Gestão de vulnerabilidades de TIC_ 11-06-2024

Bizagi Modeler

Índice

GESTÃO DE VULNERABILIDADES DE TIC_ 11-06-2024 1
BIZAGI MODELER 1
1 FLUXO PRINCIPAL 12
1.1 SETIC - GESTÃO DE VULNERABILIDADES DE TIC 13
1.1.1 Elementos do processo 13
1.1.1.1  Início do ciclo de gestão contínua 13
1.1.1.2  Processo de gestão contínua de vulnerabilidades 13
1.1.1.3  Existem vulnerabilidades a serem analisadas? 14
1.1.1.4  Final do ciclo de gestão contínua 14
1.2 MAIN PROCESS 14
1.2.1 Elementos do processo 14
1.2.1.1  Activity 14
1.3 SUBPROCESSO 15
1.3.1 Elementos do processo 15
1.3.1.1  Necessidade de análise por demanda 15
1.3.1.2  Análise de vulnerabilidades por demanda 15
1.3.1.3  Vulnerabilidades tratadas 16
2 PROCESSO DE GESTÃO CONTÍNUA DE VULNERABILIDADES 17
2.1 PROCESSO DE GESTÃO CONTÍNUA DE VULNERABILDADADES 18
2.1.1 Elementos do processo 18
2.1.1.1  Necessidade de monitoramento de vulnerabilidades 18
2.1.1.2  Preparação da gestão contínua 18
2.1.1.3  Identificação de vulnerabilidades 18
2.1.1.4  Analisar e priorizar vulnerabilidades 19
2.1.1.5  Gateway 19
2.1.1.6  Solicitação de análise e remediação 19
2.1.1.7  Gateway 20
2.1.1.8  Reavaliação e monitoramento 20
2.1.1.9  Monitoramento de vulnerabilidades realizado 20

2.1.1.10  Monitoramento de correções 20
2.1.1.11  DataStore 21
2.1.1.12  Coordenadoria de Seg. da Informação de TIC 21
2.2 MAIN PROCESS 21
2.3 AJUSTE EM ROTINA DE VERIFICAÇÃO PERIÓDICA 22
2.3.1 Elementos do processo 22
2.3.1.1  Necessidade de ajuste em rotinas de verificação periódica 22
2.3.1.2  Ajuste em rotinas de verificação periódica 22
2.3.1.3  Ajuste realizado 22
3 PREPARAÇÃO DA GESTÃO CONTÍNUA 24
3.1 PREPARAÇÃO DA GESTÃO CONTÍNUA 25
3.1.1 Elementos do processo 25
3.1.1.1  Necessidade de monitoramento de ativos 25
3.1.1.2  Gateway 25
3.1.1.3  Configurar rotinas periódicas de identificação de vulnerabilidades 25
3.1.1.4  Gateway 25
3.1.1.5  Rotinas periódicas agendadas e agentes instalados 26
3.1.1.6  Configurar ativos 26
3.1.1.7  Coordenadoria de Seg. da Informação de TIC 26
3.1.1.8  Unidade responsável por ativo de TIC 26
4 IDENTIFICAÇÃO DE VULNERABILIDADES 27
4.1 IDENTIFICAÇÃO DE VULNERABILIDADES 28
4.1.1 Elementos do processo 28
4.1.1.1  Agendamento definido 28
4.1.1.2  Executar rotina de verificação periódica de vulnerabilidades 28
4.1.1.3  Rotina de verificação periódica realizada 28
4.1.1.4  DataStore 29
4.1.1.5  Coordenadoria de Seg. da Informação de TIC 29

5 MONITORAMENTO DE CORREÇÕES 30
5.1 MONITORAMENTO DE CORREÇÕES 31
5.1.1 Elementos do processo 31
5.1.1.1 Vulnerabilidades mapeadas relativas a pacotes 31
5.1.1.2 Gateway 31
5.1.1.3 Definir e executar as rotinas de atualização de pacotes 31
5.1.1.4 Gateway 32
5.1.1.5 Problema na atualização ou requer acompanhamento específico? 32
5.1.1.6 Gateway 32
5.1.1.7 Vulnerabilidades tratadas 32
5.1.1.8 Solicitação de análise e remediação 32
5.1.1.9 Acompanhar remediação de vulnerabilidades 33
5.1.1.10 Coordenadoria de Seg. da Informação de TIC 33
5.1.1.11 Unidade responsável por ativo de TIC 33
6 SOLICITAÇÃO DE ANÁLISE E REMEDIAÇÃO 34
6.1 SOLICITAÇÃO DE ANÁLISE E REMEDIAÇÃO 35
6.1.1 Elementos do processo 35
6.1.1.1 Necessidade de solicitação de análise 35
6.1.1.2 Registrar necessidade de tratamento 35
6.1.1.3 Documentar escopo 35
6.1.1.4 Analisar vulnerabilidades e identificar tratamentos 36
6.1.1.5 Tratamento de vulnerabilidades 36
6.1.1.6 Vulnerabilidades no escopo tratadas 36
6.1.1.7 Risco de vulnerabilidade não aceito (gestão contínua) 36
6.1.1.8 Problemas na implementação de remediações (gestão contínua) 36
6.1.1.9 Planilha de acompanhamento de vulnerabilidades 37

6.1.1.10 Coordenadoria de Seg. da Informação de TIC 37
6.1.1.11 Unidade responsável pela vulnerabilidade 37
7 TRATAMENTO DE VULNERABILIDADES 38
7.1 TRATAMENTO DAS VULNERABILIDADES 39
7.1.1 Elementos do processo 39
7.1.1.1 Propostas de tratamento definidas 39
7.1.1.2 Aceitação de riscos 39
7.1.1.3 Gateway 39
7.1.1.4 Implementar ações de remediação 39
7.1.1.5 Registrar remediação 40
7.1.1.6 Gateway 40
7.1.1.7 Gateway 40
7.1.1.8 Vulnerabilidades tratadas 40
7.1.1.9 Monitorar remediação 40
7.1.1.10 Aceitação de riscos de vulnerabilidades 41
7.1.1.11 Comunicar problema 41
7.1.1.12 É gestão contínua? 41
7.1.1.13 Problemas na implementação de remediações (gestão contínua) 42
7.1.1.14 Problemas na implementação de remediações (análise sob demanda) 42
7.1.1.15 Event 42
7.1.1.16 Planilha de acompanhamento de vulnerabilidades 42
7.1.1.17 Coordenadoria de Seg. da Informação de TIC 42
7.1.1.18 Unidade responsável pela vulnerabilidade 42
8 ACEITAÇÃO DE RISCOS DE VULNERABILIDADES 43
8.1 ACEITAÇÃO DE RISCOS DE VULNERABILIDADES 44
8.1.1 Elementos do processo 44

8.1.1.1 Vulnerabilidade definida para aceitação 44
8.1.1.2 Definir nível de risco residual 44
8.1.1.3 Enviar para deliberação do subcomitê 44
8.1.1.4 Deliberar sobre aceitação do risco 45
8.1.1.5 Necessita envio ao Comitê de Proteção de Dados e Segurança da Informação? 45
8.1.1.6 Deliberar sobre aceitação do risco 45
8.1.1.7 Gateway 45
8.1.1.8 Registrar tratamento 45
8.1.1.9 Risco aceito? 46
8.1.1.10 Vulnerabilidade aceita 46
8.1.1.11 É gestão contínua? 46
8.1.1.12 Risco de vulnerabilidade não aceito (gestão contínua) 46
8.1.1.13 Risco de vulnerabilidade não aceito (análise sob demanda) 46
8.1.1.14 Planilha de acompanhamento de vulnerabilidades 47
8.1.1.15 Comitê de Proteção de Dados e Segurança da Informação 47
8.1.1.16 Subcomitê de Tecnologia da Informação e Comunicações e Crises Cibernéticas 47
8.1.1.17 Coordenadoria de Seg. da Informação de TIC 47
9 REAVALIAÇÃO E MONITORAMENTO 48
9.1 REAVALIAÇÃO E MONITORAMENTO 49
9.1.1 Elementos do processo 49
9.1.1.1 Resultados de remediações 49
9.1.1.2 Avaliar resultados de remediações 49
9.1.1.3 Divulgar resultados 49
9.1.1.4 Avaliação e divulgação concluída 50
9.1.1.5 Coordenadoria de Seg. da Informação de TIC 50

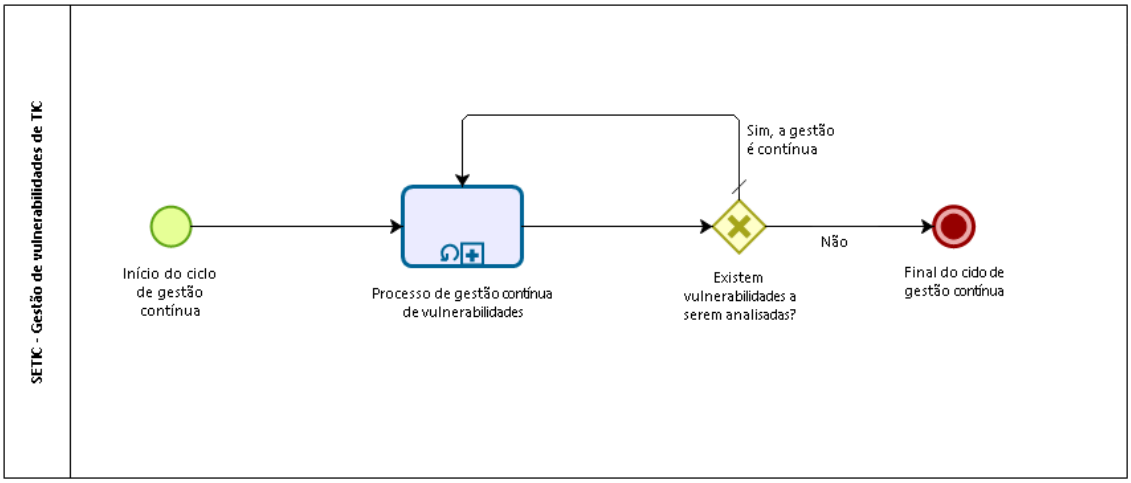
10 AJUSTE EM ROTINAS DE MONITORAMENTO 51
10.1 AJUSTE EM ROTINAS DE MONITORAMENTO 52
10.1.1 Elementos do processo 52
10.1.1.1 Necessidade de ajuste 52
10.1.1.2 Abrir solicitação de ajuste 52
10.1.1.3 Solitação priorizada 52
10.1.1.4 Analisar solicitação 52
10.1.1.5 Solicitação válida? 53
10.1.1.6 Solicitação completa? 53
10.1.1.7 Realizar alterações 53
10.1.1.8 Solicitação encerrada 53
10.1.1.9 Informar pendências 53
10.1.1.10 Registrar motivo 54
10.1.1.11 Unidade responsável por ativo de TIC 54
10.1.1.12 Coordenadoria de Seg. da Informação de TIC 54
11 PROCESSO DE ANÁLISE DE VULNERABILIDADES POR DEMANDA 55
11.1 PROCESSO DE ANÁLISE DE VULNERABILIDADES POR DEMANDA 56
11.1.1 Elementos do processo 56
11.1.1.1 Necessidade de análise por demanda 56
11.1.1.2 Solicitar análise de vulnerabilidades 56
11.1.1.3 Analisar solicitação 57
11.1.1.4 Solicitação OK? 57
11.1.1.5 Identificação de vulnerabilidades por demanda 57
11.1.1.6 Análise e definição de tratamentos 58
11.1.1.7 Tratamento das vulnerabilidades 58
11.1.1.8 Necessita reavaliação? 58
11.1.1.9 Vulnerabilidades tratadas 58

