ATO TRT13.SGP N.º 019, 12 DE FEVEREIRO DE 2026

Dispõe sobre o Processo de Gestão de Incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 13ª Região.

A DESEMBARGADORA PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA DÉCIMA TERCEIRA REGIÃO, no exercício de suas atribuições legais e regimentais e nos termos do PROAD 254/2026,

CONSIDERANDO a necessidade de revisar o Processo de Gestão de Incidentes de Segurança da Informação da instituição, instituído pelo Ato TRT13.SGP n.º 181, de 19 de dezembro de 2022.

CONSIDERANDO as diretrizes da Política de Segurança da Informação e Comunicações e da Política de Proteção de Dados Pessoais da instituição;

CONSIDERANDO as recomendações decorrentes da auditoria coordenada pelo CSJT para avaliação da gestão de Segurança da informação no âmbito da Justiça do Trabalho de 1º e 2º graus (PROAD 6227/2022);

CONSIDERANDO as recomendações referentes à auditoria coordenada pelo TCU para diagnóstico acerca dos controles implementados por organizações públicas federais para adequação à Lei Geral de Proteção de Dados Pessoais (PROAD 6471/2025);

CONSIDERANDO o Ato Conjunto TST.CSJT.GP n.º 41, de 25 de julho de 2025, que institui o Processo de Comunicação de Incidentes Cibernéticos na Justiça do Trabalho (PCIC);

CONSIDERANDO a legislação federal, assim como resoluções, normas, recomendações e boas práticas publicadas pelo CNJ, CSJT, TCU e ABNT, relacionadas à Segurança da Informação e à Proteção de Dados Pessoais,

RESOLVE:

Art. 1º Instituir o novo o Processo de Gestão de Incidentes de Segurança da Informação, no âmbito do Tribunal Regional do Trabalho da 13ª Região, conforme descrição, papéis e responsabilidades definidas no anexo, disponível no Portal de Segurança da Informação, na página do Tribunal Regional do Trabalho da 13ª Região.

Art. 2º Revogar o Ato TRT13.SGP n.º 181, de 19 de dezembro de 2022.

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

Cientifique-se e publique-se no DEJT-Adm.

HERMINEGILDA LEITE MACHADO
Desembargadora Presidente
TRT da 13ª Região

TRT-13ª REGIÃO
Paraíba

MANUAL DO PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Secretaria de Governança e Gestão Estratégica

Assessoria de Governança de Segurança da Informação e Proteção de Dados Pessoais

João Pessoa – 2026
Versão 4.0

Tribunal Regional do Trabalho da 13ª Região

Desembargadora Presidente

Herminegilda Leite Machado

Comitê Gestor de Segurança da Informação

Larissa Leônia Bezerra de Andrade Albuquerque (Coordenadora, Juíza Auxiliar da Presidência)

Alexandre Roque Pinto (Vice-coordenador, Juiz Auxiliar da Vice-Presidência)

Adriano Mesquita Dantas (Magistrado indicado pela Presidência)

Alexandre Gondim Guedes Pereira (Diretor-Geral da Secretaria)

Luís Fabiano Saldanha Bandeira (Assessor de Governança de TIC)

Max Frederico Guedes Pereira (Diretor da Secretaria de Governança e Gestão Estratégica)

Ricardo José de Medeiros II (Agente responsável pela ETIR)

Rodrigo Cartaxo Marques Duarte (Diretor da SETIC)

Rodrigo Mafra (Assessor de Governança de SI e Proteção de Dados Pessoais)

Simone Farias Perrusi (Secretária-Geral da Presidência)

Tibério Adonys de Almeida Fialho (Assessor Jurídico da Presidência)

Secretaria de Governança e Gestão Estratégica

Max Frederico Feitosa Guedes Pereira (Diretor)

Rodrigo Mafra (Assessor de Governança de SI e Proteção de Dados Pessoais)

SUMÁRIO

1. Objetivo

Definir o Processo de Gestão de Incidentes de Segurança da Informação.

2. Propósito do processo

Este processo tem como propósito definir a gestão de incidentes de Segurança da Informação no âmbito do Tribunal Regional do Trabalho – 13ª Região, garantindo que os mesmos sejam monitorados, detectados, comunicados, analisados e tratados.

