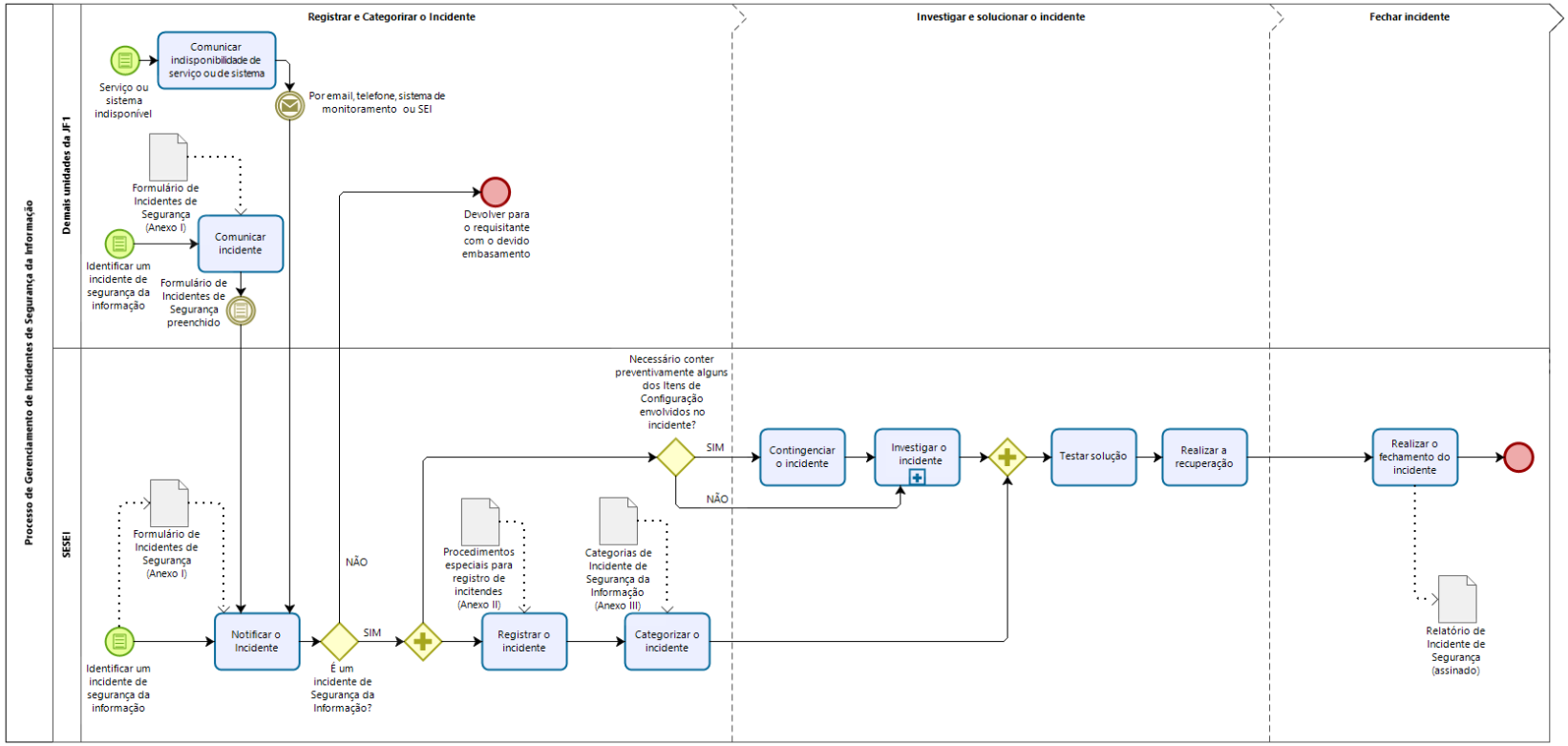
# Processo de Gerenciamento de Incidentes de SI (AS-IS) v1.4

Bizagi Modeler

Índice

# 1 PROCESSO DE GERENCIAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO



Versão:

1.0

Autor:

tr19688ps

# 1.1 PROCESSO DE GERENCIAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Descrição
Este diagrama tem o objetivo de descrever o Processo de Gerenciamento de Incidentes de Segurança da Informação ocorridos no âmbito do Tribunal Regional Federal da 1ª. Região, incluindo suas seções e subseções.