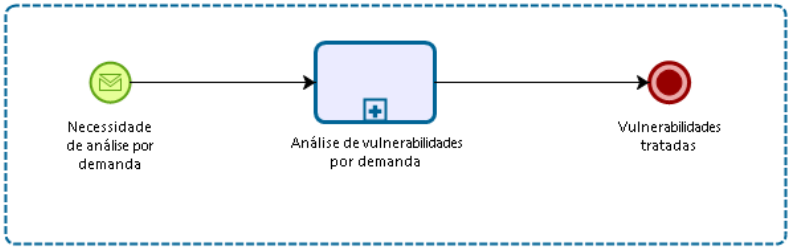
11.1.1.10 Reavaliação pontual 58
11.1.1.11 Informar pendências 59
11.1.1.12 Coordenadoria de Seg. da Informação de TIC 59
11.1.1.13 Unidade responsável por ativo de TIC 59
12 IDENTIFICAÇÃO DE VULNERABILIDADES POR DEMANDA 60
12.1 IDENTIFICAÇÃO DE VULNERABILIDADES POR DEMANDA 61
12.1.1 Elementos do processo 61
12.1.1.1 Escopo de análise definido 61
12.1.1.2 Criar scans pontuais 61
12.1.1.3 Janela de execução acordada 61
12.1.1.4 Informar início do scan 61
12.1.1.5 Gateway 62
12.1.1.6 Executar scan pontual 62
12.1.1.7 Informar término do scan 62
12.1.1.8 Gateway 62
12.1.1.9 Vulnerabilidades identificadas 62
12.1.1.10 Monitorar ambiente e serviço 63
12.1.1.11 Efetuar ajustes no scan 63
12.1.1.12 Informar problema 63
12.1.1.13 Necessita abortar scan? 63
12.1.1.14 Abortar scan 63
12.1.1.15 Event 64
12.1.1.16 Relatórios 64
12.1.1.17 DataStore 64
12.1.1.18 Coordenadoria de Seg. da Informação de TIC 64
12.1.1.19 Unidade responsável por ativo de TIC 64

13 ANÁLISE E DEFINIÇÃO DE TRATAMENTOS 65
13.1 ANÁLISE E DEFINIÇÃO DE TRATAMENTOS 66
13.1.1 Elementos do processo 66
13.1.1.1 Vulnerabilidades identificadas 66
13.1.1.2 Analisar vulnerabilidades 66
13.1.1.3 Definir recomendações 67
13.1.1.4 Propor tratamentos 67
13.1.1.5 Avaliar tratamentos propostos 67
13.1.1.6 Propostas de tratamentos OK? 67
13.1.1.7 Tratamentos definidos 68
13.1.1.8 Risco de vulnerabilidade não aceito (análise sob demanda) 68
13.1.1.9 Problemas na implementação de remediações (análise sob demanda) 68
13.1.1.10 Planilha de acompanhamento de vulnerabilidades 68
13.1.1.11 Relatórios 68
13.1.1.12 Coordenadoria de Seg. da Informação de TIC 68
13.1.1.13 Unidade responsável pela vuln. 69
14 REAVALIAÇÃO PONTUAL 70
14.1 REAVALIAÇÃO PONTUAL 71
14.1.1 Elementos do processo 71
14.1.1.1 Vulnerabilidades tratadas 71
14.1.1.2 Reexecutar scan pontual 71
14.1.1.3 Tratamentos validados? 71
14.1.1.4 Tratamentos validados 71
14.1.1.5 Problemas na implementação de remediações (análise sob demanda) 72
14.1.1.6 Coordenadoria de Seg. da Informação de TIC 72
15 RESOURCES 73
15.1 COORDENADORIA DE SEGURANÇA DA INFORMAÇÃO DE TIC (ENTIDADE) 73

15.2 Coordenadoria de Atendimento ao Usuário (Entidade) 73
15.3 Coordenadoria de Infraestrutura de TIC (Entidade) 73
15.4 Unidade responsável pela vulnerabilidade (Função) 73
15.5 Unidade responsável por ativo de TIC (Função) 73
15.6 Secretário de TIC (Função) 74
15.7 Comitê de Proteção de Dados e Segurança da Informação. (Entidade) 74

1 FLUXO PRINCIPAL





Versão: 1.0

1.1 SETIC - GESTÃO DE VULNERABILIDADES DE TIC

Descrição
Processo que estabelece as atividades relativas a identificação, análise, tratamento e monitoramento de vulnerabilidades dos ativos de TIC do Tribunal.

1.1.1 ELEMENTOS DO PROCESSO

1.1.1.1 Início do ciclo de gestão contínua

Descrição
O inicio de um ciclo recorrente de identificação, análise e tratamento de vulnerabilidades, monitorado pela Coordenadoria de Segurança da Informação de TIC; e

1.1.1.2 Processo de gestão contínua de vulnerabilidades

Descrição
O processo cíclico e recorrentemente para o monitoramento contínuo de vulnerabilidades através da ferramenta de gestão de vulnerabilidades.

Tipo de loop

Padrão

Máximo ciclo

0

Tempo de teste

Depois

Processo

Processo de gestão contínua de vulnerabilidades - Main Process

1.1.1.3 Existem vulnerabilidades a serem analisadas?

Portões

Não

Sim, a gestão é contínua

Tipo de Condição

Padrão

1.1.1.4 Final do ciclo de gestão contínua

Descrição

O processo termina com as vulnerabilidades identificadas remediadas e/ou com os riscos aceitos ou mitigados.

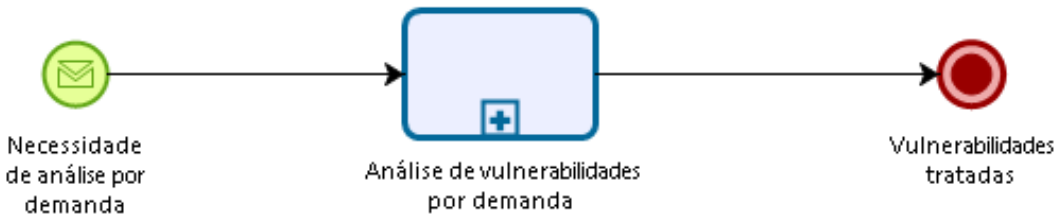
1.2 MAIN PROCESS

1.2.1 ELEMENTOS DO PROCESSO

1.2.1.1 Activity

Ver detalhes

1.3 SUBPROCESSO



Powered by bizagi Modeler

1.3.1 ELEMENTOS DO PROCESSO

1.3.1.1 Necessidade de análise por demanda

Descrição

O processo se inicia quando alguma unidade responsável por ativo de TIC detecta a necessidade de realizar análise específica de vulnerabilidades, de alguma aplicação e/ou serviço.

1.3.1.2 Análise de vulnerabilidades por demanda

Descrição

Instância do processo se inicia quando alguma unidade responsável necessita uma análise de vulnerabilidades para um ou mais ativos de TIC (aplicações, servidores, estações, equipamentos etc.).

Processo

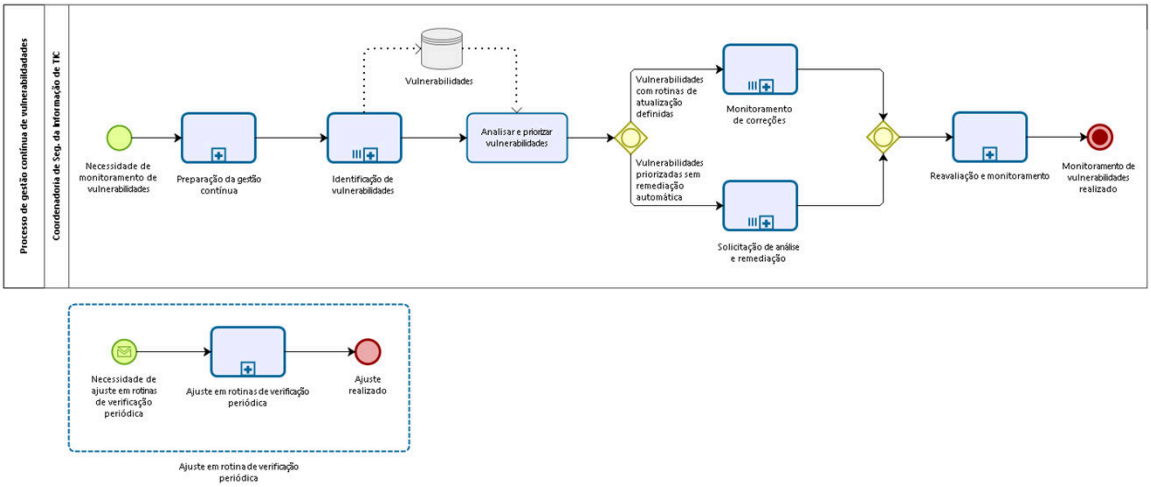
Processo de análise de vulnerabilidades por demanda - Processo de análise de vulnerabilidades por demanda

1.3.1.3  Vulnerabilidades tratadas

Descrição

As vulnerabilidades identificadas foram analisadas e tratadas conforme definido.

2 PROCESSO DE GESTÃO CONTÍNUA DE VULNERABILIDADES



Versão: 1.0

2.1 PROCESSO DE GESTÃO CONTÍNUA DE VULNERABILDADADES

Descrição
O processo de gestão contínua de vulnerabilidades visa definir o acompanhamento e ações decorrentes das rotinas períodicas de identificação de vulnerabilidades nos ativos de TIC do TRT15, estabelecidas por meio de ferramenta de gestão de vulnerabilidades.

2.1.1 ELEMENTOS DO PROCESSO

2.1.1.1 Necessidade de monitoramento de vulnerabilidades

Descrição
O processo se inicia com a necessidade de monitoramento contínuo das vulnerabilidades, como, por exemplo, quando há a inclusão de ativos no ambiente.

2.1.1.2 Preparação da gestão contínua

Descrição
Etapa de configuração dos ativos de TIC e das rotinas para o monitoramento na ferramenta de gestão de vulnerabilidades.