3. Escopo

O escopo do processo compreende os serviços de TIC, dados pessoais dos servidores, magistrados e jurisdicionados, e informações do TRT da 13ª Região.

4. Definições e abreviações

Para efeitos deste manual, aplicam-se as definições da Política de Segurança da Informação e Comunicações e da Política de Proteção de Dados Pessoais, além das seguintes:

- **Incidente de Segurança da Informação:** um evento ou uma série de eventos indesejados ou inesperados, que comprometeram ou tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a Segurança da Informação**;**
- **Ação corretiva:** ação que visa tratar adequadamente um incidente de Segurança da Informação que já ocorreu;
- **Ação preventiva:** ação que visa evitar a ocorrência de incidentes de Segurança da Informação;
- **Dado pessoal:** informação relacionada à pessoa natural identificada ou identificável;
- **Incidente envolvendo dados pessoais:** incidente que envolva dados pessoais armazenados no TRT 13;
- **Incidente de crise cibernética:** incidente em dispositivos, serviços e redes de computadores, que cause dano material ou de imagem, atraia a atenção do público e da mídia, e fuja ao controle direto da organização;
- **Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ) :** órgão técnico do CNJ para assuntos de Segurança da Informação e cibernéticos, composto por uma Rede de Cooperação do Judiciário;
- **Subcomitê Nacional de Comunicação e Acompanhamento de Incidentes Cibernéticos da Justiça do Trabalho (SNCAIC-JT):** equipe coordenada pelo CSJT, responsável pela centralização, comunicação e acompanhamento gerencial de incidentes cibernéticos de relevância nacional;
- **Agência Nacional de Proteção de Dados (ANPD):** Agência Reguladora vinculada ao Ministério da Justiça e Segurança Pública, que tem como missão zelar pela proteção de

dados pessoais orientada pela Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD);

- **Encarregado pelo tratamento de dados pessoais:** pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD);
- **Titular de dados pessoais:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- **Plano de Continuidade de TIC:** subconjunto do Plano de Continuidade de Negócios dedicado aos serviços de TIC que suportam os processos de negócio essenciais da instituição.

5. Benefícios esperados

A implementação do Processo de Gestão de Incidentes de Segurança da Informação no TRT da 13ª Região promoverá os seguintes benefícios:

- Aumento da disponibilidade dos serviços de TIC, uma vez que se diminuirá o risco e/ou tempo de parada após a ocorrência de incidentes de Segurança da Informação;
- Aderência à Política de Segurança da Informação e Comunicações (POSIC) da instituição, promovendo a confidencialidade, disponibilidade e integridade das informações;
- Aderência à Lei Geral de Proteção de Dados Pessoais;
- Aderência à Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
- Atendimento de recomendações referentes à auditoria coordenada pelo CSJT para avaliação da gestão de Segurança da informação no âmbito da Justiça do Trabalho de 1º e 2º graus (PROAD 6227/2022);
- Aderência ao Processo de Comunicação de Incidentes Cibernéticos na Justiça do Trabalho (PROAD 7916/2025);
- Atendimento de recomendações referentes à auditoria coordenada pelo TCU para diagnóstico acerca dos controles implementados por organizações públicas federais para adequação à Lei Geral de Proteção de Dados Pessoais (PROAD 6471/2025).

