO A INCIDENTES CIBERNÉTICOS

1. OBJETIVOS

1.1. Estabelecer um conjunto de diretrizes para a prevenção de incidentes cibernéticos;
1.2. Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética;
1.3. Promover ações proativas que contribuam para a prevenção de incidentes cibernéticos e também para a resiliência do ambiente tecnológico do Tribunal.

2. CONSIDERAÇÕES IMPORTANTES

2.1. Este protocolo é parte do conjunto de Protocolos de Segurança Cibernética, definido pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), do qual também fazem parte o Protocolo de Gerenciamento de Crises Cibernéticas e o Protocolo para Investigação de Ilícitos Cibernéticos;
2.2. As ações e medidas elencadas neste protocolo são complementares às políticas, aos processos, às práticas e aos procedimentos relacionados à segurança da informação já formalizados e estabelecidos no âmbito do TRT19;
2.3. Os atores atuantes ativamente na gestão de segurança cibernética no âmbito do TRT19, cujas instituições e atribuições estão definidas na Política de Segurança (Ato TRT19 nº 45/2018), Regimento Interno e demais Portarias relacionadas, são os seguintes:
  2.3.1. Secretaria de Tecnologia da Informação e Comunicação;
  2.3.2. Divisão de Segurança da Informação e Proteção de Dados;
  2.3.3. Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética;
  2.3.4. Comitê de Crise Cibernética.
2.4. Demais atores poderão ser envolvidos em atividades e ações relacionadas à gestão de segurança cibernética, tais como: Presidência, Comitê Gestor de Proteção de Dados Pessoais, Comitê Gestor de Segurança da Informação, dentre outros.

3. GLOSSÁRIO

3.1. Os conceitos utilizados neste protocolo têm como embasamento a definição constante no Anexo VIII da Portaria CNJ nº 162/2021.

4. FUNÇÕES DO PROTOCOLO

4.1. Com base na ENSEC-PJ, as funções básicas que compõem este protocolo são: identificar, proteger, detectar, responder e recuperar.

4.1.1. A função **identificar** consiste em atividades para identificar ativos tecnológicos críticos, levantar, analisar e avaliar os riscos aos quais o ambiente tecnológico está exposto, possibilitando a priorização e concentração de recursos humanos, tecnológicos e financeiros de acordo com a criticidade. No âmbito do TRT19, a função é contemplada pela seguinte atividade:

4.1.1.1. Gestão de Riscos de Segurança da Informação (Ato TRT19 n. 22/2022);

4.1.2. A função **proteger** consiste no desenvolvimento e implementação de controles que assegurem a proteção do ambiente tecnológico, dados (inclusive pessoais), além de contribuir para a eficiência e eficácia da prestação de serviços. No âmbito do TRT19, a função é contemplada pelas seguintes atividades:

4.1.2.1. Execução contínua da Política de segurança da Informação (Ato TRT19 n. 45/2018);

4.1.2.2. Gestão de Continuidade de TIC (Ato TRT19 n. 82/2019);

4.1.2.3. Gerenciamento da Disponibilidade e Capacidade de TIC;

4.1.2.4. Processo de Mudança e Liberação de Serviços;

4.1.2.5. Normatização do Uso dos Recursos de TI e controle de acesso (Ato TRT19 n. 131/2008);

4.1.2.6. Realização de cópias de segurança do ambiente tecnológico (Ato TRT19 n. 115/2022);

4.1.2.7. Implementação de boas práticas de gerenciamento e proteção do ambiente tecnológico, observando normatizações e frameworks estabelecidos no mercado (como ABNT NBR 27002 e CIS Controls), tais como:

4.1.2.7.1. Gerenciamento de vulnerabilidades;

4.1.2.7.2. Implementação de soluções de segurança do ambiente (firewall, IPS, Filtro de conteúdo web, proteção de endpoint, detecção e resposta de endpoint, dentre outras);

4.1.2.7.3. Hardening de serviços e de sistemas.

4.1.2.8. Adequação gradual aos seguintes Manuais de Referência, juntos com a ENSEC-PJ, observando a aplicabilidade de cada controle ao ambiente e maturidade do TRT19 em relação à segurança cibernética: Proteção de Infraestruturas Críticas de TIC e Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital;

4.1.3. A função **detectar** consiste no desenvolvimento e aplicação de medidas para identificação de eventos e/ou incidentes de segurança cibernética. A função **responder** consiste na definição e implementação de medidas para responder com eficiência e eficácia a incidentes de segurança cibernética. A função **recuperar** consiste no desenvolvimento, implementação e manutenção de planos e ações para prover resiliência e capacidade de recuperação aos serviços, sistemas e ativos tecnológicos quando da ocorrência de eventos e/ou incidentes de segurança cibernética. Essas três funções estão contempladas pelas seguintes atividades:

4.1.3.1. Gestão de Incidentes de Segurança da Informação;

4.1.3.2. Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética;

4.1.3.3. Gestão de Continuidade de TIC.

5. CONSIDERAÇÕES FINAIS

5.1. Na ocorrência de indícios de ilícitos criminais durante o tratamento de incidentes cibernéticos, além das ações elencadas ou referenciadas neste protocolo, deverá ser observado o Protocolo de Investigação de Ilícitos Cibernéticos.