---

## 1.1.1 ELEMENTOS DO PROCESSO

### 1.1.1.1 Serviço ou sistema indisponível

Descrição
A condição para iniciar o processo é que um serviço de rede e/ou sistema esteja indisponível.

### 1.1.1.2 Comunicar indisponibilidade de serviço ou de sistema

Descrição
Quaisquer unidade da JF1 pode identificar incialmente a indisponibilidade de um sistema ou serviço de rede à SESEI, para que possam ser tomadas as medicas cabíveis necessárias para tipificar ou não esta indisponibilidade como Incidente de Segurança da Informação para, posteriormente, executar o tratamento correspondente para restaurar o sistema ou serviço o mais breve possível.

Esta comunicação pode ser realizada por email, por telefone, pelo sistema de monitoramento ou pelo SEI.

### 1.1.1.3 Identificar um incidente de segurança da informação

Descrição
A condição para iniciar o processo é identificação ou indício que um incidente de segurança da informação tenha se concretizado.

### 1.1.1.4 Comunicar incidente

Descrição

Quaisquer unidades da JF1 podem identificar incialmente um incidente de segurança da informações e comunicar a SESEI o mais breve possível para, posteriormente, registrar o incidente e que sejam tomadas as medicas cabíveis necessárias para executar o tratamento com o intuito de restaurar o sistema ou serviço.

A unidade da JF1 deverá preencher o **Formulário de Incidentes de Segurança da Informação** e enviá-lo à SESEI.

### 1.1.1.5 Identificar um incidente de segurança da informação

Descrição
A condição para iniciar o processo é a identificação ou o indício de que um incidente de segurança da informação tenha se concretizado.

### 1.1.1.6 Notificar o Incidente

Descrição
Os incidentes serão recebidos pela SESEI através do preenchimento do Formulário de registro de Incidentes de Segurança da Informação contido no Anexo I do processo de Resposta a Incidentes de Segurança da Informação no âmbito da JF1.

Convém que incidentes que se enquadrem na lista do Anexo II sejam tratados conforme descrições dos procedimentos, visando preservação das informações e completo fornecimento de insumos para um correto tratamento pela SESEI.

### 1.1.1.7 É um incidente de Segurança da Informação?

Descrição
Após o recebimento do incidente pela SESEI deverá ser realizada triagem para decidir se o caso se trata de um incidente de segurança de informação ou de natureza divergente.

Incidentes não identificados como de segurança da informação serão devolvidos para o requisitante com devido embasamento da decisão.

Portões

NÃO

SIM

#### 1.1.1.8 Necessário conter preventivamente alguns dos Itens de Configuração envolvidos no incidente?

### Descrição
Neste momento do processo é definido se será necessário conter preventivamente alguns dos Itens de Configuração envolvidos no incidente ou não.

### Portões

SIM

NÃO

#### 1.1.1.9 Contingenciar o incidente

### Descrição
Tanto a SESEI quanto a unidade da JF1 responsável pelo ativo, serviço ou sistema deverão atuar para contingenciar o incidente, executando as atividades abaixo:

1. Preservar as informações voláteis como conexões de rede estabelecidas, processos existentes, rotas configuradas, usuários logados dentre outras informações;

2. Realizar uma cópia do sistema de arquivos, utilizando a ferramenta DD, dos itens de configuração que proveem o respectivo serviço ou sistema com o intuito de preservar as evidências do incidente;

3. Executar a criptografia Hash (MD5) para gerar a assinatura da imagem gerada da etapa acima e preservar as evidências para futuras análises do incidente ou perícia forense.

4. Habilitar os recursos de monitoramento para detectar ou identificar o *Modus Operandi* utilizado no incidente;

5. Conter o Item de configuração através da implantação deste em uma rede distinta ou configuração especial para prover a rastreabilidade e, consequentemente, evitar maiores impactos ou danos aos demais itens de configuração custodiados pela SECIN.

