PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO
GABINETE DA PRESIDÊNCIA

ATO REGULAMENTAR GP/TRT16 Nº 4/2025.

Institui o Processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 16ª Região.

A DESEMBARGADORA PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a Auditoria Interna nº 003/2022, que recomendou a interação do processo de gerenciamento de incidentes de segurança da informação/cibernética com o processo de gerenciamento de eventos;

CONSIDERANDO a Política de Segurança da Informação e Comunicação (POSIC) do TRT da 16ª Região, R.A nº 26/2021, recomenda que os processos que compõe a POSIC devem ser revisados numa periodicidade de 1 ano.

R E S O L V E:

Art. 1º Instituir o Processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 16ª Região, conforme Anexo I desta Portaria.

Art. 2º Revogar a Portaria GP nº 671/2017, de 12 de julho de 2017, bem como as demais disposições em contrário.

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

Dê-se ciência.

Publique-se no Diário Eletrônico da Justiça do Trabalho e disponibilize-se no Sítio Eletrônico do Tribunal.

São Luís (MA), datado e assinado eletronicamente.

Desembargadora MÁRCIA ANDREA FARIAS DA SILVA
Presidente do Tribunal Regional do Trabalho da 16ª Região

TRT-16ª REGIÃO
Gabinete da Presidência

Av. Senador Vitorino Freire, nº 2001, Areinha, 6º Andar
CEP 65030-015 – São Luís - Maranhão
(98) 2109-9306 / presidencia@trt16.jus.br

PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 16ª REGIÃO

PROCESSO DE MONITORAMENTO E TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

HISTÓRICO DE VERSÕES

#	DATA	DESCRIÇÃO
1	12/07/2017	Criação do Processo de Gerenciamento da Central de Serviços
2	30/01/2025	Revisão geral do processo com a atualização de formato. Inclusão das atividades ""Solicitar comunicação à ANPD" e "Comunicar a CPTRIC-PJ". Interação com o Processo de Gerenciamento de Eventos. Elaboração de um relatório conclusivo. Reorganização da matriz RACI. Alterações aprovadas na 1ª Reunião do Comitê de Segurança da Informação e Proteção de Dados de 2025 (0212915).

1. OBJETIVO

Este documento tem como objetivo estabelecer o processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 16ª Região (TRT16).

A Gestão de Incidentes de Segurança da Informação é um dos requisitos definidos pela norma internacional ISO/IEC 27001, que especifica práticas de segurança da informação.

No TRT16, esse processo visa garantir respostas rápidas e eficazes a ameaças que possam comprometer a execução da missão institucional: "Realizar justiça no âmbito trabalhista".

2. APLICABILIDADE

O processo de Monitoramento e Tratamento de Incidentes de Segurança da Informação não se restringe à unidade de Apoio à Segurança da Informação. Ele abrange todos os setores do Tribunal, com especial relevância para a Secretaria de Tecnologia da Informação e Comunicação (SETIC) e a alta administração. A proteção da informação, um dos ativos mais valiosos de qualquer organização, é responsabilidade de todos, em especial daqueles que a utilizam ou gerenciam.

Para que o processo seja bem-sucedido, sua adesão por toda a organização é fundamental. Mesmo que bem planejado, um processo só trará resultados efetivos com o apoio da alta administração e o comprometimento de todas as unidades do Tribunal.