5.2. Este documento deve ser revisado anualmente ou quando houver alteração significativa que enseje sua pronta alteração.

PROTOCOLO DE GERENCIAMENTO DE CRISES CIBERNÉTICAS

1. OBJETIVOS

1.1. Estabelecer um conjunto de diretrizes para responder efetivamente a crises decorrentes de incidentes cibernéticos;
1.2. Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética.

2. CONSIDERAÇÕES IMPORTANTES

2.1. Este protocolo é parte do conjunto de Protocolos de Segurança Cibernética, definido pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), do qual também fazem parte o Protocolo de Prevenção de Incidentes Cibernéticos e o Protocolo para Investigação de Ilícitos Cibernéticos;
2.2. As ações e medidas elencadas neste protocolo são complementares às políticas, aos processos, às práticas e aos procedimentos relacionados à segurança da informação já formalizados e estabelecidos no âmbito do TRT;
2.3. Este protocolo deve ser acionado nos casos em que as medidas estabelecidas no Protocolo de Prevenção de Incidentes Cibernéticos não forem suficientes para evitar a ocorrência de um incidente;
2.4. Para efeitos deste protocolo, são considerados críticos para o funcionamento do Tribunal os seguintes sistemas:
  2.4.1. Processo Judicial Eletrônico da Justiça do Trabalho (PJe-JT);
  2.4.2. Sistema de Gestão de Pessoas (Sigep);
  2.4.3. Sistema de Processos Administrativos Eletrônicos (Proad);
  2.4.4. Sistema de colaboração (Google Suite);
  2.4.5. Sítio Eletrônico do Tribunal.
2.5. Uma crise cibernética se configura na ocorrência de evento ou série de eventos danosos, que apresentam propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas que eles geram e que apresentam implicações que afetam uma proporção considerável da organização, bem como de seus constituintes, afetando diretamente ou indiretamente os sistemas críticos do Tribunal.
2.6. Os atores atuantes ativamente no gerenciamento de crises cibernéticas do TRT, cujas instituições e atribuições estão definidas na Política de Segurança do TRT (Ato TRT19 nº 45/2018), Regimento Interno e demais portarias relacionadas, são os seguintes:
  2.6.1. Comitê de Gestão de Segurança da Informação que atuará como Comitê de Gestão de Crises Cibernéticas;
  2.6.2. Secretaria de Tecnologia da Informação e Comunicação;
  2.6.3. Divisão de Segurança da Informação e Proteção de Dados;
  2.6.4. Equipe de Tratamento e Resposta a Incidentes Cibernéticos.

3. GLOSSÁRIO

3.1. Os conceitos utilizados neste protocolo têm como embasamento a definição constante no Anexo VIII da Portaria CNJ nº 162/2021.

4. GERENCIAMENTO DE CRISES CIBERNÉTICAS

4.1. O gerenciamento de crise cibernética se inicia quando:
- 4.1.1. Ficar caracterizado grave dano material ou de imagem;
- 4.1.2. Restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;
- 4.1.3. o incidente impactar gravemente os serviços de TIC essenciais ao funcionamento do Tribunal, extrapolando os limites determinados nas diretrizes do plano de continuidade de TIC do Tribunal;
- 4.1.4. atrair grande atenção da mídia e da população em geral; ou;
- 4.1.5. ocorrer incidente de segurança com dados pessoais;

4.2. Confirmada a crise cibernética, o Comitê de Crise Cibernética deverá se reunir.
- 4.2.1. Cabe ao Comitê o reporte da crise ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ);
- 4.2.2. Caso a crise envolva dados pessoais, o Encarregado de Tratamento de Dados Pessoais do Tribunal deve informar as entidades externas nos termos da LGPD e das demais normativas relacionadas à proteção de dados pessoais vigentes no TRT.
- 4.2.3. A sala de situação de onde serão geridas as crises será a Presidência, devendo dispor dos meios necessários (ex.: sistemas de áudio, vídeo, chamadas telefônicas) e estar preferencialmente próxima a um local onde se possa fazer declarações públicas à imprensa e com acesso restrito ao Comitê de Crise e a outros entes eventualmente convidados a participar das reuniões.