Processo

Preparação da gestão contínua - Preparação da gestão contínua

2.1.1.3 Identificação de vulnerabilidades

Descrição
Etapa de execução das rotinas de verificação, visando detectar a presença de possíveis vulnerabilidades.
São executadas múltiplas instâncias desse subprocesso, uma para cada rotina de verificação periódica definida.

Tipo de loop

Múltiplas instâncias

Pedido MI

Paralelo

Condição de fluxo

Todos

Processo

Identificação de vulnerabilidades - Identificação de vulnerabilidades

2.1.1.4 Analisar e priorizar vulnerabilidades

Descrição

Categorizar, classificar as vulnerabilidades encontradas, com o auxílio da ferramenta de gestão de vulnerabilidades, e priorizar conjuntos de vulnerabilidades para tratamento.
Vulnerabilidades que sejam relativas a aplicações com alguma rotina de atualização periódica já definida (como, por exemplo, navegadores e sistema operacional Windows) seguem para um fluxo de remediação automática monitorada.
Vulnerabilidades priorizadas para tratamento seguem para um fluxo de solicitação de análise e remediação por parte dos responsáveis.
Vulnerabilidades não priorizadas integram a base de dados da ferramenta e serão divulgadas aos responsáveis, que poderão tratá-las, ainda que não se formalize uma solicitação de tratamento.
Detalhes sobre os critérios podem ser consultados no documento de orientações auxiliares
.

Executantes

Coordenadoria de Segurança da Informação de TIC

2.1.1.5 Gateway

Portões

Vulnerabilidades com rotinas de atualização definidas

Vulnerabilidades priorizadas sem remediação automática

2.1.1.6 Solicitação de análise e remediação

Descrição

Etapa de análise e possível tratamento de conjunto de vulnerabilidades priorizado na etapa anterior.

Essa etapa pode possuir múltiplas instâncias, mapeadas em diversas iniciativas de remediação de vulnerabilidades envolvendo diferentes grupos de ativos e/ou responsáveis por ativos.

Tipo de loop

Múltiplas instâncias

Pedido MI

Paralelo

Condição de fluxo

Todos

Processo

Solicitação de análise e remediação - Solicitação de análise e remediação

2.1.1.7  Gateway

Portões

Reavaliação e monitoramento

2.1.1.8  Reavaliação e monitoramento

Descrição

Etapa de reavaliação sobre os tratamentos realizados, apuração de indicadores e identificação de melhorias no processo e seus componentes.

Processo

Reavaliação e monitoramento - Reavaliação e monitoramento

2.1.1.9  Monitoramento de vulnerabilidades realizado

Descrição

O processo termina com o monitoramento periódico de vulnerabilidades realizado.

2.1.1.10  Monitoramento de correções

Descrição

Etapa de acompanhamento das atualizações de sistemas e aplicações que ocorrem de forma autônoma, seja por configuração empregada (sistema operacional, navegadores), seja por rotina preexistente de atualização já definida.
Esta etapa possui múltiplas instâncias, mapeadas para as múltiplas situações de atualização autônoma que existem na infraestrutura.

Tipo de loop

Múltiplas instâncias

Pedido MI

Paralelo

Condição de fluxo

Todos

Processo

Monitoramento de correções - Monitoramento de correções

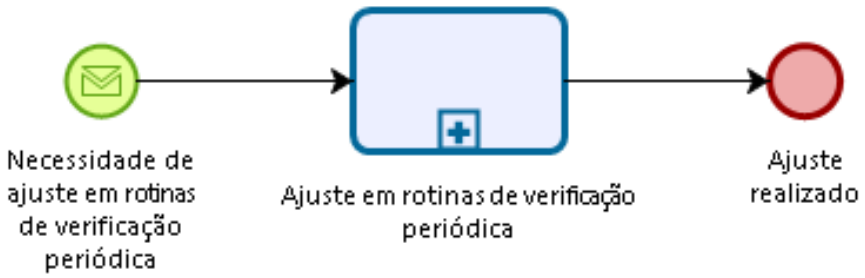
2.1.1.11  DataStore

Descrição
Vulnerabilidades registradas na ferramenta de gestão de vulnerabilidades.

2.1.1.12  Coordenadoria de Seg. da Informação de TIC

2.2 MAIN PROCESS

2.3 AJUSTE EM ROTINA DE VERIFICAÇÃO PERIÓDICA



Powered by bizagi Modeler

2.3.1 ELEMENTOS DO PROCESSO

2.3.1.1 Necessidade de ajuste em rotinas de verificação periódica

Descrição

É identificada uma necessidade de ajuste em rotinas de verificação periódica, visando incluir algum novo recurso ou ajustar periodicidade.

2.3.1.2 Ajuste em rotinas de verificação periódica

Descrição

Processamento de solicitações de ajuste em rotinas de verificação periódicas.

Processo

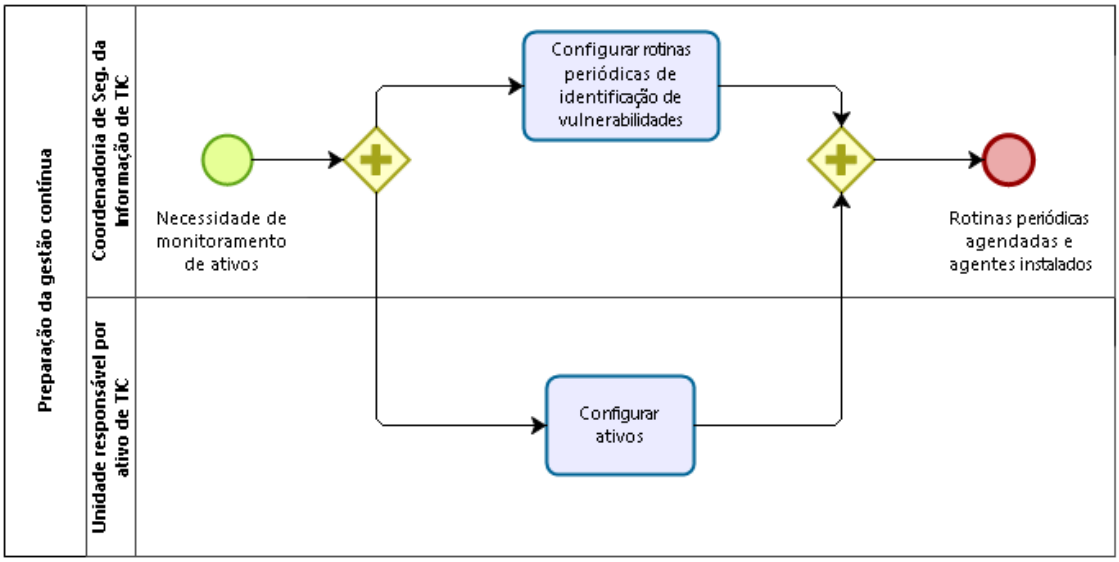
Ajuste em rotinas de monitoramento - Ajuste em rotinas de monitoramento

2.3.1.3 Ajuste realizado

Descrição

As rotinas de verificação periódicas estão ajustadas.

3 PREPARAÇÃO DA GESTÃO CONTÍNUA



Versão: 1.0

3.1 PREPARAÇÃO DA GESTÃO CONTÍNUA

Descrição
Etapa de configuração dos ativos de TIC e das rotinas para o monitoramento.
Entradas: ranges de IPs que definem ativos, periodicidade, agentes, credenciais de acesso
Saídas: rotinas de monitoramento definidas, ativos com agentes instalados

3.1.1 ELEMENTOS DO PROCESSO

3.1.1.1  Necessidade de monitoramento de ativos

Descrição
O processo se inicia a partir da necessidade de se configurar as configurações das rotinas periódicas de identificação de vulnerabilidades.

3.1.1.2  Gateway

3.1.1.3  Configurar rotinas periódicas de identificação de vulnerabilidades

Descrição
Configurar a ferramenta de gestão de vulnerabilidades para conter rotinas periódicas de descoberta e varredura de ativos.
Os detalhes sobre os procedimentos para configuração das rotinas periódicas, bem como as rotinas atualmente empregadas podem ser consultadas no documento auxiliar.

Executantes

Coordenadoria de Segurança da Informação de TIC

3.1.1.4  Gateway

3.1.1.5 Rotinas periódicas agendadas e agentes instalados

Descrição

O processo termina com as rotinas periódicas de identificação de vulnerabilidades agendadas, com os agentes instalados em estações de trabalho e servidores aplicáveis.

3.1.1.6 Configurar ativos

Descrição

Definir e executar procedimentos internos para garantir a correta identificação e análise dos ativos de TIC pela ferramenta de gestão de vulnerabilidades.
O documento de orientações auxiliares possui maiores detalhes sobre esta tarefa.

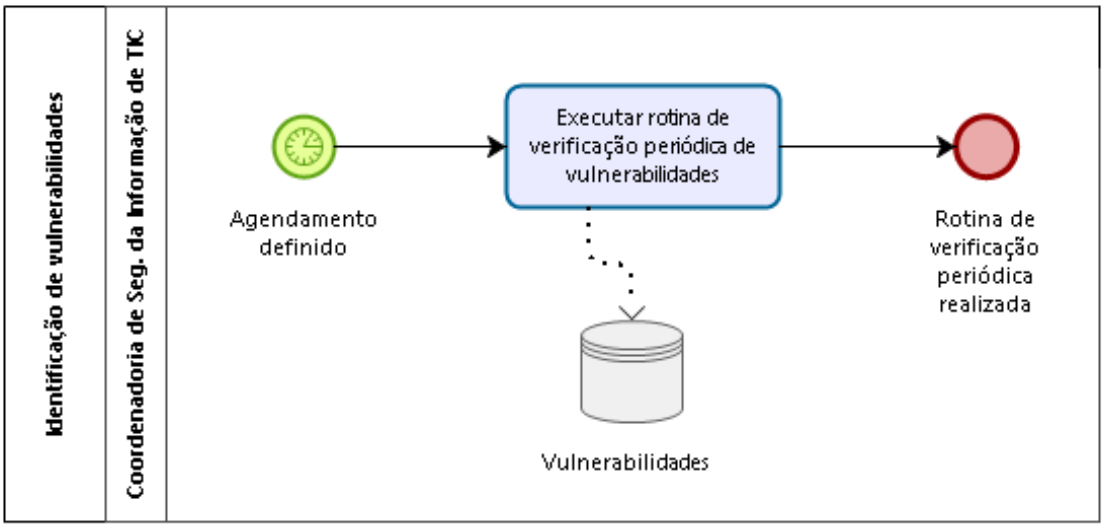
Executantes

Coordenadoria de Atendimento ao Usuário

3.1.1.7 Coordenadoria de Seg. da Informação de TIC

3.1.1.8 Unidade responsável por ativo de TIC

4 IDENTIFICAÇÃO DE VULNERABILIDADES



Versão: 1.0

4.1 IDENTIFICAÇÃO DE VULNERABILIDADES

Descrição
Etapa de execução das rotinas de verificação, visando detectar a presença de possíveis vulnerabilidades.
São executadas múltiplas instâncias desse subprocesso, uma para cada rotina de verificação periódica definida.
Entradas: rotinas periódicas de verificação.
Saídas: vulnerabilidades registradas na ferramenta de gestão de vulnerabilidades.

