Gestão de Vulnerabilidades Técnicas
Processos e Ferramentas

José Gildásio, Rogerio Bastos, Fábio Costa, Italo Valcy
Universidade Federal da Bahia
Ponto de Presença da RNP na Bahia

POP-BA

STI
Superintendência de
Tecnologia da Informação | UFBA

Quem somos

É responsável pela conexão das instituições baianas à Rede Acadêmica Brasileira (Rede Ipê) e operação da Rede Metropolitana de Salvador (Remessa).

Coordenação de Segurança da Informação e Comunicações da STI/UFBA, responsável pela ETIR da Universidade Federal da Bahia.

É um CSIRT de coordenação para as instituições clientes do PoP-BA/RNP e parceiras da Remessa.

Gestão de Vulnerabilidades

- **Gestão de Vulnerabilidades** é o processo de identificação, classificação e tratamento das vulnerabilidades;

- O tratamento consiste na correção da vulnerabilidade, aplicação de controles para minimizar a probabilidade de exploração ou o impacto, ou na aceitação do risco;

Gestão de Vulnerabilidades

- Não confundir com *Scanner* de Vulnerabilidades;
- *Scanner* de Vulnerabilidades consiste no uso de ferramentas para a identificação de vulnerabilidades;
- Faz parte do processo de Gestão de Vulnerabilidades;

Gestão de Vulnerabilidades

- Item 12.6 da ISO 27002;
- Tem como objetivo prevenir a exploração de vulnerabilidades técnicas.
- Controles:
  - Obter informações sobre as vulnerabilidades em tempo hábil;
  - Avaliar a exposição às vulnerabilidades;
  - Tomar as medidas apropriadas para lidar com os riscos;