4.3. Para o tratamento do incidente que ocasionou a crise, deverão ser utilizadas políticas, planos de resposta a incidentes, planos de continuidade e de recuperação de desastres e procedimentos técnicos já elaborados e formalizados.

4.4. A crise encerra-se no momento em que for constatado o retorno à normalidade das operações.
- 4.4.1. Deve ser elaborado um relatório da crise com o intuito de registrar as ações que foram efetivas e as melhorias necessárias para corrigir as causas do incidente que originou a crise (lições aprendidas). O relatório deve conter as seguintes informações:
  - 4.4.1.1. A identificação e análise da causa-raiz do incidente;
  - 4.4.1.2. A linha do tempo das ações realizadas;
  - 4.4.1.3. A escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise;
  - 4.4.1.4. Os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;

4.4.1.5. As ações realizadas para tratamento da crise e avaliação de sua eficácia.

5. CONSIDERAÇÕES FINAIS

5.1. Na ocorrência de indícios de ilícitos criminais durante o tratamento de incidentes cibernéticos, além das ações elencadas ou referenciadas neste protocolo, deverá ser observado o Protocolo de Investigação de Ilícitos Cibernéticos.

5.2. Este documento deve ser revisado anualmente ou quando houver alteração significativa que enseje sua pronta alteração.

PROTOCOLO PARA INVESTIGAÇÃO DE ILÍCITOS CIBERNÉTICOS

1. OBJETIVOS

1.1. Estabelecer os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente;
1.2. Promover adequação e alinhamento às regulamentações, normas e melhores práticas relacionadas à segurança cibernética;
1.3. Definir requisitos para adequação dos ativos de tecnologia da informação no que tange à configuração e ao registro de informações de auditoria.

2. CONSIDERAÇÕES IMPORTANTES

2.1. Este protocolo é parte do conjunto de Protocolos de Segurança Cibernética, definido pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), do qual também fazem parte o Protocolo de Prevenção de Incidentes Cibernéticos e o Protocolo de Gerenciamento de Crises Cibernéticas;
2.2. As ações e medidas elencadas neste protocolo são complementares às políticas, aos processos, às práticas e aos procedimentos relacionados à segurança da informação já formalizados e estabelecidos no âmbito do TRT.

3. GLOSSÁRIO

3.1. Os conceitos utilizados neste protocolo têm como embasamento a definição constante no Anexo VIII da Portaria CNJ nº 162/2021.

4. DA ADEQUAÇÃO DOS ATIVOS TECNOLÓGICOS EM RELAÇÃO AO REGISTRO DE INFORMAÇÕES

4.1. Os ativos tecnológicos do Tribunal (estações de trabalho, servidores, serviços, sistemas etc.) devem:
4.1.1. Ser configurados de acordo com a Hora Legal Brasileira (HLB), de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON);
4.1.2. Ser configurados de forma a registrar eventos relevantes de segurança da informação, bem como de informações que possibilitem a depuração de incidentes e de problemas;
4.1.3. Registrar, sempre que possível, as seguintes informações:
4.1.3.1. Identificação inequívoca do usuário que acessou o recurso;
4.1.3.2. Natureza do evento, como, por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha etc.;
4.1.3.3. Data, hora e fuso horário, observando-se a HLB; e

4.1.3.4. Endereço IP (Internet Protocol), porta de origem da conexão, identificador do ativo de informação e demais informações que possibilitem identificar a origem do evento;

4.2. Os registros devem ser armazenados pelo período mínimo de 3 (três) meses, sem prejuízo de outros prazos previstos em normativos específicos;

4.3. O armazenamento dos registros de auditoria deve ser realizado remotamente (e não apenas localmente), por meio do uso de tecnologia aplicável, para, ao menos, os ativos tecnológicos considerados críticos.

5. CONSIDERAÇÕES FINAIS

5.1. A investigação do ilícito cibernético deve ser realizada de acordo com as normas estabelecidas na Política de Segurança da Informação vigente, especificamente no tocante ao assunto de gestão de incidentes de segurança da informação e à Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética;

5.2. Os incidentes de segurança cibernética devem ser registrados em Relatório de Incidente de Segurança da Informação, que contém os dados de identificação de quem o preencheu, data e hora da ocorrência, informações sobre o incidente, como ele foi tratado, oportunidades de melhoria e lições aprendidas;

5.3. Caso seja necessária a coleta de evidências, ela deverá ser realizada de acordo com a prática forense digital, de forma a garantir a devida confidencialidade, integridade e autenticidade das informações coletadas;

5.4. Se o incidente de segurança envolver a suspeita de crime, o Ministério Público e o órgão de polícia judiciária devem ser acionados com atribuição para o início da persecução penal.