#### 1.1.1.10 Investigar o incidente

Ver detalhes

### Descrição
Convém tomar como ponto de partida para a investigação as informações inseridas no processo eletrônico relacionado ao incidente de segurança da informação, incluindo o formulário do Anexo I, preenchido pelo responsável do registro do incidente.

Caso necessário a SESEI poderá consultar outras áreas e as pessoas envolvidas no incidente a fim de obtenção de informações detalhadas que auxiliarão nesta fase.

Ações que deverão estar inclusas nesta fase:

· Estabelecer o que ocorreu de errado;

· Entender a ordem cronológica dos eventos associados ao incidente;

· Confirmar o impacto do incidente, incluindo áreas, sistemas e o número de usuários afetados;

· Identificar quais eventos causaram o incidente;

#### 1.1.1.11 ☐Registrar o incidente

Descrição

• Incidentes que forem identificados como de segurança da informação serão registrados via processo eletrônico com classificação de Restrito no SEI, através do endereço eletrônico https://sei.trf1.jus.br .

• Convém que para cada incidente seja criado um processo eletrônico exclusivo.

• Convém que os insumos recebidos junto com o incidente sejam anexados no processo eletrônico relacionado ao incidente, incluindo e-mails, ofícios e relatórios.

• Convém que durante o todo o processo de tratamento do incidente quaisquer artefatos gerados resultantes do trabalho sejam registrados no processo.

Quando percebe-se que o respectivo incidente está associado ao uso indevido de uma estação de trabalho, o procedimento abaixo deverá ser adotado imediatamente no momento da ciência do incidente:

- Identificar os seguintes dados do usuário da estação de trabalho:
  - Matrícula;
  - Nome completo;
  - Lotação;

• □ Notificar o usuário e sua chefia imediata sobre a retenção do equipamento através de e-mail onde deverá conter os dados do usuário e a identificação da estação de

• trabalho;

• □ Recolher o equipamento (gabinete) e não ligar mais. Este procedimento visa preservação da integridade dos dados no disco rígido;

• □ Remover o disco rígido do equipamento e criar uma imagem bit a bit utilizando o aplicativo “dd” do Linux:

  - Ao se montar o disco rígido na estação Linux deverá ser utilizada a opção de montagem read only “-o ro” do aplicativo “mount”

• □ Entregar o arquivo de imagem gerada do disco rígido para a SESEI, junto com o formulário do Anexo I preenchido e um relatório das ações executadas:

  o No relatório deverá constar na literalidade os comandos que foram usados para montagem e geração de imagem do disco rígido;

• □ Devolver a estação do usuário.

#### 1.1.1.12 ☐Categorizar o incidente

Descrição
Convém que os incidentes de segurança da informação sejam categorizados conforme a natureza do evento e de acordo com as categorias abaixo:

• Os incidentes deverão ser categorizados em primeira instância como Intencionais e Não-Intencionais e em seguida serão enquadrados conforme subcategorias abaixo:

  o Incidentes Intencionais:

    • Uso Indevido

      o Malwares;

      o Cópia ilegal de software;

      o Concessão de acesso não autorizado;

      o Spam;

      o Mau uso de banco de dados;

      o Mau uso de sistemas de informação;

    • Ataques de Segurança

      o DoS e DDoS;

      o Flooding;

      o Mailbombs;

    • Fraudes

      o Uso indevido de recursos;

      o Venda de conteúdo pessoal e impróprio;

    • Violação de Privacidade

- Violação de dados pessoais;
- Violação de dados corporativos;
- Violação de e-mail;

- Incidentes Não-Intencionais:
  - Acidentes de Segurança
    - Exposição de credenciais de acesso e senhas;
    - Exposição de dados corporativos;
    - Exposição de sistemas corporativos;

Um incidente poderá sofrer recategorização diversas vezes durante o seu tratamento, conforme novas informações forem surgindo à medida em que se vai aprofundando em sua análise.

#### 1.1.1.13 ☐Testar solução

Descrição
Convém que quando uma solução em potencial for encontrada, seja testada antes de proceder com a recuperação.

#### 1.1.1.14 ☐Realizar a recuperação

Descrição
Dependendo da natureza do incidente e conforme a situação demandar, a SESEI poderá solicitar que áreas envolvidas nas operações dos recursos envolvidos no incidente apliquem a solução para recuperação do ativo.