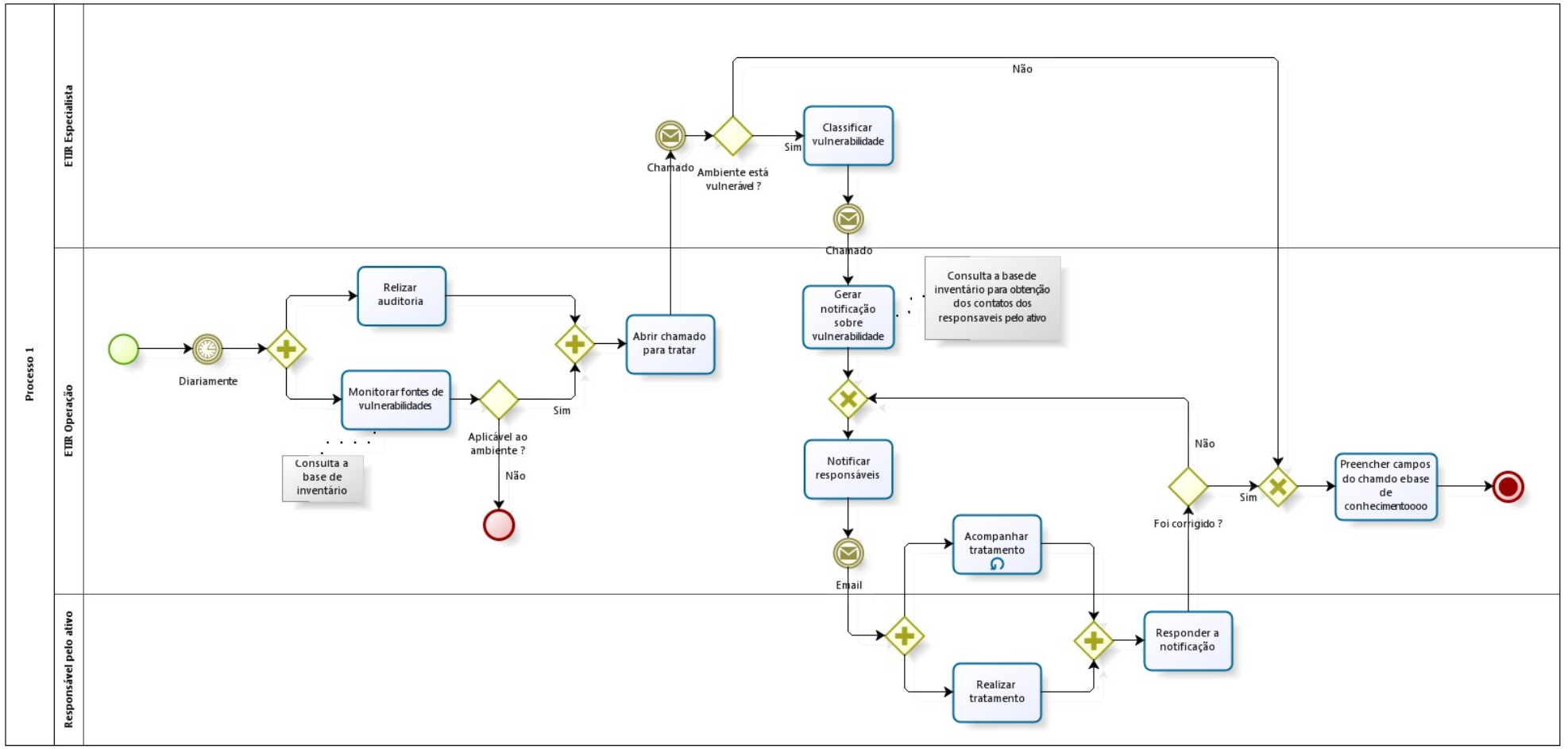
Gestão de Vulnerabilidades

- Diretrizes:
  - Inventário completo e atualizado é um pré-requisito;
  - Definir funções e responsabilidades;
  - Estabelecer prazo para reação;
  - Avaliar os riscos e ações a serem tomadas;
    - Aplicação de *patches*;
    - Desativação de serviço ou funcionalidade;
    - Adaptação ou agregação de controles (e.g. *virtual patching*);
    - Aumento do monitoramento;
    - Aumento da conscientização;
  - Alinhamento com o processo de Gestão de Incidentes;
  - Documentar e Monitorar.

Inventário

- Wiki (manual)
- Itop (manual)
- OCS Inventory (semi-automático)
  - Possui agente para registro automático de hosts e softwares;
  - Suporta diversos sistemas operacionais;
  - API para consultas;
  - Falta de padronização dos nomes;
  - Não detecta aplicações webs e *custom instalations*.