4.1.1 ELEMENTOS DO PROCESSO

4.1.1.1 Agendamento definido

Descrição
O processo inicia quando a data e horário determinado pelo agendamento de rotina periódica de identificação de vulnerabilidades ocorre.

Data do timer

2024-02-28T00:00:00

4.1.1.2 Executar rotina de verificação periódica de vulnerabilidades

Descrição
A ferramenta de gestão de vulnerabilidades executa a rotina de verificação periódica agendada, registrando as vulnerabilidades encontradas.

Executantes

Coordenadoria de Segurança da Informação de TIC

4.1.1.3 Rotina de verificação periódica realizada

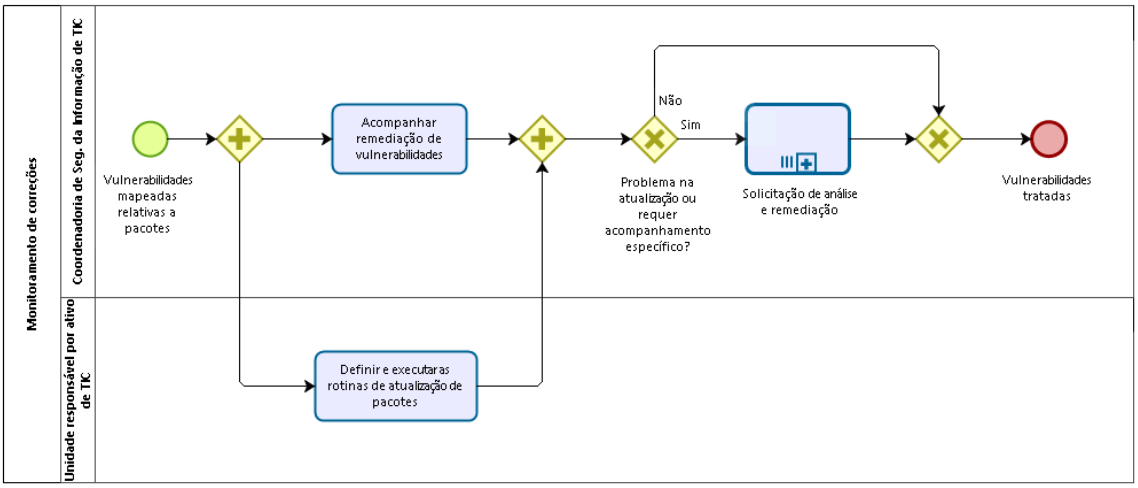
Descrição
A processo termina após a execução da rotina de verificação periódica.

4.1.1.4  DataStore

Descrição
Vulnerabilidades registradas na ferramenta de gestão de vulnerabilidades.

4.1.1.5  Coordenadoria de Seg. da Informação de TIC

5 MONITORAMENTO DE CORREÇÕES



Versão: 1.0

5.1 MONITORAMENTO DE CORREÇÕES

Descrição
Etapa de acompanhamento das atualizações de sistemas e aplicações que ocorrem de forma autônoma, seja por configuração empregada (sistema operacional, navegadores), seja por rotina preexistente de atualização já definida.
Esta etapa possui múltiplas instâncias, mapeadas para as múltiplas situações de atualização autônoma que existem na infraestrutura.
Entradas: conjunto de vulnerabilidades relativas a sistemas ou aplicações que possuem atualização autônoma.
Saídas: vulnerabilidades decorrentes de atualização autônoma tratadas.

5.1.1 ELEMENTOS DO PROCESSO

5.1.1.1 Vulnerabilidades mapeadas relativas a pacotes

Descrição
O processo se inicia com a priorização de vulnerabilidades associadas a sistemas ou aplicativos com rotina de atualização de pacotes definida.

5.1.1.2 Gateway

5.1.1.3 Definir e executar as rotinas de atualização de pacotes

Descrição
Definir, configurar e executar as políticas aplicáveis de atualização de sistemas e aplicações do parque computacional do Tribunal.
Maiores detalhes sobre sistemas e aplicativos com rotina automática de atualização de pacotes podem ser encontrados no documento de orientações auxiliares .

Executantes

Unidade responsável por ativo de TIC

5.1.1.4  Gateway

5.1.1.5  Problema na atualização ou requer acompanhamento específico?

Portões

Sim

Não

5.1.1.6  Gateway

Portões

Vulnerabilidades tratadas

5.1.1.7  Vulnerabilidades tratadas

Descrição

O processo termina com as vulnerabilidades relativas a sistemas e aplicativos com rotinas de atualização de pacotes tratadas.

5.1.1.8  Solicitação de análise e remediação

Descrição

Etapa que consiste na solicitação de análise e remediação para um determinado conjunto de vulnerabilidades.

Tipo de loop

Múltiplas instâncias

Pedido MI

Paralelo

Condição de fluxo

Todos

Processo

Solicitação de análise e remediação - Solicitação de análise e remediação

5.1.1.9  Acompanhar remediação de vulnerabilidades

Descrição

Com a ferramenta de gestão de vulnerabilidades, acompanhar a resolução das vulnerabilidades relativas a serviços ou aplicativos que possuem rotinas de atualização de pacotes definidas.
Caso seja identificado algum problema no número de remediações decorrentes das atualizações, ou seja alguma atualização importante para o ambiente (por exemplo, vulnerabilidades zero-day), pode-se optar por abrir uma solicitação formal ao responsável.

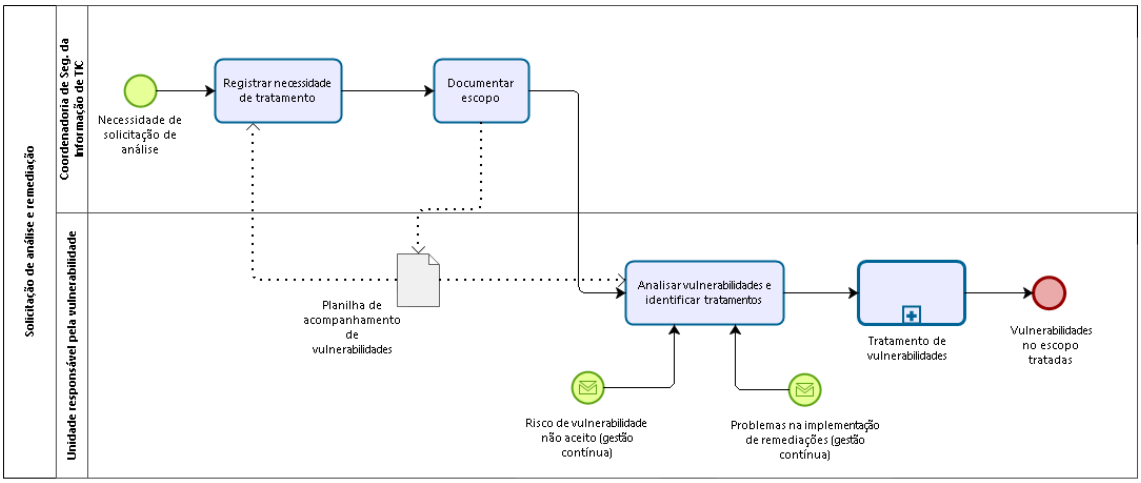
Executantes

Coordenadoria de Segurança da Informação de TIC

5.1.1.10  Coordenadoria de Seg. da Informação de TIC

5.1.1.11  Unidade responsável por ativo de TIC

6 SOLICITAÇÃO DE ANÁLISE E REMEDIAÇÃO



Versão: 1.0

6.1 SOLICITAÇÃO DE ANÁLISE E REMEDIAÇÃO

Descrição
Etapa que consiste na solicitação de análise e remediação para um determinado conjunto de vulnerabilidades.

6.1.1 ELEMENTOS DO PROCESSO

6.1.1.1 Necessidade de solicitação de análise

Descrição
O processo se inicia quando há necessidade de se estabelecer um esforço pontual de tratamento de vulnerabilidades com alguma unidade responsável por ativos de TIC.

6.1.1.2 Registrar necessidade de tratamento

Descrição
A necessidade de análise e mitigação deve ser formalizada por meio de uma requisição na central de serviços.
As orientações para a abertura da requisição estão em documentação auxiliar .

Executantes

Coordenadoria de Segurança da Informação de TIC

6.1.1.3 Documentar escopo

Descrição
Com o auxílio da ferramenta de gestão de vulnerabilidades, determinar os critérios que definem o conjunto de vulnerabilidades necessitando de tratamento.
A planilha de acompanhamento de vulnerabilidades é preenchida com as informações iniciais sobre o escopo e vulnerabilidades, conforme instruções.

Executantes

Coordenadoria de Segurança da Informação de TIC

6.1.1.4  Analisar vulnerabilidades e identificar tratamentos

Descrição

As vulnerabilidades apontadas são analisadas e os tratamentos possíveis são registrados. As orientações aplicáveis a esta etapa estão registradas em documentação auxiliar .
Esta tarefa pode ser acionada também por evento de risco de vulnerabilidade não aceito pelos responsáveis, ou por problemas durante a implementação das remediações. Nestes casos, deve-se buscar uma remediação alternativa, ou um tratamento alternativo (como por exemplo, a eliminação do risco, com a exclusão do ativo do ambiente).

Executantes

Unidade responsável pela vulnerabilidade

6.1.1.5  Tratamento de vulnerabilidades

Descrição

Etapa de tratamento das vulnerabilidades, conforme definido após avaliação conduzida nas etapas anteriores.

Processo

Tratamento de vulnerabilidades - Tratamento das vulnerabilidades

6.1.1.6  Vulnerabilidades no escopo tratadas

Descrição

O processo termina com as vulnerabilidades definidas no escopo tratadas.