3. TERMOS E DEFINIÇÕES

- **Ameaça**: causa potencial de um incidente de segurança da informação. Exemplos: pessoas interessadas em obter acesso a processos em segredo de justiça, em antecipar votos ou sentenças judiciais, em coletar dados pessoais de servidores e magistrados, ou em manchar a reputação do Tribunal.
- **Ativo**: qualquer recurso que represente valor para a organização e que, por isso, precisa ser protegido. Exemplos: documentos físicos ou digitais, sistemas, equipamentos, gravações, etc.
- **Conformidade**: cumprimento de um requisito, que pode ser técnico, processual ou legal. Exemplos: conformidade com o processo de monitoramento de incidentes, com a Lei de Acesso à Informação, com a Lei Geral de Proteção de Dados Pessoais (LGPD) e com as boas práticas da Microsoft para o Active Directory.
- **Contato institucional**: canal de comunicação estabelecido entre o TRT da 16ª Região e órgãos externos, como provedores de acesso, empresas, órgãos governamentais e a polícia.
- **Evento**: ocorrência ou mudança em um conjunto de circunstâncias dentro de um ambiente. Eventos podem ser positivos (melhorias, mudanças), negativos (incidentes, problemas) ou neutros (comportamentos normais, como um sistema informando que está funcionando corretamente).
- **Evidências**: artefatos utilizados para analisar incidentes, identificar a origem de ataques e atribuir responsabilidades. Exemplos de evidências: logs, documentos físicos ou digitais, imagens, gravações, etc.
- **Exploração de vulnerabilidade**: sinônimo de ataque. Ocorre quando uma ameaça explora uma vulnerabilidade de um ativo, visando destruir, expor, alterar ou obter acesso não autorizado a informações.
- **Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação (GRTISI)**: equipe formada para atuar na solução de incidentes de segurança da informação.
- **Incidente**: qualquer evento que não faça parte da operação normal de um serviço e que cause, ou possa causar, interrupção ou redução na qualidade do serviço. Exemplos: falha de computadores, lentidão no acesso à internet, problemas no uso do PJe.
- **Incidente de Segurança da Informação**: tipo específico de incidente relacionado à segurança da informação, o ativo mais importante de qualquer organização. Exemplos: roubo de senhas de e-mail, infecção por vírus, ameaças digitais, violação de políticas de segurança da informação, deixar um computador desbloqueado e desassistido.
- **Índice**: medida utilizada para acompanhar um determinado aspecto. Exemplos: quantidade de incidentes por mês, número de novos conhecimentos gerados, percentual de ataques com origem identificada.

- **Meta**: valor que se deseja atingir em um índice. Exemplos: criar pelo menos 3 novos conhecimentos por mês, identificar a origem de pelo menos 30% dos ataques, implementar 2 controles da norma NBR/ISO/IEC 27002 por semestre.
- **Ordenar despesa**: autorizar um pagamento.
- **Parte interessada**: pessoa ou organização que pode afetar, ser afetada, ou que se percebe como afetada por uma decisão ou atividade relacionada a um incidente de segurança da informação. Exemplos: provedores de acesso, diretoria geral, coordenador da SETIC, Polícia Federal, CERT.br, unidades da Justiça do Trabalho.
- **Processo**: fluxo ou conjunto de atividades relacionadas à segurança da informação.
- **Solucionar incidente**: ação ou conjunto de ações tomadas para restabelecer o funcionamento normal de um ambiente. Sempre que possível, a solução inclui a correção da vulnerabilidade e medidas preventivas para evitar a proliferação do ataque.
- **Vulnerabilidade**: ponto fraco em um sistema de segurança da informação que pode ser explorado e causar danos à organização. Exemplos: ausência de criptografia de senhas em banco de dados, uso de HTTP em vez de HTTPS em páginas que trafegam dados sensíveis, senhas anotadas em papéis sobre a mesa.