#### 1.1.1.15 ☐Realizar o fechamento do incidente

Descrição
Convém que o incidente só seja oficialmente fechado após confirmação de aplicação correta da recuperação e satisfação dos usuários finais do recurso/ativo envolvido.

Convém que toda a documentação seja verificada para se certificar de que todo o procedimento foi corretamente documentado.

Convém que seja verificado se a categorização inicial do incidente está correta e pertinente de acordo com toda a informação reunida durante o procedimento. Caso necessário deverá ser alterada para a categoria pertinente.

Convém que seja verificado se a classificação inicial do processo está correta e pertinente de acordo com toda a informação reunida durante o procedimento. Caso necessário deverá ser alterada para a classificação de “Sigiloso”.

Convém que o incidente seja formalmente fechado mediante parecer e assinatura do supervisor da SESEI.

#### 1.1.1.16 Devolver para o requisitante com o devido embasamento

### Descrição

Caso o incidente comunicado ou identificado por quaisquer unidade da JF1 não seja tipificado como Incidente de Segurança da Informação, o requisitante deverá ser comunicado pela SESEI sobre a não classificação deste incidente e contendo o devido embasamento técnico.

#### 1.1.1.17 Formulário de Incidentes de Segurança (Anexo I)

### Descrição

A SESEI definiu o Formulário de registro de Incidentes de Segurança da Informação que deve ser preenchido por quaisquer unidade da JF1 caso queira comunicar formalmente um possível incidente de segurança da informação em um item de configuração ou ativo de rede provido ou custodiado em sua respectiva unidade judiciária.

Deve ser informado no formulário:

- Data da Ocorrência;
- Data de Percepção;
- Local de ocorrência (físico);
- Local de ocorrência (lógico);
- Dados de quem reportou o incidente como nome, matrícula, email e telefone;
- Dados de quem tratou inicialmente o incidente como nome, matrícula, email e telefone;
- Método de Notificação;
- Tempo que o serviço ficou/está indisponível;
- Descrição dos sintomas do incidente;
- Diagnóstico inicial;
- Descrição das ações tomadas até o momento.

### Ações de apresentação

FORMULARIO - INCIDENTE DE SEGURANCA DA INFORMACAO - v1.docx

1.1.1.18 Categorias de Incidente de Segurança da Informação (Anexo III)

Descrição
Convém que os incidentes de segurança da informação sejam categorizados conforme a natureza do evento e de acordo com as categorias abaixo:

- Os incidentes deverão ser categorizados em primeira instância como Intencionais e Não-Intencionais e em seguida serão enquadrados conforme subcategorias abaixo:
  - Incidentes Intencionais:
    - Uso Indevido
      - Malwares;
      - Cópia ilegal de software;
      - Concessão de acesso não autorizado;
      - Spam;
      - Mau uso de banco de dados;
      - Mau uso de sistemas de informação;
    - Ataques de Segurança
      - DoS e DDoS;
      - Flooding;
      - Mailbombs;
    - Fraudes
      - Uso indevido de recursos;
      - Venda de conteúdo pessoal e impróprio;
    - Violação de Privacidade
      - Violação de dados pessoais;
      - Violação de dados corporativos;
      - Violação de e-mail;

- Incidentes Não-Intencionais:
  - Acidentes de Segurança
    - Exposição de credenciais de acesso e senhas;
    - Exposição de dados corporativos;
    - Exposição de sistemas corporativos;

1.1.1.19 Relatório de Incidente de Segurança (assinado)

Descrição
Convém que o incidente seja formalmente fechado mediante parecer e assinatura do supervisor da SESEI.

