Tratamento de incidente cibernético_v2

Bizagi Modeler

Índice

TRATAMENTO DE INCIDENTE CIBERNÉTICO_V2 1
BIZAGI MODELER 1
1 PROCESSO DE TRATAMENTO DE INCIDENTE CIBENÉTICO 3
1.1 PROCESSO DE TRATAMENTO DE INCIDENTE CIBERNÉTICO 5
1.1.1 Elementos do processo 5
1.1.1.1 Abrir registro de indisponibilidade no sistema 5
1.1.1.2 Informar no canal de comunicação de Indisponibilidade 5
1.1.1.3 Notificar suspeita ou ocorrência de incidente cibernético 6
1.1.1.4 Encaminhar p/ unidades responsáveis pelo(s) serviço(s) afetado(s) 6
1.1.1.5 Realizar análise inicial 6
1.1.1.6 Comunicar Central de Atendimento sobre a indisponibilidade do serviço afetado 7
1.1.1.7 Comunicar Partes interessadas sobre o incidente cibernético 7
1.1.1.8 Solicitar divulgação institucional 8
1.1.1.9 Preparar nota para divulgação na instituição 8
1.1.1.10 Divulgar p/usuários internos 9
1.1.1.11 Divulgar p/usuários externos 9
1.1.1.12 Tratar o incidente no ativo/serviço de TI afetado 9
1.1.1.13 Atualizar a AGSI sobre o tratamento do incidente no serviço afetado 10
1.1.1.14 Atualizar partes interessadas sobre o tratamento do incidente 10
1.1.1.15 Comunicar Partes interessadas 11
1.1.1.16 Tratar o incidente 12
1.1.1.17 Preencher formulário RISI com as informações do incidente 13
1.1.1.18 Encaminhar o RISI para a AGSI 13
1.1.1.19 Elaborar relatório com análise final (juntamente c/ STI) 14
1.1.1.20 Encaminhar relatório p/ CLRI 14
2 RECURSOS 16
2.1 CENTRAL DE ATENDIMENTO DA TI (FUNÇÃO) 16
2.2 DETECTOR DO INCIDENTE (FUNÇÃO) 16
2.3 GERENTE DO SERVIÇO / GRUPO SOLUCIONADOR (FUNÇÃO) 16
2.4 DIREÇÃO DA STI (ENTIDADE) 16
2.5 AGSI (ENTIDADE) 16
2.6 COMUNICAÇÃO SOCIAL (ENTIDADE) 16
2.7 CLRI (FUNÇÃO) 16