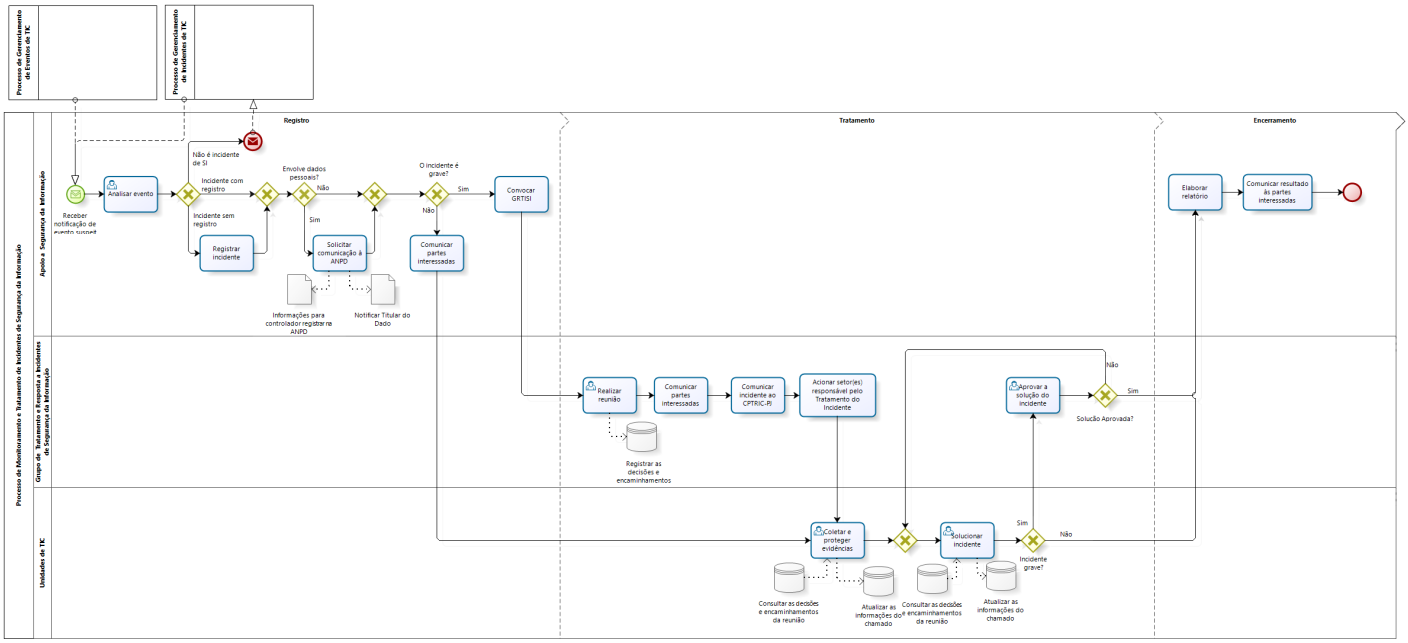
4. PAPÉIS E RESPONSABILIDADES

PAPEL	RESPONSABILIDADE
Dono do Processo (Secretário de TIC)	• Buscar a qualidade e eficiência geral do processo; • Propor e/ou autorizar mudanças no processo; • Assegurar que todos os envolvidos na execução do processo sejam informados de mudanças; • Prover recursos para execução do processo;
Chefe do Apoio a Segurança da Informação (SSI)	• Emitir relatórios gerenciais; • Realizar o contato com os demais setores da SETIC; • Coordenar as atividades do Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação e do Apoio a Segurança da Informação; • Manter o Secretário da SETIC e o chefe da Divisão de Infraestrutura e Segurança da Informação atualizados sobre os incidentes; • Submeter novos processos de tratamento de incidentes, bem como eventuais alterações dos já existentes; • Iniciar, conduzir e encerrar a execução do processo de tratamento; • Manter-se informado sobre o incidente durante todo o seu ciclo de vida; • Apoiar o Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação; • Avaliar e validar a conformidade da atuação do Grupo de Resposta a Incidentes de Segurança da Informação; • Estabelecer contato com unidades de TI ou de Segurança da Informação externa, quando houver necessidade; • Classificar os eventos e registrar as informações pertinentes ao escopo da sua função; • Manter todas as partes envolvidas informadas; • Emitir sugestões de melhorias; • Submeter novos processos de tratamento de incidentes, bem como eventuais alterações dos já existentes.
Grupo de Tratamento e Resposta a Incidentes de segurança da informação (GTRISI)	• Decidir sobre os procedimentos técnicos a serem adotados na resposta a incidentes; • Diligenciar para coletar e proteger evidências; • Solucionar e documentar o incidente.
Unidades da SETIC	• Fornecer apoio humano especializado para compor o Grupo de Tratamento e Resposta a Incidentes de Segurança da Informação • Notificar o Apoio a Segurança da Informação sobre eventos com potencial de serem incidentes de segurança da informação; • Reassumir o evento quando o Apoio a Segurança da Informação ou o GRTIS não o classificar como incidente de segurança da Informação; • Analisar de forma crítica as recomendações do Apoio a Segurança da Informação e definir a melhor estratégia para sua aplicação.