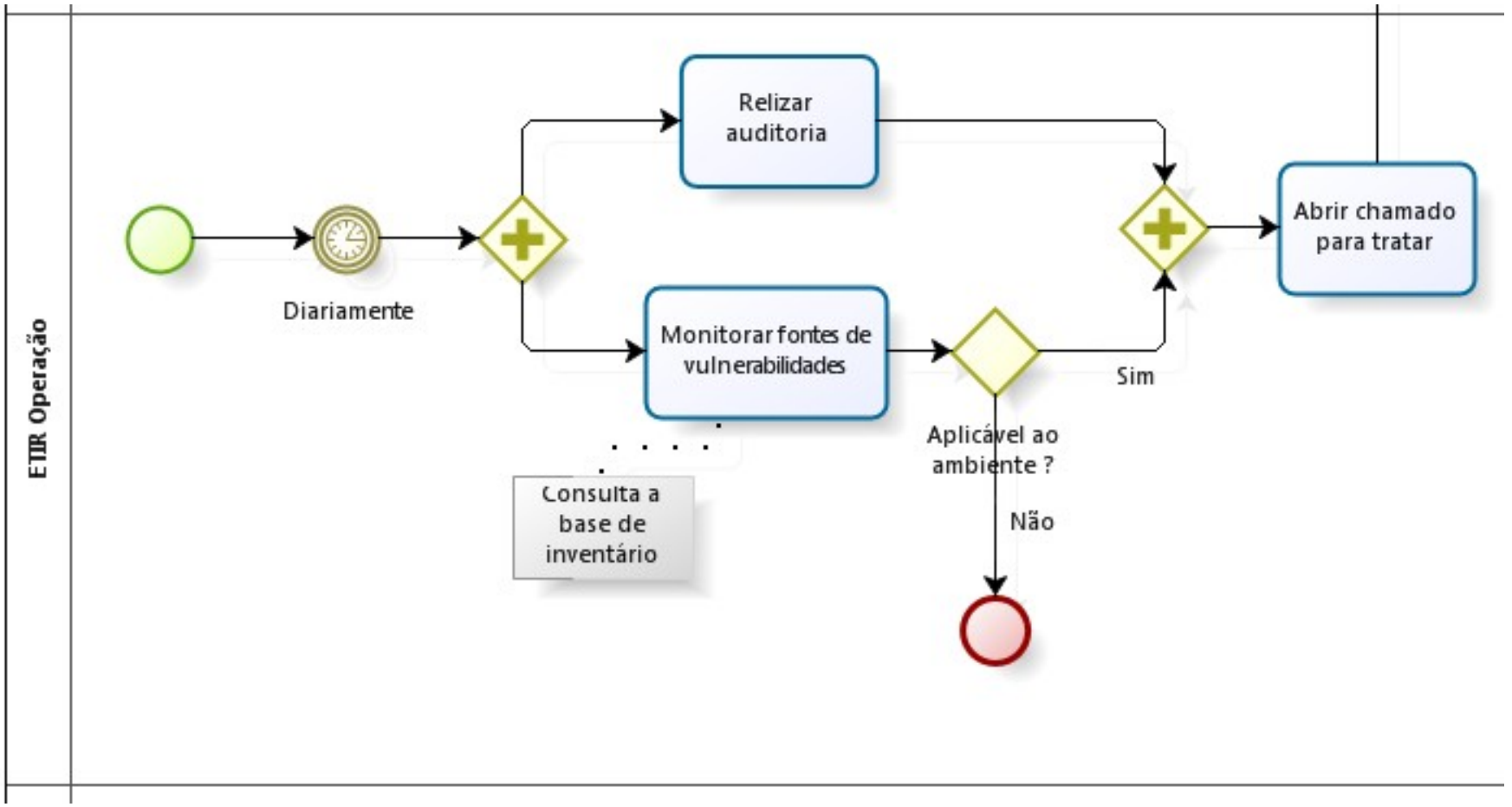
Fluxo do Processo da UFBA



Papéis

- ETIR Operação;
- ETIR Especialista;
- Responsável pelo Ativo;

Descoberta


ETIR Operação
Diariamente
Relizar auditoria
Monitorar fontes de vulnerabilidades
Consulta a base de inventário
Aplicável ao ambiente ?
Sim
Não
Abrir chamado para tratar

Fontes de Vulnerabilidades

- Mail Lists:
  - BugTraq - https://seclists.org/bugtraq/
  - FullDisclosure - https://seclists.org/fulldisclosure/
  - US-CERT - https://www.us-cert.gov/
  - CAIS - http://listas.rnp.br/mailman/listinfo/rnp-alerta
  - Fabricantes, comunidades e projetos;
  - Grande volume de mensagens.

Fontes de Vulnerabilidades

- CVE-Search
  - Importa CVE e CPE no MongoDB para fazer busca e processamento;
  - Armazena vulnerabilidades e informações relacionadas;
  - Interface e API web;
  - *Resource Hungry*;
  - Falta de padronização dos nomes;
  - Script de buscar por vulnerabilidades dos softwares registrados no sistema de inventário.