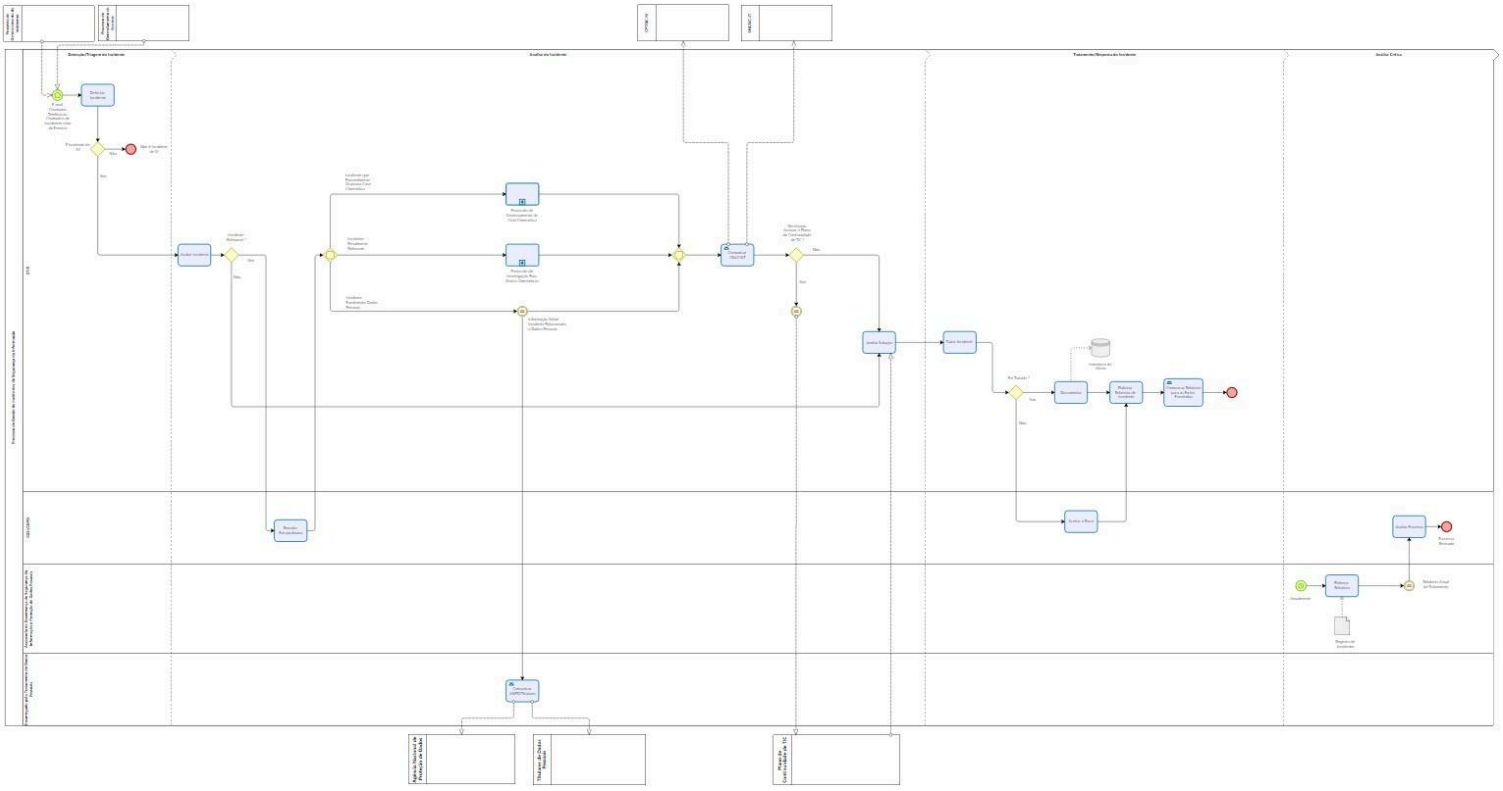
6. Interfaces com processos, planos e atores externos

- **Plano de Continuidade de TIC**: dependendo do incidente de Segurança da Informação, poderá ser acionada a execução do Plano de Continuidade de TIC;
- **Processo de Gerenciamento de Incidentes**: caso um incidente registrado seja um possível incidente de Segurança da Informação, a equipe responsável acionará o PGISI;
- **Processo de Gerenciamento de Eventos**: caso um evento seja um possível incidente de Segurança da Informação, a equipe responsável acionará o PGISI;

- **Agência Nacional de Proteção de Dados (ANPD):** acionada no caso de haver uma violação relevante em termos de dados pessoais;
- **Titulares de dados pessoais:** acionados no caso de haver uma violação relevante em termos de dados pessoais dos quais são titulares;
- **Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ)**: acionado em caso de incidentes relevantes;
- **Subcomitê Nacional de Comunicação e Acompanhamento de Incidentes Cibernéticos da Justiça do Trabalho (SNCAIC-JT):** acionado em caso de incidentes relevantes.