6.1.1.7  Risco de vulnerabilidade não aceito (gestão contínua)

6.1.1.8  Problemas na implementação de remediações (gestão contínua)

6.1.1.9 Planilha de acompanhamento de vulnerabilidades

Descrição

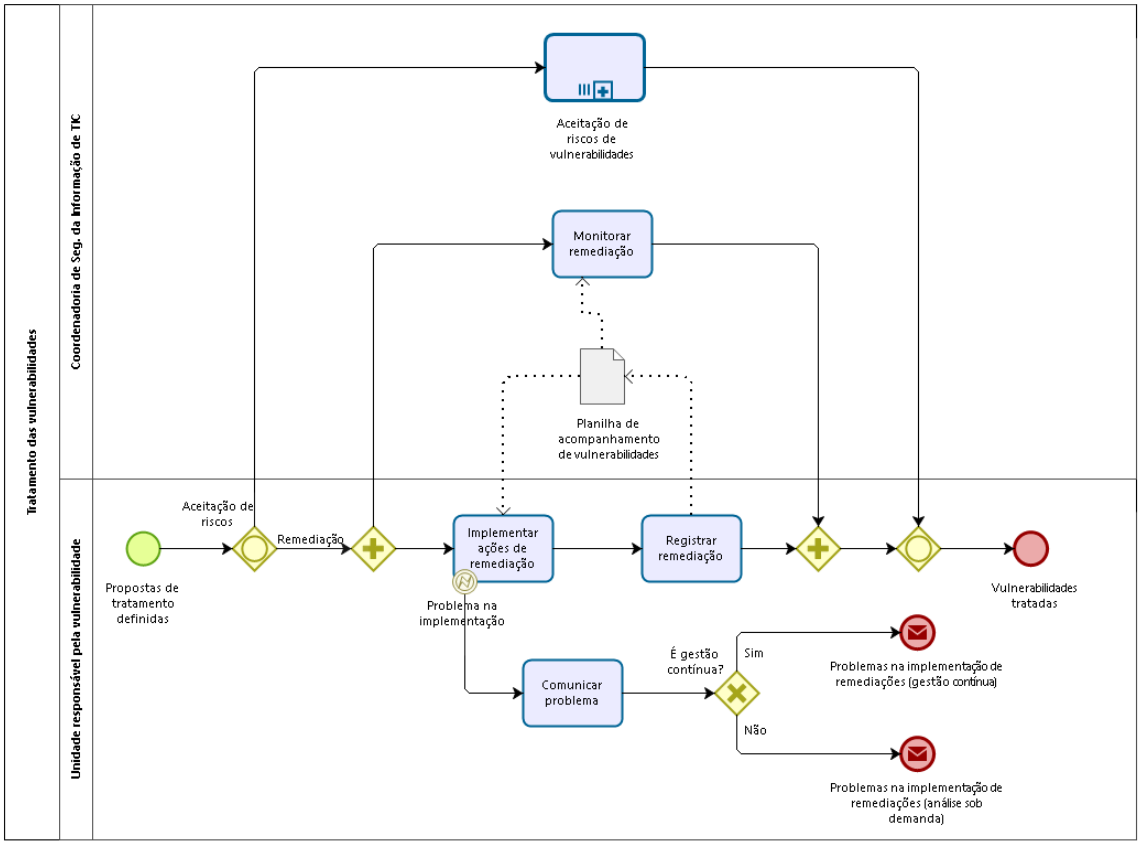
Documento que visa consolidar todas as informações referentes a identificação, análise e tratamento de vulnerabilidades de um escopo específico.

O template para a versão deste documento aplicável para os acionamentos de análise e remediação do processo de gestão contínua de vulnerabilidades encontra-se no Google Drive .

6.1.1.10 Coordenadoria de Seg. da Informação de TIC

6.1.1.11 Unidade responsável pela vulnerabilidade

7 TRATAMENTO DE VULNERABILIDADES



Versão: 1.0

7.1 TRATAMENTO DAS VULNERABILIDADES

Descrição
Etapa de tratamento das vulnerabilidades, conforme definido após avaliação conduzida nas etapas anteriores.

7.1.1 ELEMENTOS DO PROCESSO

7.1.1.1  Propostas de tratamento definidas

Descrição
O processo se inicia quando todas as vulnerabilidades identificadas são analisadas e registradas na planilha de acompanhamento de vulnerabilidades.

7.1.1.2  Aceitação de riscos

Portões

Remediação

Aceitação de riscos de vulnerabilidades

7.1.1.3  Gateway

7.1.1.4  Implementar ações de remediação

Descrição
Utilizando a planilha de acompanhamento de vulnerabilidades e o relatório gerado pela ferramenta de gestão de vulnerabilidades, a unidade responsável pela vulnerabilidade executa a remediação das vulnerabilidades identificadas.

Executantes

Unidade responsável pela vulnerabilidade

7.1.1.5  Registrar remediação

Descrição

Após a implementação das remediações de vulnerabilidades identificadas, a unidade responsável pela vulnerabilidade registra as informações sobre as remediações executadas na Planilha de acompanhamento de vulnerabilidades e encaminha o chamado para a Coordenadoria de Segurança da Informação de TIC.

Executantes

Unidade responsável pela vulnerabilidade

7.1.1.6  Gateway

7.1.1.7  Gateway

Portões

Vulnerabilidades tratadas

7.1.1.8  Vulnerabilidades tratadas

Descrição

O processo finaliza quando todas as vulnerabilidades identificadas e registradas na planilha de acompanhamento de vulnerabilidades são remediadas de acordo com as ações propostas e/ou os riscos associados são analisados e aceitos pelos devidos responsáveis.

7.1.1.9  Monitorar remediação

Descrição

Enquanto a unidade responsável realiza as remediações previstas, realizar o monitoramento por meio da ferramenta de gestão de vulnerabilidades e/ou planilha de acompanhamento de vulnerabilidades. Essa atividade tem o objetivo de verificar se as remediações:

- estão causando efeitos colaterais,
- estão sendo devidamente registradas, e
- estão sendo efetivas.

O documento de orientações auxiliares possui detalhes sobre a execução desta tarefa.

Executantes

Coordenadoria de Segurança da Informação de TIC

7.1.1.10  Aceitação de riscos de vulnerabilidades

Descrição

Processo que define os passos para as vulnerabilidades cujo tratamento proposto é o de aceitação de riscos, conforme identificado na Planilha de acompanhamento de vulnerabilidades.

Tipo de loop

Múltiplas instâncias

Pedido MI

Paralelo

Condição de fluxo

Todos

Processo

Aceitação de riscos de vulnerabilidades - Aceitação de riscos de vulnerabilidades

7.1.1.11  Comunicar problema

Descrição

Em caso de problema(s) na implementação das ações de remediação, a unidade responsável comunica a situação à Coordenadoria de Segurança da Informação de TIC e registra o fato na planilha de acompanhamento de vulnerabilidades.
Caso o tratamento seja decorrente de uma solicitação de análise e remediação da gestão contínua de vulnerabilidades, o processo retorna à esta etapa.
Caso o tratamento seja decorrente de vulnerabilidades identificadas em uma análise sob demanda, o processo retorna para a análise e definição de tratamentos.

7.1.1.12  É gestão contínua?

Portões

Sim

Não

7.1.1.13  Problemas na implementação de remediações (gestão contínua)

7.1.1.14  Problemas na implementação de remediações (análise sob demanda)

7.1.1.15  Event

7.1.1.16  Planilha de acompanhamento de vulnerabilidades

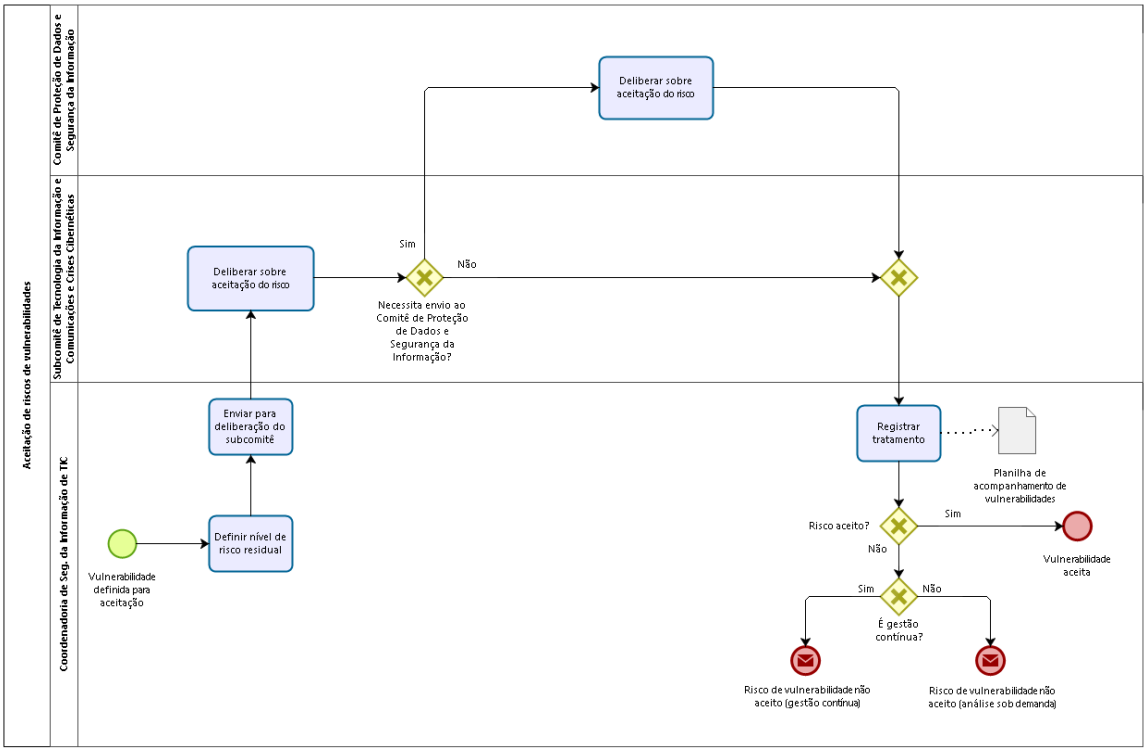
Descrição
Documento que visa consolidar todas as informações referentes a identificação, análise e tratamento de vulnerabilidades de um escopo específico.
O template para este documento possui duas versões:

- Versão aplicável para os acionamentos de análise e remediação na gestão contínua de vulnerabilidades: Google Drive .
- Versão aplicável para as análise de vulnerabilidades sob demanda: Google Drive .

7.1.1.17  Coordenadoria de Seg. da Informação de TIC

7.1.1.18  Unidade responsável pela vulnerabilidade

8 ACEITAÇÃO DE RISCOS DE VULNERABILIDADES



Versão: 1.0

8.1 ACEITAÇÃO DE RISCOS DE VULNERABILIDADES

Descrição
Processo que define os passos para as vulnerabilidades cujo tratamento proposto é o de aceitação de riscos, conforme identificado na Planilha de acompanhamento de vulnerabilidades.

8.1.1 ELEMENTOS DO PROCESSO

8.1.1.1 Vulnerabilidade definida para aceitação

Descrição
O processo se inicia quando a proposta de tratamento para uma vulnerabilidade do escopo é a de aceitação dos riscos associados.

8.1.1.2 Definir nível de risco residual

Descrição
Calcular o nível de risco com base em eventuais fatores atenuantes/agravantes e medidas de mitigação listadas pelas unidades técnicas.
O documento de orientações auxiliares possui detalhes sobre a execução desta tarefa.

8.1.1.3 Enviar para deliberação do subcomitê

Descrição
Encaminhar a análise do risco ao Subcomitê de Tecnologia da Informação e Comunicações e Crises Cibernéticas para deliberação através de comunicado formal.
O documento de orientações auxiliares possui detalhes sobre a execução desta tarefa.