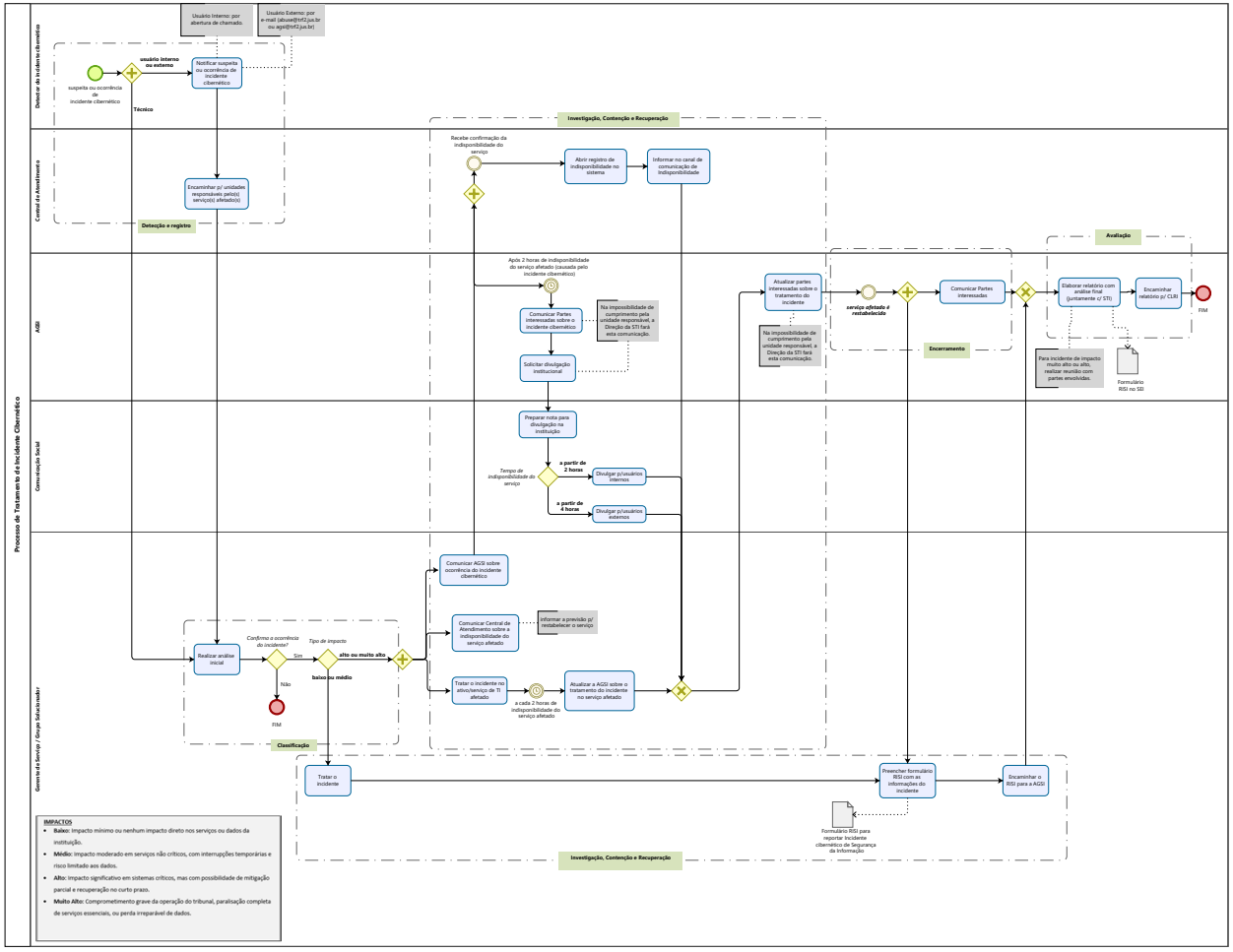
1 PROCESSO DE TRATAMENTO DE INCIDENTE CIBENÉTICO

Processo de Tratamento de Incidente Cibenético

Autor: COGEST/STI

Versão: 1.0 (Ato Normativo Portarias PRES/TRF2 Nº 340/2025 e 859/2025)

Descrição: Tem como objetivo garantir a gestão de incidentes cibernéticos, tratando os incidentes p/ restaurar a operação normal dos serviços com a maior brevidade possível, minimizando prejuízos às atividades institucionais, além de identificar e mitigar riscos e vulnerabilidades, prevenindo a recorrência de incidentes semelhantes.
Atividades (etapas do tratamento de incidentes cibernéticos): detecção e registro; classificação investigação e contenção; recuperação; encerramento e análise.



Descrição
Tem como objetivo garantir a gestão de incidentes cibernéticos, tratando os incidentes p/ restaurar a operação normal dos serviços com a maior brevidade possível, minimizando prejuízos às atividades institucionais, além de identificar e mitigar riscos e vulnerabilidades, prevenindo a recorrência de incidentes semelhantes.

Atividades (etapas do tratamento de incidentes cibernético): detecção e registro; classificação; investigação e contenção; recuperação; encerramento e análise.