7. O Processo de Gestão de Incidentes de Segurança da Informação

7.1 Diagrama do Processo



7.2 Atividades

Detectar Incidente	
Objetivo	Detectar incidentes suspeitos de serem incidentes de Segurança da Informação.
Descrição	• A ETIR verifica se o chamado, e-mail ou ligação telefônica é um incidente de Segurança da Informação, conforme a Tabela Categorias de Incidentes de Segurança da Informação (Anexo I); • Caso seja um incidente de SI, deve-se registrar em sistema e enviar para a atividade Avaliar Incidente. Caso contrário, devolver o chamado, e-mail ou retornar a ligação telefônica.
Observações	A informação do chamado, e-mail ou ligação deve ser registrada em sistema e deve conter: • Nome do usuário; • E-mail do usuário; • Dados do incidente (descrição e qualquer informação relevante sobre o incidente); • Telefone/ramal, setor, anexos (*logs*, imagens, arquivos ou qualquer objeto relevante para o incidente); • Data da ocorrência (data da primeira ocorrência identificada); • Hora da ocorrência (hora da primeira ocorrência); • Serviços afetados (conforme catálogo de serviços de TIC);
Papéis	ETIR
Entradas	Chamados de eventos ou incidentes, e-mail, chamadas telefônicas.
Saídas	Chamado de incidente de Segurança da Informação.
Modelos	Tabela Categorias de Incidentes de Segurança da Informação (Anexo I).

Avaliar Incidente	
Objetivo	Avaliar se o incidente é relevante ou não.

Descrição	Avaliar o incidente de Segurança da Informação quanto ao seu nível de gravidade, sugerir possíveis soluções e acrescentar informações pertinentes. **Para incidentes relevantes:** Os incidentes relevantes podem ser dos tipos : ● Incidente envolvendo dados pessoais ○ Ação: Informar ao Encarregado sobre o incidente envolvendo dados pessoais, para que este comunique à ANPD/Titulares; ● Incidente que possivelmente ocasiona crise cibernética ○ Ação: Acionar o Protocolo de Gerenciamento de Crises Cibernéticas; ● Incidente penalmente relevante ○ Ação: Acionar o Protocolo de Investigação para Ilícitos Cibernéticos. Esses tipos não são excludentes, ou seja, podem ocorrer simultaneamente. Após a avaliação, ir para atividade Reunião Extraordinária. De acordo com o tipo de incidente, deverá ser acionado o protocolo de segurança cibernética correspondente, instituído por Ato da Presidência do Tribunal. Deve-se verificar a necessidade de acionar o Plano de Continuidade de TIC. Após, ir para a atividade Comunicar CNJ/CSJT. **Para incidentes não relevantes:** Em caso de não ser um incidente relevante, ir para atividade Avaliar Solução.
Observações	● Na avaliação da relevância, considerar o risco atrelado ao incidente e a Tabela de Classificação do Nível de Gravidade de Incidentes de Segurança da Informação (Anexo II); ● Incidentes avaliados com gravidade média, alta ou crítica devem ser considerados relevantes; ● Providenciar a realização de cópias de segurança atualizadas e segregadas, de forma automática e em local protegido, em formato que permita a investigação de incidentes;

	● Caso seja um incidente na nuvem, especificar nas informações do incidente; ● Caso necessária, a informação para o Encarregado pelo tratamento de dados pessoais deve ocorrer em um prazo razoável, contendo no mínimo: ○ A descrição da natureza dos dados pessoais afetados; ○ As informações sobre os Titulares envolvidos; ○ A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; ○ Os riscos relacionados ao incidente; ○ Os motivos da demora, no caso da comunicação não ter sido imediata; ○ As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
Papéis	ETIR
Entradas	Incidente de Segurança da Informação.
Saídas	Incidente avaliado.
Modelos	Tabela de Classificação do Nível de Gravidade de Incidentes de Segurança da Informação (Anexo II). Protocolos de Segurança Cibernética https://www.trt13.jus.br/institucional/gestao-estrategica/seguranca-da-informacao/SGSI/seguranca-cibernetica

Realizar Reunião Extraordinária	
Objetivo	Realizar a reunião extraordinária para tomar as decisões pertinentes sobre o incidente relevante.
Descrição	● O CGSI/CGPD convoca todos os seus membros para participarem da reunião de forma urgente e decidir quais ações e decisões pertinentes serão tomadas sobre o incidente relevante.
Observações	● Na reunião, o CGSI/CGPD deverá deliberar sobre: ○ Necessidade de suspensão dos serviços afetados; ○ Ações pertinentes para resposta ao incidente;