1.1.1.20 Procedimentos especiais para registro de incitendes (Anexo II)

Descrição
**Procedimentos especiais para registros de incidentes**

***Uso indevido envolvendo estação de trabalho***

Quando percebe-se que o respectivo incidente está associado ao uso indevido de uma estação de trabalho, o procedimento abaixo deverá ser adotado imediatamente no momento da ciência do incidente:

- Identificar os seguintes dados do usuário da estação de trabalho:
  - Matrícula;
  - Nome completo;
  - Lotação;
- · Notificar o usuário e sua chefia imediata sobre a retenção do equipamento através de e-mail onde deverá conter os dados do usuário e a identificação da estação de
- trabalho;

- · Recolher o equipamento (gabinete) e não ligar mais. Este procedimento visa preservação da integridade dos dados no disco rígido;

- · Remover o disco rígido do equipamento e criar uma imagem bit a bit utilizando o aplicativo “dd” do Linux:

    - Ao se montar o disco rígido na estação Linux deverá ser utilizada a opção de montagem read only “-o ro” do aplicativo “mount”

- · Entregar o arquivo de imagem gerada do disco rígido para a SESEI, junto com o formulário do Anexo I preenchido e um relatório das ações executadas:

    - No relatório deverá constar na literalidade os comandos que foram usados para montagem e geração de imagem do disco rígido;

- · Devolver a estação do usuário.

#### 1.1.1.21 Formulário de Incidentes de Segurança (Anexo I)

### Descrição

A SESEI definiu o Formulário de regisrto de Incidentes de Segruança da Informação que deve ser preenchido por quaisquer unidade da JF1 caso queira comunicar formalmente um possível incidente de segurança da informação em um item de configuração ou ativo de rede provido ou custodiado em sua respectiva unidade judiciária.

Deve ser informado no formulário:

- Data da Ocorrência;
- Data de Percepção;
- Local de ocorrência (físico);
- Local de ocorrência (lógico);
- Dados de quem reportou como nome, matrícula, email e telefone;
- Dados de quem tratou inicialmente como nome, matrícula, email e telefone;
- Método de Notificação;
- Tempo que o serviço ficou/está indisponível;
- Descrição dos sintomas do incidente;
- Diagnóstico inicial;

• Descrição das ações tomadas até o momento.

### Ações de apresentação

FORMULARIO - INCIDENTE DE SEGURANCA DA INFORMACAO - v1.docx

#### 1.1.1.22 Demais unidades da JF1

### Descrição

Quaisquer unidade da Justiça Federal da Primeira Região - JF1 deve comunicar imediatamente à SESEI os incidentes de segurança da informação ocorridos ou cometidos em suas respectivas unidades para, posteriormente, sejam executadas as etapas de registro, de classificação, de análise, de teste e de solução do incidente sobre orientação da Seção de Segurança da Informação - SESEI.

#### 1.1.1.23 SESEI

### Descrição

Seção de Segurança da Informação - SESEI

• Finalidade:

o Propor as políticas e diretrizes de Tecnologia da Informação – TI referentes à segurança da informação digital no âmbito da Justiça Federal da Primeira Região – JF1, coordenar as ações e os investimentos delas decorrentes no TRF1 e orientá-los nas seções e subseções judiciárias, de modo a dotar a JF1 de segurança da informação digital que sustente e alavanque as suas estratégias e resultados

• Competência - Dentre as diversas competências da SESEI, destacam-se:

o Propor a elaboração e atualização e acompanhar as políticas, planejamentos, diretrizes, procedimentos, padrões, metodologias e normas que orientem e disciplinem a segurança da informação digital no âmbito da JF1.

o Monitorar e avaliar os desempenhos, indicadores, riscos e demais controles internos referentes à segurança da informação digital no âmbito da JF1, em conjunto com as unidades de TI das seções e subseções judiciárias.

o Prover segurança da informação digital compatível com as necessidades da JF1, de acordo com o catálogo de serviços, níveis de serviço e procedimentos de TI estabelecidos

o Orientar tecnicamente as unidades de segurança da informação digital da JF1.

#### 1.1.1.24 Registrar e Categorirar o Incidente

### Descrição

Nesta fase ocorre ou não a comunicação, o registro e a classificação dos incidentes de segurança da informação comunicados ou indentificados por quaisquer unidade da JF1.

#### 1.1.1.25 Investigar e solucionar o incidente

### Descrição

Nesta fase é realizada a investigação do incidente para, posteriormente, propor as soluções identificadas para recuperar e restaurar o serviço de rede ou sistema envolvido no incidente de Segurança da Informação.