Executantes

Coordenadoria de Segurança da Informação de TIC

8.1.1.4  Deliberar sobre aceitação do risco

Descrição
O Subcomitê de Tecnologia da Informação e Comunicações e Crises Cibernéticas delibera sobre os riscos associados à vulnerabilidade e decide sobre a aceitação.

Executantes

Secretário de TIC

8.1.1.5  Necessita envio ao Comitê de Proteção de Dados e Segurança da Informação?

Portões

Não

Sim

8.1.1.6  Deliberar sobre aceitação do risco

Descrição
O Comitê de Proteção de Dados e Segurança da Informação formaliza o recebimento, dá ciência sobre a análise realizada pelo Subcomitê de Tecnologia da Informação e Comunicações e Crises Cibernéticas e, se for o caso, delibera sobre a análise.

Executantes

Comitê de Proteção de Dados e Segurança da Informação.

8.1.1.7  Gateway

Portões

Registrar tratamento

8.1.1.8  Registrar tratamento

Descrição
Registrar a aceitação ou não na Planilha de acompanhamento de vulnerabilidades.

Executantes

Coordenadoria de Segurança da Informação de TIC

8.1.1.9  Risco aceito?

Portões

Sim

Não

8.1.1.10  Vulnerabilidade aceita

Descrição

O processo se encerra quando os riscos associados à vulnerabilidade identificada são formalmente aceitos pelo responsável

8.1.1.11  É gestão contínua?

Portões

Sim

Não

8.1.1.12  Risco de vulnerabilidade não aceito (gestão contínua)

Descrição

Quando os riscos associados à vulnerabilidade não são aceitos pelo responsável, é preciso avaliar se existem alternativas.
Caso a proposta de aceitação de riscos seja oriunda de um tratamento proposto no processo de gestão contínua de vulnerabilidades, volta-se a etapa de solicitação de análise e remediação.

8.1.1.13  Risco de vulnerabilidade não aceito (análise sob demanda)

Descrição

Quando os riscos associados à vulnerabilidade não são aceitos pelo responsável, é preciso avaliar se existem alternativas.
Caso a proposta de aceitação de riscos venha de uma análise de riscos sob demanda, volta-se à etapa de análise e definição de tratamentos.

8.1.1.14 Planilha de acompanhamento de vulnerabilidades

Descrição
Documento que visa consolidar todas as informações referentes a identificação, análise e tratamento de vulnerabilidades de um escopo específico.
O template para este documento possui duas versões:

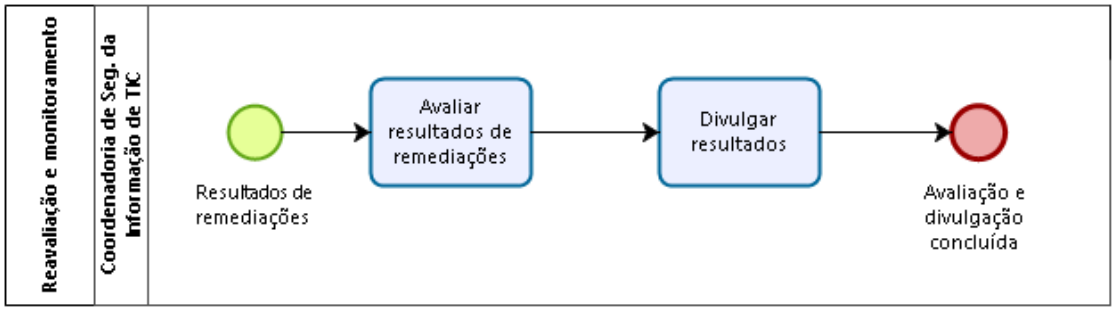
- Versão aplicável para os acionamentos de análise e remediação na gestão contínua de vulnerabilidades: Google Drive .
- Versão aplicável para as análise de vulnerabilidades sob demanda: Google Drive .

8.1.1.15 Comitê de Proteção de Dados e Segurança da Informação

8.1.1.16 Subcomitê de Tecnologia da Informação e Comunicações e Crises Cibernéticas

8.1.1.17 Coordenadoria de Seg. da Informação de TIC

9 REAVALIAÇÃO E MONITORAMENTO



Versão: 1.0

Autor: Gabriel TRT

9.1 REAVALIAÇÃO E MONITORAMENTO

Descrição
Etapa de reavaliação sobre os tratamentos realizados, apuração de indicadores e identificação de melhorias no processo e seus componentes.

9.1.1 ELEMENTOS DO PROCESSO

9.1.1.1  Resultados de remediações

Descrição
O processo se inicia com a obtenção dos resultados de solicitações de remediações e dos tratamentos realizados de forma autônoma.

9.1.1.2  Avaliar resultados de remediações

Descrição
Verificar o resultado das iniciativas de remediação, apurar indicadores definidos para acompanhamento do nível de risco do ambiente, identificar possibilidades de melhoria no monitoramento realizado.

Executantes

Coordenadoria de Segurança da Informação de TIC

9.1.1.3  Divulgar resultados

Descrição
Gerar, relatórios, gráficos de acompanhamento e atualizar painéis na ferramenta de gestão de vulnerabilidades para a divulgação dos resultados de tratamento de vulnerabilidades ao Secretário de TIC e demais unidades responsáveis. Por meio da ferramenta de gestão de vulnerabilidades, as unidades responsáveis também podem acessar o banco de dados completo de vulnerabilidades e seus históricos.

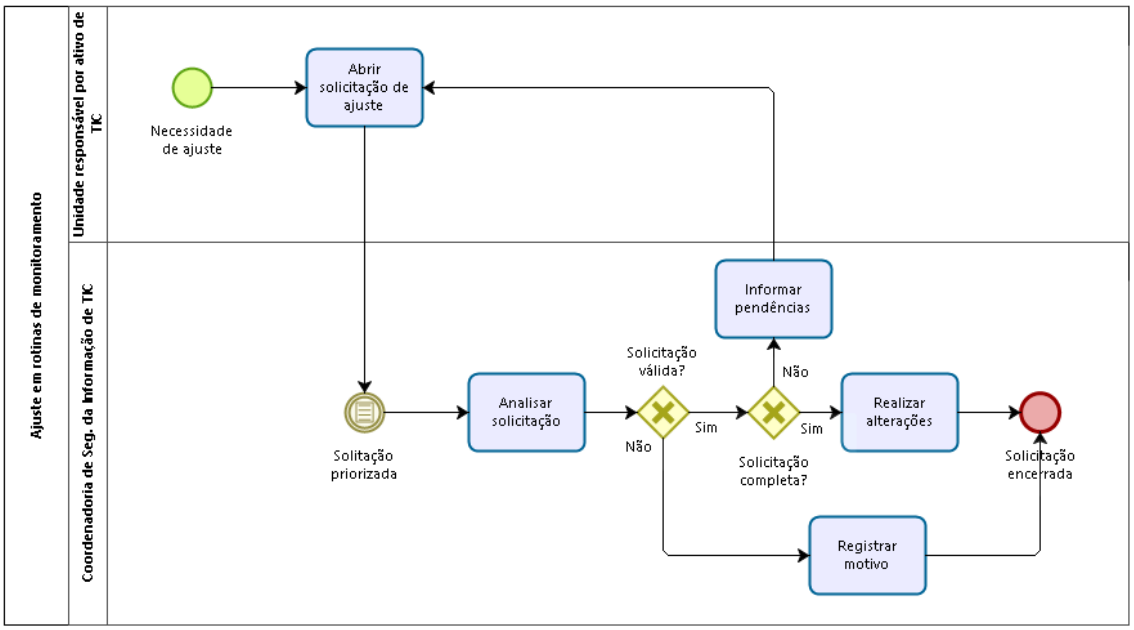
Executantes

9.1.1.4 Avaliação e divulgação concluída

Descrição
O processo termina com as remediações de vulnerabilidades analisadas e com os resultados do processo divulgados.

9.1.1.5 Coordenadoria de Seg. da Informação de TIC

10 AJUSTE EM ROTINAS DE MONITORAMENTO



Versão: 1.0

Autor: Gabriel TRT

10.1 AJUSTE EM ROTINAS DE MONITORAMENTO

10.1.1 ELEMENTOS DO PROCESSO

10.1.1.1 Necessidade de ajuste

Descrição
É identificada uma necessidade de ajuste em rotinas de monitoramento.

10.1.1.2 Abrir solicitação de ajuste

Descrição
Realizar uma solicitação de ajuste nas rotinas, seja para inclusão/exclusão de ativos, ajuste em periodicidade ou ajuste de classificação, por meio de uma solicitação na central de serviços.

Executantes

Unidade responsável pela vulnerabilidade

10.1.1.3 Solitação priorizada

Descrição
O chamado aberto foi priorizado para atendimento.

10.1.1.4 Analisar solicitação

Descrição
Verificar se a solicitação de ajuste é pertinente, factível e todas as informações necessárias foram lançadas.

Executantes

Coordenadoria de Segurança da Informação de TIC

10.1.1.5  Solicitação válida?

Portões

Sim

Não

10.1.1.6  Solicitação completa?

Portões

Sim

Não

10.1.1.7  Realizar alterações

Descrição

Efetivar as solicitações de alteração nas rotinas de monitoramento.
O documento de orientações auxiliares possui detalhes sobre a execução.

Executantes

Coordenadoria de Segurança da Informação de TIC

10.1.1.8  Solicitação encerrada

Descrição

A solicitação de ajuste é encerrada.

10.1.1.9  Informar pendências

Descrição

Indicar na solicitação quais as informações necessárias para que a solicitação seja executada.

Executantes

Coordenadoria de Segurança da Informação de TIC

10.1.1.10  Registrar motivo

Descrição
Encerrar a solicitação, indicando o motivo pelo qual sua execução não foi aceita.

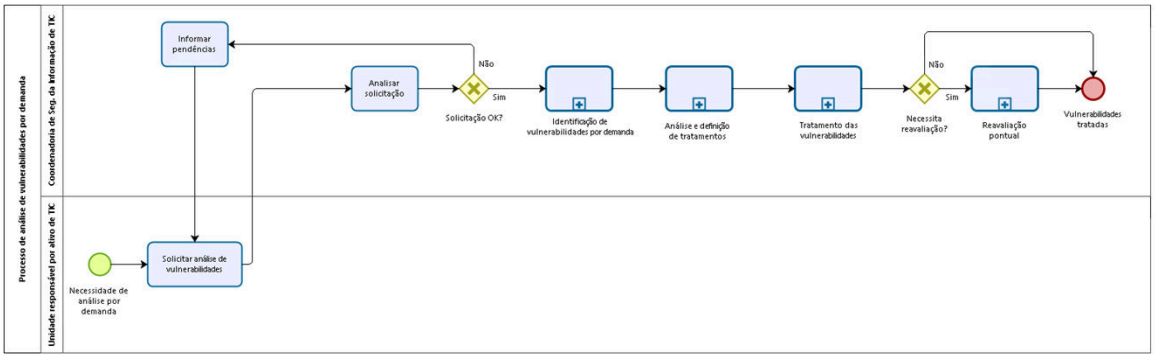
Executantes

Coordenadoria de Segurança da Informação de TIC

10.1.1.11  Unidade responsável por ativo de TIC

10.1.1.12  Coordenadoria de Seg. da Informação de TIC

11 PROCESSO DE ANÁLISE DE VULNERABILIDADES POR DEMANDA



Versão: 1.0

11.1 PROCESSO DE ANÁLISE DE VULNERABILIDADES POR DEMANDA

Descrição
Instância do processo se inicia quando alguma unidade responsável necessita uma análise de vulnerabilidades para um ou mais ativos de TIC (aplicações, servidores, estações, equipamentos etc.).