	○ Plano de comunicação sobre o incidente, a ser executado pela ACS; ○ Outros pontos relevantes.
Papéis	CGSI/CGPD
Entradas	Incidente avaliado.
Saídas	Ata da reunião.
Modelos	N/A

Comunicar ANPD/Titulares	
Objetivo	Comunicar à ANPD e aos Titulares de dados pessoais sobre o incidente relevante envolvendo dados pessoais.
Descrição	● O Encarregado pelo tratamento de dados pessoais comunicará à ANPD e aos Titulares sobre o incidente.
Observações	● A comunicação de incidente à ANPD deve ser realizada pelo Encarregado ou por um representante legalmente constituído do Controlador, por peticionamento eletrônico via Sistema Eletrônico de Informações da ANPD; ● A comunicação à ANPD e ao Titular deve observar o prazo de três (3) dias úteis da identificação do incidente, ressalvada a existência de prazo para comunicação previsto em legislação específica; ● A comunicação deve ser feita de forma individual e diretamente aos Titulares, sempre que possível. Pode ser realizada por quaisquer meios tais como e-mail, SMS, carta ou mensagem eletrônica e, preferencialmente, através do canal já habitualmente utilizado pelo TRT13 para se comunicar com o Titular; ● Se não for possível individualizar os Titulares afetados, pode ser necessário comunicar a todos cujos dados estejam presentes na base de dados violada; ● Excepcionalmente, e de forma justificada, pode ser feita a comunicação indireta aos Titulares por meio de publicação em meios de comunicação. O meio utilizado deve ser capaz de alcançar o maior número possível de Titulares, e deve ser dado o devido destaque à divulgação; ● O comunicado aos Titulares deve utilizar linguagem clara e conter, ao menos, as seguintes informações:

	○ Resumo e data de ocorrência do incidente; ○ Descrição dos dados pessoais afetados; ○ Riscos e consequências aos titulares de dados; ○ Medidas tomadas e recomendadas para mitigar seus efeitos, se cabíveis; ○ Dados de contato do Controlador para obtenção de informações adicionais sobre o incidente.
Papéis	Encarregado pelo tratamento de dados pessoais
Entradas	Informações sobre incidente relacionado a dados pessoais.
Saídas	Comunicado à ANPD/Titulares.
Modelos	Procedimento para Comunicação de Incidente à ANPD https://www.trt13.jus.br/institucional/lgpd/legislacao/governo-federal/procedimento-para-comunicacao-de-incidente-a-anpd Formulário de Comunicação de Incidente à ANPD https://www.trt13.jus.br/institucional/lgpd/legislacao/governo-federal/formulario-de-comunicacao-de-incidente-a-anpd Regulamento ANPD de Comunicação de Incidente de Segurança https://www.trt13.jus.br/institucional/lgpd/legislacao/governo-federal/regulamento-anpd

Comunicar CNJ/CSJT	
Objetivo	Comunicar ao CNJ e ao CSJT sobre o incidente relevante.
Descrição	● O responsável pela ETIR comunicará ao CNJ e ao CSJT sobre o incidente.
Observações	● A comunicação de incidente ao CNJ deve ser realizada pela ETIR por meio do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ); ● A comunicação de incidente ao CSJT deve ser realizada pela ETIR por meio do Subcomitê Nacional de Comunicação e Acompanhamento de Incidentes Cibernéticos da Justiça do Trabalho (SNCAIC-JT); ● O comunicado deve observar o Processo de Comunicação de Incidentes Cibernéticos na Justiça do Trabalho (PCIC); ● O comunicado deve conter, ao menos, as seguintes informações:

	○ Descrição sucinta do incidente; ○ Data e hora da ocorrência ou da detecção; ○ Produtos ou ativos afetados; ○ Classificação da gravidade do incidente; ○ Impactos observados; ○ Providências iniciais adotadas; ○ Tipo de incidente; ○ Evidências coletadas.
Papéis	ETIR
Entradas	Informações sobre o incidente relevante.
Saídas	Comunicado ao CNJ/CSJT.
Modelos	Processo de Comunicação de Incidentes Cibernéticos na Justiça do Trabalho https://www.trt13.jus.br/institucional/gestao-estrategica/seguranca-da-informacao/legislacao/csjt/processo-comunicacao Regulamento CPTRIC-PJ https://www.trt13.jus.br/institucional/gestao-estrategica/seguranca-da-informacao/legislacao/cnj/portaria-cnj