5. INTERFACES COM OUTROS PROCESSOS

- **Processo de Gerenciamento de Eventos de TIC**: este processo tem como uma de suas saídas, o registro de um chamado de incidente de segurança da informação quando for identificada uma exceção que comprometa um dos tripés da segurança da informação: Confidencialidade, Disponibilidade e Integridade;
- **Processo de Gerenciamento de Incidentes de TIC**: o Processo de Gerenciamento de Incidentes de TIC habilita o Processo de Gerenciamento de Monitoramento e Tratamento de Incidentes de TIC após um chamado ser pré-classificado como um incidente de segurança da informação.

6. FLUXO DO PROCESSO



ATIVIDADE	RESPONSÁVEL	DETALHAMENTO
Receber notificação de evento suspeito	Apoio à Segurança da Informação (SSI)	Entradas: • Chamado aberto na central de atendimento; • Notificação recebida de uma entidade externa (CERT.br, CSJT, CNJ, provedores de acesso, etc); • Alertas de ferramentas de segurança da informação do Tribunal; • Atividades proativas das unidades da SETIC. Descrição: 1. Receber a notificação de um evento/chamado; 2. Encaminhar o evento para análise. Saídas: • Evento encaminhado para o analista responsável.
Analisar evento	Analista do Setor de Apoio a Segurança da Informação	Entradas: • Evento suspeito. Descrição: 1. Diligenciar na busca por informações adicionais; 2. Classificar o evento; 3. Verificar se já tem chamado registrado. Saídas: • Encaminhamento do evento para gerenciamento de incidente (caso não seja de Segurança da Informação); • Evento ou alerta classificado como de Segurança da Informação.
Registrar incidente	Analista do Setor de Apoio a Segurança da Informação.	Entradas: • Chamado classificado; • Evento ou alerta classificado. Descrição: 1. Entrar em contato com o usuário ou entidade demandante; 2. Obter informações adicionais sobre o incidente; 3. Registrar as informações necessárias para o entendimento e suporte para solução do incidente. 4. Se existir chamado aberto, reclassificá-lo como incidente de segurança da informação; caso não tenha chamado, criar um chamado do tipo incidente de segurança da informação. Saídas: • Chamado registrado/reclassificado.

Comunicar às partes interessadas (fase de registro)	Analista do Setor de Apoio a Segurança da Informação.	Entradas: • Chamado registrado/classificado Descrição: 1. Identificar as partes interessadas; 2. Montar comunicado com conteúdo adequado relacionado ao incidente, como por exemplo: a. dados preliminares do incidente; b. ações iniciais; c. potenciais impactos e cuidados a serem tomados; d. dados que possam ser relevantes na contenção ou não proliferação do incidente em questão. 3. Encaminhar comunicado às partes interessadas. Saídas: • Comunicado encaminhado às partes interessadas.
Coletar e proteger evidências	Técnico da Unidade de TIC que vai tratar do incidente.	Entradas: • Chamado do incidente classificado como incidente de segurança da informação. Descrição: 1. Diligenciar em busca de evidências que possam subsidiar a análise do incidente; 2. Se a evidência for digital, armazená-la em sistema próprio para este fim; 3. Se a evidência for física, coletá-la com o apoio das seções competentes, inclusive a Coordenadoria de Material e Patrimônio, a Divisão de Polícia Judicial e, se necessário, com entidades externas; 1. Manter a evidência física sob custódia da Divisão de Polícia Judicial, instruindo-a sobre a sensibilidade dos dados e os cuidados no armazenamento dos mesmos; Saídas: • Evidências como logs, prints screens, e-mails, gravações em áudio e vídeo, papéis, imagens, fotografias, equipamentos, mídias digitais e dispositivos de armazenamento interno e externo, etc.
Solucionar incidente	Técnico da Unidade de TIC que vai tratar do incidente.	Entradas: • Chamado do incidente classificado como de segurança da informação;; • Evidências; Descrição: 1. Consultar a base de conhecimento; 2. Isolar os sistemas ou serviços afetados (evitar propagação do incidente); 3. Emitir recomendações e esclarecimento para os usuários quando necessário; 4. Testar a solução encontrada no ambiente de teste; 5. Encaminhar solução para o GRTISI avaliar e aprovar; 6. Aplicar solução para restabelecer a normalidade os sistemas e serviços afetados; 7. Registrar informações no chamado e na base de conhecimento; 8. Se possível, identificar a origem do ataque; Saídas: • Chamado resolvido; • Informações para elaboração do relatório; • Recomendações e esclarecimentos para os usuários, quando necessário.
Convocar GRTISI	Coordenador do Grupo de Resposta e Tratamento de Incidente de Segurança da Informação.	Entradas: • Chamado classificado. Descrição: 1. Entrar em contato com os membros da ETIR; 2. Reportar o incidente; 3. Agendar reunião. Saídas: • Reunião convocada.