11.1.1 ELEMENTOS DO PROCESSO

11.1.1.1  Necessidade de análise por demanda

Descrição
O processo se inicia com o registro de chamado pelo usuário solicitante na central de serviço utilizando a oferta "Serviços > Serviços de Tecnologia da Informação e Comunicação > Segurança da Informação de TIC > Segurança Cibernética > Tenable One" descrevendo qual ou quais aplicações e/serviços serão analisados, além de informações adicionais necessárias como URLs, credencias, servidores, especificidades, e outras relevantes para que seja realizada a análise de vulnerabilidades na aplicação ou serviço solicitado.

11.1.1.2  Solicitar análise de vulnerabilidades

Descrição
Existem duas formas de solicitação:

- Abertura de chamado
Registrar o chamado no serviço relacionado através da Central de Serviços, contendo no mínimo as seguintes informações:

- Informações do ativo
  - hostname
  - IP
  - URL (se aplicação ou serviço)
  - descrição sucinta (se aplicação ou serviço)

- se possui funcionalidades autenticadas

- Esteira de desenvolvimento
Nesse caso, a solicitação poderá se dar com a inclusão da análise de vulnerabilidades no projeto/demanda de desenvolvimento. A Coordenadoria de Desenvolvimento de Sistemas deverá notificar a Coordenadoria de Segurança da Informação da necessidade, para planejamento e estruturação da análise no âmbito do projeto.

O documento de orientações auxiliares possui detalhes sobre a execução desta tarefa.

11.1.1.3  Analisar solicitação

Descrição
Analisar a solicitação de análise de vulnerabilidades verificando se todas as informações necessárias foram preenchidas na solicitação, se o serviço ou aplicação está acessível, se as credenciais eventualmente necessárias são válidas e quaisquer outras pendências para a execução da análise de vulnerabilidades solicitada.

Executantes

Coordenadoria de Segurança da Informação de TIC

11.1.1.4  Solicitação OK?

Portões

Sim

Não

11.1.1.5  Identificação de vulnerabilidades por demanda

Descrição
Execução da identificação de vulnerabilidades relacionadas aos ativos elencados na solicitação de análise.

Processo

Identificação de vulnerabilidades por demanda - Identificação de vulnerabilidades por demanda

11.1.1.6  Análise e definição de tratamentos

Descrição
Análise das vulnerabilidades encontradas e definição dos tratamentos a serem propostos.

Processo

Análise e definição de tratamentos - Análise e definição de tratamentos

11.1.1.7  Tratamento das vulnerabilidades

Descrição
Execução dos tratamentos definidos para as vulnerabilidades identificadas dentro do escopo delimitado pela análise e definição de tratamentos.

Processo

Tratamento de vulnerabilidades - Tratamento das vulnerabilidades

11.1.1.8  Necessita reavaliação?

Portões

Não

Sim

11.1.1.9  Vulnerabilidades tratadas

Descrição
O processo é encerrado quando as vulnerabilidades são remediadas e/ou os riscos são aceitos. Nessa etapa, o chamado relacionado à solicitação de análise de vulnerabilidades por demanda é encerrado.

11.1.1.10  Reavaliação pontual

Descrição

Reexecução da análise de vulnerabilidades para verificação de efetividade dos tratamentos realizados.

Processo

Reavaliação pontual - Reavaliação pontual

11.1.1.11 Informar pendências

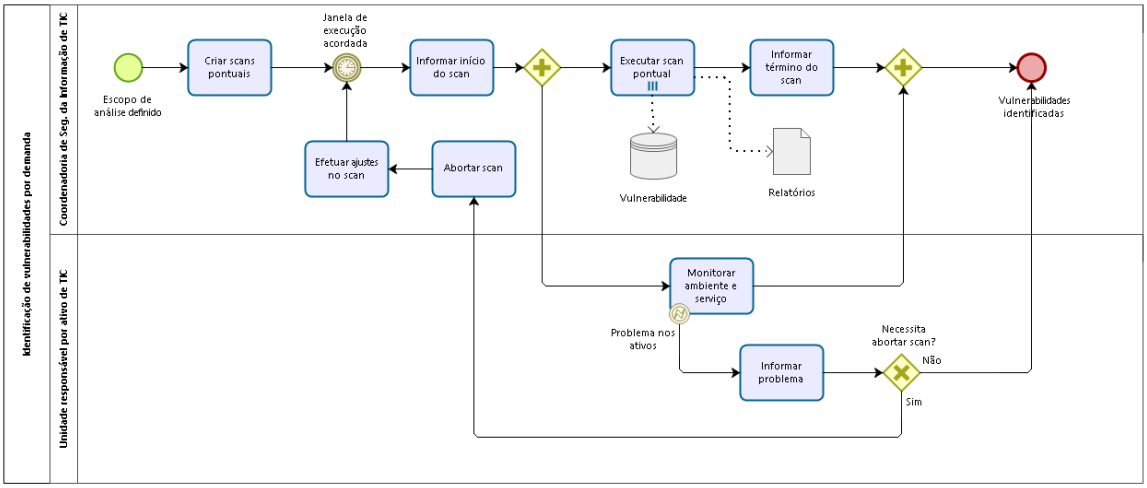
Descrição

Informar no chamado as pendências encontradas que inviabilizam a análise de vulnerabilidades solicitada e indicar a necessidade de saneamento. Assim que o solicitante conclui a resolução de todas as pendências, registra a informação no chamado, que retorna para nova análise. No caso de projetos de desenvolvimento da Coordenadoria de Desenvolvimento de Sistemas, as informações sobre as pendências são registradas nos meios utilizados para interação com a Coordenadoria de Segurança da Informação, bem como a informação de conclusão de resolução de todas as pendências, quando assim for.

11.1.1.12 Coordenadoria de Seg. da Informação de TIC

11.1.1.13 Unidade responsável por ativo de TIC

12 IDENTIFICAÇÃO DE VULNERABILIDADES POR DEMANDA



Versão: 1.0

12.1 IDENTIFICAÇÃO DE VULNERABILIDADES POR DEMANDA

Descrição
Execução da identificação de vulnerabilidades relacionadas aos ativos elencados na solicitação de análise.

12.1.1 ELEMENTOS DO PROCESSO

12.1.1.1 Escopo de análise definido

Descrição
O processo se inicia quando a solicitação de análise é validada e o escopo está definido.

12.1.1.2 Criar scans pontuais

Descrição
Registrar um ou mais scans na ferramenta de gestão de vulnerabilidades, de acordo com a demanda solicitada. O documento de orientações auxiliares possui detalhes sobre a criação de scans.

Executantes

Coordenadoria de Segurança da Informação de TIC

12.1.1.3 Janela de execução acordada

12.1.1.4 Informar início do scan

Descrição
Notificar o solicitante sobre o início do(s) scan(s), podendo acrescentar informações como estimativa de tempo.

Executantes

Coordenadoria de Segurança da Informação de TIC

12.1.1.5  Gateway

12.1.1.6  Executar scan pontual

Descrição
Executar os scans definidos na ferramenta de gestão de vulnerabilidades, a qual registrará as vulnerabilidades identificadas em sua base de dados.

Executantes

Coordenadoria de Segurança da Informação de TIC

Tipo de loop

Múltiplas instâncias

Pedido MI

Paralelo

Condição de fluxo

Todos

12.1.1.7  Informar término do scan

Descrição
Notificar o solicitante sobre o encerramento da execução dos scans adicionados à ferramenta de gestão de vulnerabilidades.

Executantes

Coordenadoria de Segurança da Informação de TIC

12.1.1.8  Gateway

12.1.1.9  Vulnerabilidades identificadas

Descrição
O processo é finalizado quando todos os scans necessários são concluídos e as vulnerabilidades identificadas.

12.1.1.10  Monitorar ambiente e serviço

Descrição

Realizar o monitoramento do ambiente sobre possíveis impactos que afetem a disponibilidade e utilização dos ativos de TIC envolvidos.

Executantes

Unidade responsável por ativo de TIC

12.1.1.11  Efetuar ajustes no scan

Descrição

Com base nas informações comunicadas no evento de problema pela unidade responsável pelo ativo de TIC, caso possível, realizar os ajustes necessários nas instâncias dos scans adicionados à ferramenta de gestão de vulnerabilidades. Caso não possível, registra-se a impossibilidade de scan na solicitação e encerra-se a solicitação.

Executantes

Coordenadoria de Segurança da Informação de TIC

12.1.1.12  Informar problema

Descrição

Ao encontrar um problema durante a execução do scan, comunicar o fato à Coordenadoria de Segurança da Informação de TIC, como o efeito negativo causado, aplicações e/ou serviços impactados, assets afetados e quaisquer outras informações relevantes.

Executantes

Unidade responsável por ativo de TIC

12.1.1.13  Necessita abortar scan?

Portões

Não

Sim

12.1.1.14  Abortar scan

Descrição

Com base na comunicação de evento de problema da unidade responsável pelo ativo de TIC, solicitar na ferramenta de gestão de vulnerabilidades a interrupção das instâncias de scans em andamento.

Executantes

Coordenadoria de Segurança da Informação de TIC

12.1.1.15 Event

12.1.1.16 Relatórios

Descrição

Relatórios gerados pela ferramenta de gestão de vulnerabilidades.