#### 1.1.1.26 Fechar incidente

### Descrição
Nesta fase é realizado o fechamento do incidente.

#### 1.1.1.27 Demais unidades da JF1

### Descrição
Quaisquer unidade da Justiça Federal da Primeira Região - JF1 deve comunicar imediatamente à SESEI os incidentes de segurança da informação ocorridos ou cometidos em suas respectivas unidades para, posteriormente, sejam executadas as etapas de registro, de classificação, de análise, de teste e de solução do incidente sobre orientação da Seção de Segurança da Informação - SESEI.

#### 1.1.1.28 SESEI

### Descrição
Seção de Segurança da Informação - SESEI

- Finalidade:
  - Propor as políticas e diretrizes de Tecnologia da Informação – TI referentes à segurança da informação digital no âmbito da Justiça Federal da Primeira Região – JF1, coordenar as ações e os investimentos delas decorrentes no TRF1 e orientá-los nas seções e subseções judiciárias, de modo a dotar a JF1 de segurança da informação digital que sustente e alavanque as suas estratégias e resultados

- Competência - Dentre as diversas competências da SESEI, destacam-se:
  - Propor a elaboração e atualização e acompanhar as políticas, planejamentos, diretrizes, procedimentos, padrões, metodologias e normas que orientem e disciplinem a segurança da informação digital no âmbito da JF1.
  - Monitorar e avaliar os desempenhos, indicadores, riscos e demais controles internos referentes à segurança da informação digital no âmbito da JF1, em conjunto com as unidades de TI das seções e subseções judiciárias.
  - Prover segurança da informação digital compatível com as necessidades da JF1, de acordo com o catálogo de serviços, níveis de serviço e procedimentos de TI estabelecidos
  - Orientar tecnicamente as unidades de segurança da informação digital da JF1.

#### 1.1.1.29 Registrar e Categorirar o Incidente

### Descrição
Nesta fase ocorre ou não a comunicação, o registro e a classificação dos incidentes de segurança da informação comunicados ou indentificados por quaisquer unidade da JF1.

#### 1.1.1.30 Investigar e solucionar o incidente

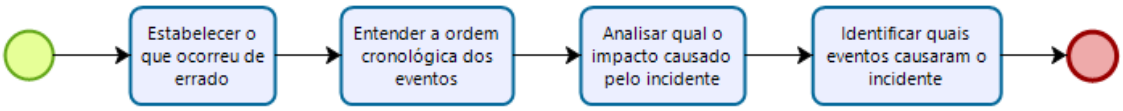
Descrição
Nesta fase é realizada a investigação do incidente para, posteriormente, propor as soluções identificadas para recuperar e restaurar o serviço de rede ou sistema envolvido no incidente de Segurança da Informação.

#### 1.1.1.31 Fechar incidente

Descrição
Nesta fase é realizado o fechamento do incidente.

## 1.2 INVESTIGAR O

## 1.3 INCIDENTE




Powered by bizagi Modeler

### 1.3.1 ELEMENTOS DO PROCESSO

#### 1.3.1.1 Estabelecer o que ocorreu de errado

Descrição
Durante a investigação do incidente, tanto a SESEI quanto a unidade responsável pelo IC, sistema ou serviço, deverá ser estabelecido o que ocorreu de errado que contribuiu para concretizar o incidente de segurança da informação.

#### 1.3.1.2 Entender a ordem cronológica dos eventos

Descrição
Durante a investigação do incidente, tanto a SESEI quanto a unidade responsável pelo IC, sistema ou serviço, deverá ,através das evidências encontradas, estabelecer a ordem cronológica dos eventos que contribuiu diretamente para concretizar o respectivo incidente de segurança da informação.

#### 1.3.1.3 Analisar qual o impacto causado pelo incidente

### Descrição

Durante a investigação do incidente, tanto a SESEI quanto a unidade responsável pelo IC, sistema ou serviço, deverá analisar qual o impacto causado com a concretização do incidente de segurança da informação.

#### 1.3.1.4 ☐ Identificar quais eventos causaram o incidente

### Descrição

Durante a investigação do incidente, tanto a SESEI quanto a unidade responsável pelo IC, sistema ou serviço, deverá ser identificados quais os eventos ou vulnerabilidades contribuiu diretamente para concretizar o respectivo incidente de segurança da informação.