Realizar reunião	Coordenador do Grupo de Resposta e Tratamento de Incidente de Segurança da Informação.	Entradas: • Reunião convocada. Descrição: 1. Fornecer informações sobre o incidente; 2. Fornecer informações sobre o impacto; 3. Informar as áreas afetadas; 4. Identificar a equipe para tratar o incidente Saídas: • Ata da reunião com as seguintes deliberações: ◦ a equipe que vai trabalhar no incidente; ◦ informações a serem comunicadas às partes interessadas; ◦ informações a serem comunicadas ao CPTRIC-PJ.
Solicitar comunicação a ANPD	Analista do Setor de Apoio a Segurança da Informação.	Entradas: • Incidente de segurança da informação registrado. Descrição: 1. Identificar o titular dos dados; 2. Descrever a natureza dos dados pessoais; 3. Descrever as medidas técnicas e de segurança utilizadas para proteger os dados pessoais; 4. Identificar os riscos relacionados ao incidente; 5. Verificar as medidas adotadas para mitigar ou reverter o incidente; 6. Consolidar as informações num documento para ser encaminhado ao Encarregado para que o mesmo possa comunicar à ANPD via abertura de processo SEI da ANPD (https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis); Saídas: • Documento com as informações necessárias para abertura do processo no SEI da ANPD.
Comunicar partes interessadas (fase de tratamento do incidente)	Analista do Setor de Apoio a Segurança da Informação.	Entradas: • Ata da reunião. Descrição: 1. Identificar as partes interessadas; 2. Comunicar o conteúdo adequado, como por exemplo: a. dados preliminares do incidente; b. ações iniciais; c. potenciais impactos e cuidados a serem tomados; d. dados que possam ser relevantes na contenção ou não proliferação do incidente em questão; e. próximas ações a serem executadas. Saídas: • Pedido à Direção da Setic para comunicar áreas afetadas com as informações necessárias sobre o incidente; • Texto básico para ser comunicado.
Comunicar a CPTRIC-PJ	Coordenador do Grupo de Resposta e Tratamento de Incidente de Segurança da Informação.	Entradas: • Ata da reunião. Descrição: 1. Criar documento com informações sobre o incidente; 2. Notificar o incidente para abuse@cnj.jus.br: a. O assunto do e-mail deve ser a descrição do incidente. b. Anexar o documento criado no passo 1. Saídas: • Confirmação de recebimento do e-mail enviado; • Registro do envio da comunicação no chamado.