Avaliar Solução	
Objetivo	Investigar o incidente de Segurança da Informação e propor solução viável para o tratamento do mesmo.
Descrição	● Coletar todas as informações pertinentes ao incidente de Segurança da Informação: causas, impacto, serviços afetados, ativos envolvidos, etc; ● Formular soluções (ações corretivas e preventivas) e avaliar a viabilidade das mesmas para o tratamento do incidente de Segurança da Informação. As mesmas devem ser testadas, preferencialmente, em ambiente de teste controlado, considerando os possíveis impactos e os recursos necessários. A solução escolhida deve conter os os procedimentos detalhados de implementação e de *rollback*; ● Avaliar a viabilidade da solução proposta para o tratamento do incidente de Segurança da Informação; ● Aprovar a solução proposta, fazendo os ajustes necessários, ou não aprovar, aceitando os riscos.

Observações	N/A
Papéis	ETIR
Entradas	Incidente avaliado.
Saídas	Incidente com solução aprovada.
Modelos	N/A

Tratar Incidente	
Objetivo	Realizar o tratamento do incidente de Segurança da Informação, aplicando a solução aprovada.
Descrição	• Realizar as ações corretivas e preventivas necessárias para o tratamento do incidente de Segurança da Informação, de acordo com a solução aprovada; • Atualizar o incidente com as informações pertinentes; • Ir para a atividade Documentar, caso o incidente seja tratado com sucesso; • Ir para a atividade Aceitar o Risco, caso o incidente não seja tratado.
Observações	N/A
Papéis	ETIR
Entradas	Incidente com solução aprovada.
Saídas	Incidente tratado ou não.
Modelos	N/A

Documentar	
Objetivo	Atualizar a Base de Conhecimento e o Inventário de Ativos, quando for o caso.

Descrição	● Quando o incidente de Segurança da Informação for tratado, registrar na Base de Conhecimento os procedimentos adotados e outras informações pertinentes; ● Quando necessário, atualizar as informações no Inventário de Ativos para os ativos de TIC afetados no tratamento do incidente de Segurança da Informação. A documentação servirá de base para a elaboração do relatório do incidente.
Observações	● Colocar na documentação a solução, os riscos envolvidos, os ativos que foram afetados ou pessoas afetadas.
Papéis	ETIR
Entradas	Incidente tratado.
Saídas	Incidente tratado junto com a sua documentação.
Modelos	N/A

Elaborar Relatório de Incidente	
Objetivo	Elaborar Relatório de incidente tratado e não tratado
Descrição	● Elaborar relatório contendo: ○ As informações sobre o tipo do chamado, se houver; ○ A solução aprovada e aplicada; ○ Riscos do incidente, se houver; ○ Ativação do Plano de Continuidade de TIC, se aplicável; ○ Relatório de Comunicação de Incidente de Segurança da Informação/Cibernética, contendo a descrição e o detalhamento da crise e o plano de ação tomado; ○ Lições aprendidas, caso seja um incidente que envolva crise cibernética, vazamento de dados pessoais ou ilícitos cibernéticos; ● No caso específico de incidente não tratado ele deve conter : ○ Documentação do incidente não tratado; ○ Informações sobre os riscos ; ○ Solução aplicada e aprovada; ○ Quais as causas para o não tratamento do incidente; ○ Possíveis impactos do incidente não tratado.

Observações	N/A
Papéis	ETIR
Entradas	Incidente e sua documentação.
Saídas	Relatório de incidente.
Modelos	N/A

Comunicar Relatório para as Partes Envolvidas	
Objetivo	Comunicar o relatório de incidente para as partes envolvidas e interessadas no tratamento do incidente.
Descrição	● A ETIR dever comunicar o relatório para: ○ SETIC; ○ Assessoria de Governança de Segurança da Informação e Proteção de Dados Pessoais; ○ Comitê Gestor de Segurança da Informação/Comitê Gestor de Proteção de Dados Pessoais; ○ Outras partes envolvidas.
Observações	A comunicação deverá ser feita preferencialmente por e-mail, ou outro meio, desde que fique registrada em algum sistema.
Papéis	ETIR
Entradas	Relatório de incidente.
Saídas	Envio de relatório para as partes interessadas.
Modelos	N/A

Aceitar o Risco	
Objetivo	Aceitar o risco do incidente não tratado.