Versão:

1.0 (Ato Normativo Portarias PRES/TRF2 Nº 340/2025 e 859/2025)

Autor:

COGEST/STI

1.1 PROCESSO DE TRATAMENTO DE INCIDENTE CIBERNÉTICO

1.1.1 ELEMENTOS DO PROCESSO

1.1.1.1 ☐ Abrir registro de indisponibilidade no sistema

Descrição
Abrir registro de indisponibilidade no sistema

https://status.trf2.jus.br/

Responsável

Central de Atendimento da TI

1.1.1.2 ☐ Informar no canal de comunicação de Indisponibilidade

Descrição
Informar no canal de comunicação de Indisponibilidade na ferramenta Colabora

- grupo #Indisponibilidade 2R

Responsável

Central de Atendimento da TI

1.1.1.3 ☐ Notificar suspeita ou ocorrência de incidente cibernético

Descrição

Informar à TI a suspeita ou a ocorrência de incidente cibernético.

- **Quando detectado por usuários internos:** notificar por um dos canais:
  - abertura de chamado na **Central de Atendimento de TI**; ou
  - e-mail para **tiajuda@trf2.jus.br**, **abuse@trf2.jus.br** ou **agsi@trf2.jus.br**.
- **Quando detectado por usuários externos:** enviar e-mail para **tiajuda@trf2.jus.br**, **abuse@trf2.jus.br** ou **agsi@trf2.jus.br**.
- **Quando detectado tecnicamente (monitoramento/equipe responsável):** a área responsável pelo serviço deve **registrar a ocorrência** e realizar a **análise inicial** do incidente.

Responsável

Detector do incidente

1.1.1.4 ☐ Encaminhar p/ unidades responsáveis pelo(s) serviço(s) afetado(s)

Descrição

Acionar as unidades responsáveis pelos serviços afetados, para que seja realizada a análise inicial, a contenção do incidente e a recuperação do serviço.

Responsável

Central de Atendimento da TI

1.1.1.5 ☐ Realizar análise inicial

Descrição

Realizar a análise inicial do incidente ou suspeita, confirmando a ocorrência, identificando o tipo de incidente e avaliando o impacto nos serviços afetados (definição do nível de criticidade).

Referência: Portaria PRES/TRF2 Nº 340/2025

Art. 9º A etapa de Classificação consiste na avaliação do impacto e priorização de incidentes com base em sua criticidade, conforme especificado nos Anexos I e II deste Protocolo.

ANEXO I - Classificação de Incidentes de Segurança da Informação

- classificação detalhada dos tipos de incidentes de segurança da informação e cibernética que podem ocorrer na JF2R, com o objetivo de facilitar sua identificação, priorização e tratamento.

Anexo II - Tabela de Nível de Criticidade de Incidentes Cibernéticos (muito alta, alta, média e baixa).

Responsável

Gerente do Serviço / Grupo Solucionador

1.1.1.6 ☐ Comunicar Central de Atendimento sobre a indisponibilidade do serviço afetado

Descrição
Comunicar Central de Atendimento sobre a ocorrência do incidente (confirmado)

Responsável

Gerente do Serviço / Grupo Solucionador

1.1.1.7 ☐ Comunicar Partes interessadas sobre o incidente cibernético

Descrição
Comunicar Partes interessadas

Partes Interessadas:

- DIRFO SJRJ e DIRFO SJES.
- Juízes auxiliares da Presidência.

- Diretor-Geral.
- Comunicação Social (responsável pela divulgação).
- GSI
- SAJ
- OAB

O canal único será **Grupo de WhatsApp**, composto por: DIRFO SJRJ e DIRFO SJES; Juízes Auxiliares da Presidência; representante da Comunicação Social do TRF2; Diretor-Geral; representante da GSI; titular e suplente da STI e da AGSI; representante da SAJ.

Executantes

Direção da STI

Responsável

AGSI

1.1.1.8 ☐Solicitar divulgação institucional

Descrição

Solicitar divulgação institucional para a área de Comunicação social.

Responsável

AGSI

1.1.1.9 ☐Preparar nota para divulgação na instituição

Descrição

Preparar nota para divulgação na instituição.