12.1.1.17 DataStore

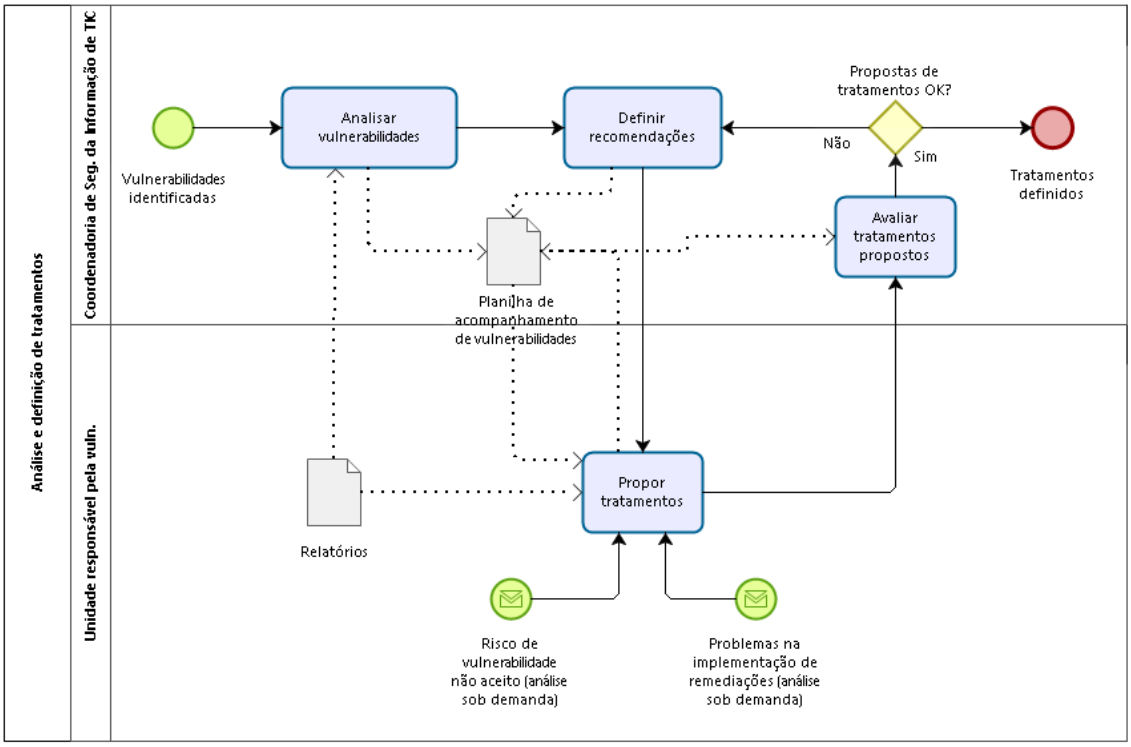
Descrição

Vulnerabilidades registradas na ferramenta de gestão de vulnerabilidades.

12.1.1.18 Coordenadoria de Seg. da Informação de TIC

12.1.1.19 Unidade responsável por ativo de TIC

13 ANÁLISE E DEFINIÇÃO DE TRATAMENTOS



Versão: 1.0

13.1 ANÁLISE E DEFINIÇÃO DE TRATAMENTOS

Descrição
Análise das vulnerabilidades encontradas e definição dos tratamentos a serem propostos.

Executantes

Coordenadoria de Segurança da Informação de TIC

13.1.1 ELEMENTOS DO PROCESSO

13.1.1.1 Vulnerabilidades identificadas

Descrição
O processo se inicia de três formas:

- No fluxo padrão, iniciando o procedimento de análise e priorização das vulnerabilidades identificadas e registradas na planilha de acompanhamento de vulnerabilidades
- No caso de riscos de vulnerabilidades não aceitos (evento)
- No caso de prolema na implementação de remediações de vulnerabilidades (evento)

13.1.1.2 Analisar vulnerabilidades

Descrição
Realizar a análise das vulnerabilidades identificadas, efetuar a priorização destas e registrar todos os dados na "Planilha de acompanhamento de vulnerabilidades".
Se o escopo de análise é pequeno e, em conjunto com a unidade responsável pelas vulnerabilidades identificadas, conclui-se que as vulnerabilidades são em sua maioria remediáveis e não restará vulnerabilidades com risco residual médio ou alto (não necessitará de aceitação de riscos por outras partes), a utilização da planilha é opcional. Caso a planilha não seja utilizada, as informações que estariam registradas nela devem ser sumarizadas no próprio chamado, onde aplicável.
O documento de orientações auxiliares possui detalhes sobre a avaliação e priorização de vulnerabilidades.

Executantes

Coordenadoria de Segurança da Informação de TIC

13.1.1.3 Definir recomendações

Descrição

Registrar as recomendações de tratamento das vulnerabilidades identificadas na Planilha de acompanhamento de vulnerabilidades.
O documento de orientações auxiliares possui detalhes sobre a execução desta tarefa.

Executantes

Coordenadoria de Segurança da Informação de TIC

13.1.1.4 Propor tratamentos

Descrição

Utilizando as recomendações registradas na planilha de acompanhamento de vulnerabilidades e o relatório de diagnóstico gerado pela ferramenta de gestão de vulnerabilidades, a unidade responsável pelas vulnerabilidades faz também a sua análise e propõe tratamentos e repriorizações, registrando informações na Planilha de acompanhamento de vulnerabilidades.
Ao ter uma proposta de aceitação de risco rejeitada, ou algum problema na implementação de remediação, esta tarefa é novamente acionada para estabelecer as alternativas.

Executantes

Unidade responsável pela vulnerabilidade

13.1.1.5 Avaliar tratamentos propostos

Descrição

Avaliar se todas as vulnerabilidades priorizadas foram consideradas nas propostas, e identificar qualquer necessidade de esclarecimento ou complementação pela unidade responsável pela vulnerabilidade.

13.1.1.6 Propostas de tratamentos OK?

Portões

Não

Sim

13.1.1.7  Tratamentos definidos

Descrição
O processo se encerra quando os tratamentos propostos estão definidos e registrados.

13.1.1.8  Risco de vulnerabilidade não aceito (análise sob demanda)

13.1.1.9  Problemas na implementação de remediações (análise sob demanda)

13.1.1.10  Planilha de acompanhamento de vulnerabilidades

Descrição
Planilha de gerenciamento do ciclo de vida da análise de vulnerabilidades por demanda, incluindo informações como (mas não limitados a):

- Escopo da análise
- Dados do ambiente
- Scans adicionados à ferramenta de gestão
- Vulnerabilidades identificadas
- Estatísticas gerais das instâncias dos scans
- Recomendações de remediações
- Propostas de tratamentos
- Resultados de reanálise

O template para a planilha se encontra no Google Drive .

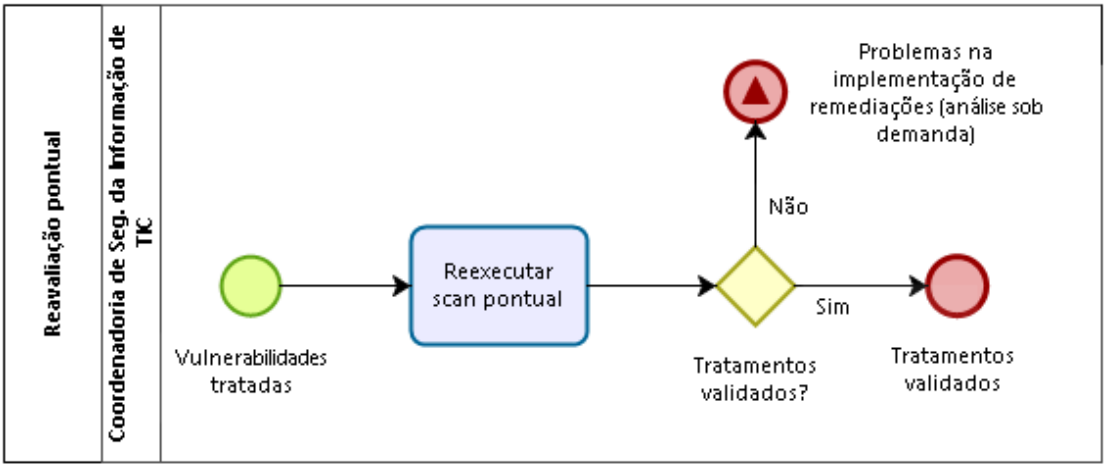
13.1.1.11  Relatórios

Descrição
Documento gerado pela ferramenta de gestão de vulnerabilidades detalhando os scans realizados, vulnerabilidades encontradas, entre outras informações.

13.1.1.12  Coordenadoria de Seg. da Informação de TIC

13.1.1.13  Unidade responsável pela vuln.

14 REAVALIAÇÃO PONTUAL



Versão: 1.0

14.1 REAVALIAÇÃO PONTUAL

14.1.1 ELEMENTOS DO PROCESSO

14.1.1.1  Vulnerabilidades tratadas

Descrição
O processo se inicia quando as vulnerabilidades identificadas foram remediadas de acordo com os tratamentos propostos

14.1.1.2  Reexecutar scan pontual

Descrição
Reexecutar as instâncias de scan criadas para a solicitação de análise por demanda, conforme a necessidade, objetivando conferir a efetividade das ações de remediação implementadas. Nos casos em que a planilha de acompanhamento de vulnerabilidades não é utilizada, a reexecução do scan é obrigatória para documentar a resolução das vulnerabilidades, e o novo relatório deve constar no chamado.

Executantes

Coordenadoria de Segurança da Informação de TIC

14.1.1.3  Tratamentos validados?

Portões

Sim

Não

14.1.1.4  Tratamentos validados

Descrição
O processo se encerra quando a reexecução dos scans relativos à vulnerabilidades remediadas foram finalizados e validados.

14.1.1.5  Problemas na implementação de remediações (análise sob demanda)

Descrição

Caso identificado que o tratamento não ocorreu conforme proposto, notificar a unidade responsável pela vuln. para análise e proposição de novos tratamentos, se for o caso.

14.1.1.6  Coordenadoria de Seg. da Informação de TIC

15 RESOURCES

15.1 COORDENADORIA DE SEGURANÇA DA INFORMAÇÃO DE TIC (ENTIDADE)

Descrição

Unidade responsável por estabelecer as rotinas de monitoramento de vulnerabilidades, operar a ferramenta de gestão de vulnerabilidades especializadas, e apoiar as demais unidades no tratamento das vulnerabilidades.

15.2 COORDENADORIA DE ATENDIMENTO AO USUÁRIO (ENTIDADE)

Descrição

Unidade responsável por configurar e manter estações de trabalhos do parque tecnológico do Tribunal.

15.3 COORDENADORIA DE INFRAESTRUTURA DE TIC (ENTIDADE)

Descrição

Unidade responsável por configurar e manter os ativos do tipo servidor do parque tecnológico do Tribunal.

15.4 UNIDADE RESPONSÁVEL PELA VULNERABILIDADE (FUNÇÃO)

Descrição

Unidade responsável pelo ativo em que a determinada vulnerabilidade ou conjunto de vulnerabilidades se encontra.

15.5 UNIDADE RESPONSÁVEL POR ATIVO DE TIC (FUNÇÃO)

Descrição

Unidade responsável por algum ativo de TIC.

15.6 SECRETÁRIO DE TIC (FUNÇÃO)

Descrição

Gestor da área de tecnologia da informação e comunicação.

15.7 COMITÊ DE PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO. (ENTIDADE)

Descrição

Órgão colegiado com atribuições relacionadas à gestão de segurança da informação do Tribunal.