Descrição	O Comitê de Gestor de Segurança da Informação/Comitê Gestor de Proteção de Dados Pessoais deve avaliar e aprovar o risco inerente ao incidente não tratado.
Observações	N/A
Papéis	CGSI/CGPD
Entradas	Relatório de Incidente não tratado.
Saídas	Risco avaliado e aceito.
Modelos	N/A

Elaborar Relatório	
Objetivo	Elaborar Relatório Anual de Tratamento de Incidentes de Segurança da Informação e informar ao Comitê Gestor de Segurança da Informação.
Descrição	• Consultar os chamados sobre tratamento de incidentes de Segurança da Informação registrados no ano; • Consultar os relatórios sobre os incidentes tratados e não tratados; • Calcular os indicadores do processo; • Elaborar relatório com as informações obtidas; • Encaminhar e apresentar o relatório ao Comitê Gestor de Segurança da Informação.
Observações	N/A
Papéis	AGSIPD
Entradas	Registro de incidentes, relatórios.
Saídas	Relatório Anual de Tratamento de Incidentes.
Modelos	N/A

Avaliar Processo

Objetivo	Avaliar criticamente o processo e propor mudanças.
Descrição	• Avaliar os indicadores do processo; • Propor alterações no processo, caso seja necessário.
Observações	N/A
Papéis	CGSI/CGPD
Entradas	Relatório Anual de Tratamento de Incidentes de Segurança da Informação.
Saídas	Revisão do processo, quando necessário.
Modelos	N/A

8. Entradas e saídas

As principais entradas e saídas do Processo de Gestão de Incidentes de Segurança da Informação são:

8.1 Entradas

- Chamados de Incidentes;
- Chamados de Eventos;
- E-mail;
- Telefonemas.

8.2 Saídas

- Relatório de Incidente não tratado;
- Relatórios de incidentes;
- Relatório Anual de Tratamento de Incidentes de Segurança da Informação.

9. Papéis e responsabilidades

Abaixo estão definidos os papéis, seus executores e suas responsabilidades:

PAPEL	DESCRIÇÃO	RESPONSABILIDADES
Comitê Gestor de Segurança da Informação (CGSI)	Comitê multidisciplinar formado por magistrados e servidores, de assessoramento da Administração na área de Segurança da Informação.	● Analisar e manifestar-se sobre o Processo de Gestão de Incidentes de Segurança da Informação, apoiando a Presidência na avaliação do processo; ● Realizar reunião extraordinária; ● Aceitar o risco do incidente não tratado.
Comitê Gestor de Proteção de Dados Pessoais (CGPD)	Comitê multidisciplinar formado por magistrados e servidores, de assessoramento da Administração na área de Proteção de Dados Pessoais.	● Analisar e manifestar-se sobre o Processo de Gestão de Incidentes de Segurança da Informação, apoiando a Presidência na avaliação do processo; ● Realizar reunião extraordinária; ● Aceitar o risco do incidente envolvendo dados pessoais não tratado.
Encarregado pelo Tratamento de Dados Pessoais	Magistrado indicado pela Presidência do Tribunal para atuar como canal de comunicação entre a instituição, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD).	● Comunicar à ANPD e aos Titulares de dados pessoais sobre incidentes envolvendo dados pessoais.
Assessoria de Governança de SI e Proteção de Dados Pessoais (AGSIPD)	Unidade responsável pelo macroprocesso de Segurança da Informação e pelo Processo de Gestão de Incidentes de Segurança da Informação.	● Fazer o Relatório Anual de Tratamento de Incidentes de Segurança da Informação; ● Assessorar o Comitê Gestor de Segurança da Informação/Comitê Gestor de Proteção de Dados Pessoais na análise e na tomada de decisões a respeito do Processo de Gestão de Incidentes de Segurança da Informação; ● Gerenciar o Processo de Incidentes de Segurança da Informação e manter documentação relacionada atualizada.