A Comunicação Social deverá divulgar nota oficial:

- Para usuários internos: quando transcorrida 1 hora de indisponibilidade do serviço afetado.

- Para usuários externos: quando transcorridas e 4 horas de indisponibilidade do serviço afetado.

Responsável

Comunicação Social

1.1.1.10 ☐ Divulgar p/usuários internos

Descrição

Divulgar informativo para os usuários internos da instituição.

- divulgar nota oficial para usuários internos, quando transcorrida 1 hora de indisponibilidade do serviço afetado.

Responsável

Comunicação Social

1.1.1.11 ☐ Divulgar p/usuários externos

Descrição

Divulgar informativo para os usuários externos da instituição.

- divulgar nota oficial para usuários externos, quando transcorridas 4 hora de indisponibilidade do serviço afetado.

Responsável

Comunicação Social

1.1.1.12 ☐ Tratar o incidente no ativo/serviço de TI afetado

Descrição

Tratar o incidente no ativo ou serviço de TI afetado, aplicando, quando necessário, ações de contenção, com o objetivo de restabelecer a operação no menor prazo possível.

Referência: Portaria PRES/TRF2 Nº 340/2025

> *Art. 10. A etapa de Investigação compreende a investigação, o* ***tratamento do incidente****, a coleta de dados, a comunicação às áreas afetadas e a proposição* ***e aplicação de ações de contenção****, quando necessário.*
>
> *§ 1º A investigação e o tratamento de incidentes devem ser realizados de forma a garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação, visando ao retorno das operações à normalidade no menor prazo possível e minimização de futuras ocorrências, por meio da proposição de medidas corretivas, quando cabíveis.*
>
> *Art. 11. etapa de Recuperação visa* ***restabelecer os serviços afetados e à comunicação com as partes interessadas.***

Responsável

Gerente do Serviço / Grupo Solucionador

1.1.1.13 ☐ Atualizar a AGSI sobre o tratamento do incidente no serviço afetado

Descrição

Atualizar a AGSI com as informações sobre o tratamento do incidente.

Responsável

Gerente do Serviço / Grupo Solucionador

1.1.1.14 ☐ Atualizar partes interessadas sobre o tratamento do incidente

Descrição

A cada duas horas de indisponibilidade do serviço afetado pelo incidente, atualizar as partes interessadas sobre o tratamento em andamento.

Partes Interessadas:

- DIRFO SJRJ e DIRFO SJES.
- Juízes auxiliares da Presidência.
- Diretor-Geral.
- Comunicação Social (responsável pela divulgação).
- GSI

O canal único será **Grupo de WhatsApp**, composto por: DIRFO SJRJ e DIRFO SJES; Juízes Auxiliares da Presidência; representante da Comunicação Social do TRF2; Diretor-Geral; representante da GSI; titular e suplente da STI e da AGSI.

Executantes

Direção da STI

Responsável

Central de Atendimento da TI

1.1.1.15 ☐Comunicar Partes interessadas

Descrição

Comunicar Partes interessadas sobre restabelecimento da operação do serviço afetado pelo incidente.

Partes Interessadas:

- DIRFO SJRJ e DIRFO SJES.
- Juízes auxiliares da Presidência.
- Diretor-Geral.

- Comunicação Social (responsável pela divulgação).
- GSI
- SAJ
- OAB

O canal único será **Grupo de WhatsApp**, composto por: DIRFO SJRJ e DIRFO SJES; Juízes Auxiliares da Presidência; representante da Comunicação Social do TRF2; Diretor-Geral; representante da GSI; titular e suplente da STI e da AGSI; representante da SAJ.

Executantes

Direção da STI

Responsável

AGSI

1.1.1.16 ☐ Tratar o incidente

Descrição

Tratar o incidente no ativo ou serviço de TI afetado, aplicando, quando necessário, ações de contenção, com o objetivo de restabelecer a operação no menor prazo possível.