Acionar setor(es) responsável(eis) pelo tratamento do incidente	Coordenador do Grupo de Resposta e Tratamento de Incidente de Segurança da Informação.	Entradas: • Ata da reunião - Deliberação do GRTISI; • Chamado do incidente. Descrição: 1. Comunicar o(s) setor(es) que vão resolver o incidentes; 2. Encaminhar o chamado ao responsável pelo(s) setor(es) escolhido(s) para tratar o incidente. Saídas: • Confirmação de recebimento do e-mail enviado; • Registro do envio da comunicação no chamado.
Aprovar solução do incidente	GRTISI	Entradas: • Solução proposta. Descrição: 1. Conhecer a solução; 2. Conhecer o impacto; 3. Conhecer os riscos; 4. Aprovar ou recusar a solução. Saídas: • Em caso de recusa, comunicar imediatamente a equipe técnica de resolução do incidente; • Em caso de aprovação, elaborar ata da reunião com deliberações sobre a solução apresentada.
Elaborar Relatório	Coordenador do Grupo de Resposta e Tratamento de Incidente de Segurança da Informação.	Entradas: • Chamado do incidente classificado como de segurança da informação; • Evidências; • Solução aplicada. Descrição: Elaborar um relatório que deverá conter as seguintes informações: 1. Detalhes completo do incidente, incluindo data, hora, sistemas ou recursos afetados; 2. Informar o impacto provocado pelo incidente; 3. Ações tomadas para conter o incidente; 4. Cronograma de resposta; 5. Comunicações realizadas; 6. Lições aprendidas; 7. Sugestões de melhorias. Saídas: • Relatório sobre o incidente.
Comunicar resultado às partes interessadas	Coordenador do Grupo de Resposta e Tratamento de Incidente de Segurança da Informação.	Entradas: • Chamado do incidente classificado como de segurança da informação; • Relatório do incidente. Descrição: 1. Elaborar comunicado sobre o incidente contendo as informações mais relevantes, como: a. partes afetadas; b. ativos afetados; c. causa; d. solução do incidente. Saídas: • Comprovante de envio do comunicado.

7. MATRIZ RACI

ATIVIDADE	Apoio de Segurança da Informação	GRTISI	Unidades de TIC
Receber notificação de evento suspeito	R/A	-	-
Analisar evento	R/A	-	-
Registrar incidente	R/A	I	-
Comunicar às partes interessadas (fase de registro)	R/A	I	-
Coletar e proteger evidências	C/I	A	R
Solucionar incidente	C/I	A	R
Convocar GRTISI	R	-	-
Solicitar comunicação a ANPD	R	A	-
Comunicar partes interessadas (fase de tratamento do incidente)	C/I	R/A	-

Comunicar a CPTRIC-PJ	R	A	-
Acionar setor(es) responsável(eis) pelo tratamento do incidente	C/I	R/A	-
Aprovar solução do incidente	I	R/A	I
Elaborar Relatório	R	A	C/I
Comunicar resultado às partes interessadas	R	A	-

8. INDICADORES

1 - Tempo médio de registro de um incidente de segurança da informação	
Objetivo	Calcular o tempo que leva, em média, desde que um incidente de segurança da informação é detectado até o momento em que ele é formalmente registrado.
Periodicidade	Semestral
Forma de cálculo	Total de horas para registrar cada incidente / total de incidentes registrados no período apurado.
Fonte	GLPI
Meta	< 3 horas entre a detecção, análise e registro formal.

2 - Taxa de incidentes solucionados	
Objetivo	Calcular a proporção de incidentes que foram resolvidos com sucesso dentro do período apurado.
Periodicidade	Semestral
Forma de cálculo	Total de incidentes de segurança da informação resolvidos / total de incidentes de segurança da informação registrado.
Fonte	GLPI
Meta	> 80%

9. DIVULGAÇÃO DOS RESULTADOS

Os resultados do processo, indicadores e relatórios, serão demonstrados na página de Governança de TIC do Tribunal.

Documento assinado eletronicamente por **RAFAEL ROBINSON DE SOUSA NETO**, **Secretário de Tecnologia da Informação e Comunicação**, em 02/04/2025, às 14:01, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site Autenticar Documentos informando o código verificador **0172550** e o código CRC **6C4B74EF**.