PAPEL	DESCRIÇÃO	RESPONSABILIDADES
Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR)	Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de Segurança da Informação.	• Detectar incidente; • Avaliar os incidentes de Segurança da Informação, determinando as suas causas, possíveis soluções, áreas envolvidas, impacto, etc. • Avaliar e aprovar a solução para o incidente (ações corretivas e preventivas); • Comunicar CNJ/CSJT sobre incidentes relevantes; • Tratar incidente; • Documentar; • Elaborar Relatório de Incidente; • Comunicar Relatório para as partes interessadas; • Elaborar relatório de Incidente não tratado.

10. Indicadores de desempenho

10.1 Eficácia do Processo de Gestão de Incidentes de Segurança da Informação

Indicador 1	
Objetivo	Avaliar a eficácia do Processo de Gestão de Incidentes de Segurança da Informação.
Indicador	Percentual de incidentes de Segurança da Informação tratados em relação ao total de incidentes de Segurança da Informação identificados.
Fórmula de cálculo	(Quantidade total de incidentes de segurança da informação tratados/ quantidade total de incidentes de segurança da informação identificados)*100.
Meta	80%.
Polaridade	Quanto maior melhor.

Responsável pela medição	AGSIPD.
Período de Medição	Anual.

11. Anexos

11.1 Anexo I – Categorias de Incidentes de Segurança da Informação

CATEGORIAS DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO	
CATEGORIA	**DESCRIÇÃO**
Conteúdo abusivo	Envio/recebimento de e-mails não solicitados (*spam*), envio/recebimento/armazenamento de materiais relacionados à difamação, assédio, discriminação, pornografia, pedofilia, entre outros.
Código malicioso	Contaminação de sistemas por *malware*, como vírus, *spyware*, *ransomware*, etc.
Coleta de Informações	Envio de solicitações a sistemas para descobrir vulnerabilidades, configurações ou serviços. Abrange: varredura (processo de testes não solicitados), escuta não autorizada (monitorar ou gravar tráfego de rede sem autorização), engenharia social (obter informações sigilosas de pessoas se utilizando de manipulação, confiança, boa fé).
Tentativa de intrusão	Tentativa de comprometimento ou acesso a sistemas/serviços através de ataques que explorem vulnerabilidades, acesso não autorizado, utilizando força bruta ou não.
Intrusão	Comprometimento bem-sucedido de sistemas por meio da exploração de vulnerabilidades ou de acesso não autorizado.
Indisponibilidade	Indisponibilidade de serviços ou informações, ou incidentes que promovam a exaustão de recursos de hardware, software ou de conectividade. Ex.: Ataques de negação de serviço (DoS), sabotagem, etc.
Fraude	Violação de direitos autorais (cópia, venda, instalação, download ou distribuição de material protegido por direitos autorais), falsificação de identidade, utilização de recursos de TIC de forma não autorizada (correntes de e-mail, servidores de jogos, entre outros).
Desconformidade	Violação das disposições da Política de Segurança da Informação e Comunicação (POSIC) e normas relacionadas.

Nuvem	Incidentes relacionados a sistemas ou serviços que não estão alocados em servidores locais.
Vazamento de dados pessoais	Incidentes relacionados a vazamentos de dados pessoais.
Outros	Incidentes não representados anteriormente que comprometam de alguma forma a integridade, disponibilidade e confidencialidade da informação.

11.2 Anexo II – Tabela de Classificação do Nível de Gravidade de Incidentes de Segurança da Informação

Nível de Gravidade	Descrição
Crítica	Ameaça que compromete totalmente as atividades do órgão, exigindo resposta imediata e integral das equipes responsáveis.
Alta	Ameaça que compromete parcialmente as atividades, exigindo resposta imediata com mobilização significativa de recursos.
Média	Incidente cibernético com impacto moderado, que pode causar atrasos ou retrabalho, devendo ser tratado com prioridade intermediária.
Baixa	Incidente cibernético com impacto localizado e sem prejuízo relevante às atividades.
Muito Baixa	Incidentes cibernéticos de baixa criticidade ou em ativos secundários, que podem ser acompanhados com menor urgência.