Referência: Portaria PRES/TRF2 Nº 340/2025

Art. 10. A etapa de Investigação compreende a investigação, o ***tratamento do incidente****, a coleta de dados, a comunicação às áreas afetadas e a proposição* ***e aplicação de ações de contenção****, quando necessário.*

§ 1º A investigação e o tratamento de incidentes devem ser realizados de forma a garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação, visando ao retorno das operações à normalidade no menor prazo

possível e minimização de futuras ocorrências, por meio da proposição de medidas corretivas, quando cabíveis.

Art. 11. etapa de Recuperação visa ***restabelecer os serviços afetados e à comunicação com as partes interessadas.***

Responsável

Gerente do Serviço / Grupo Solucionador

1.1.1.17 ☐ Preencher formulário RISI com as informações do incidente

Descrição

Preencher formulário do tipo RISI (Relatório de Incidente de Segurança da Informação) no SEI.

Referência: artigo 8º da Portaria PRES/TRF2 Nº 340/2025

§ 1º Todos os incidentes, sejam notificados ou detectados, devem ser registrados para

garantir a manutenção do histórico e auxiliar na geração de indicadores, por meio da elaboração do Relatório

de Incidentes de Segurança da Informação (RISI).

Responsável

Gerente do Serviço / Grupo Solucionador

1.1.1.18 ☐ Encaminhar o RISI para a AGSI

Descrição

Encaminhar o RISI para a AGSI

Responsável

Gerente do Serviço / Grupo Solucionador

1.1.1.19 ☐ Elaborar relatório com análise final (juntamente c/ STI)

Descrição
Elaborar relatório com análise final (juntamente c/ STI).

Referência: Portaria PRES/TRF2 Nº 340/2025

> *Art. 13. Avaliação é o registro e* ***análise do incidente****, com o objetivo de identificar falhas, aprendizados e oportunidades de melhoria, ocorrendo ao final de todo o processo.*
>
> *§ 1º O tratamento de incidentes cibernéticos deverá ser avaliado por meio do seu respectivo histórico, pela Assessoria de Gestão de Segurança da Informação (AGSI), com o apoio da CLRI, visando identificar oportunidades de aprimoramento.*

Executantes

Direção da STI

Responsável

AGSI

Informado

CLRI

1.1.1.20 ☐ Encaminhar relatório p/ CLRI

Descrição
Encaminhar relatório com análise final para a Comissão de Resposta a Incidentes (CLRI)

Referência: Portaria PRES/TRF2 Nº 340/2025

Art. 13. Avaliação é o registro e ***análise do incidente, com o objetivo de identificar falhas, aprendizados e oportunidades de melhoria, ocorrendo ao final de todo o processo.***

§ 1º O tratamento de incidentes cibernéticos deverá ser avaliado por meio do seu respectivo histórico, pela Assessoria de Gestão de Segurança da Informação (AGSI), com o apoio da CLRI, visando identificar oportunidades de aprimoramento.

Responsável

AGSI

2 RECURSOS

2.1 CENTRAL DE ATENDIMENTO DA TI (FUNÇÃO)

Descrição

Central de Atendimento da TI

2.2 DETECTOR DO INCIDENTE (FUNÇÃO)

Descrição

Pessoa que detectou a ocorrência ou suspeita de um incidente.

2.3 GERENTE DO SERVIÇO / GRUPO SOLUCIONADOR (FUNÇÃO)

Descrição

É a equipe técnica responsável pelo serviço/ativo

2.4 DIREÇÃO DA STI (ENTIDADE)

Descrição

Direção da Secretaria de Tecnologia da Informação

2.5 AGSI (ENTIDADE)

Descrição

Assessoria de Gestão de Segurança da Informação

2.6 COMUNICAÇÃO SOCIAL (ENTIDADE)

2.7 CLRI (FUNÇÃO)

Descrição

Comissão de Resposta a Incidentes