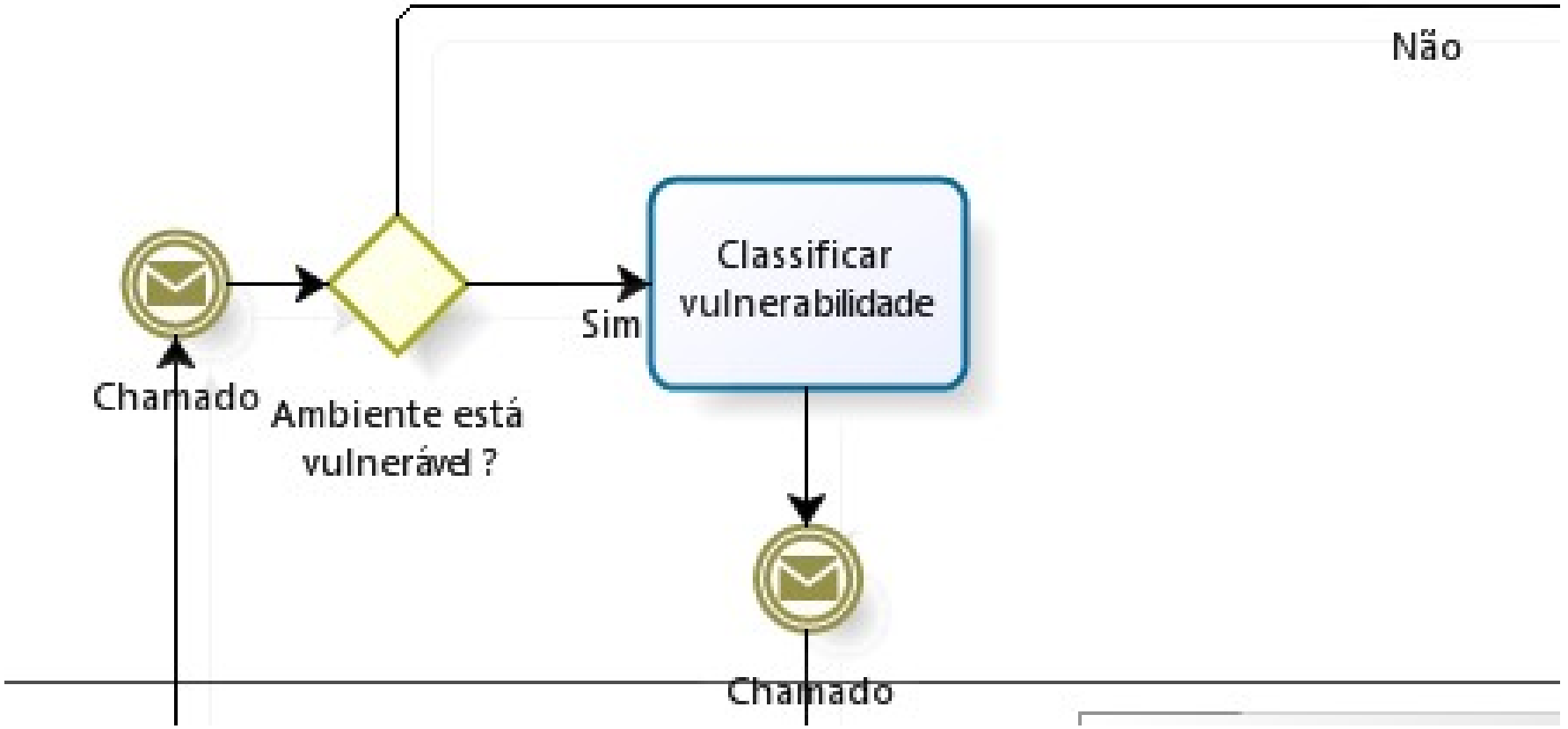
Auditoria

- Nmap + NSE
- OpenVAS
  - Scanner de Vulnerabilidade;
  - Feed de vulnerabilidades gratuito;
  - Baixo impacto nos alvos;
  - *Dashboard*;
  - *Resource Hungry* e lento;
  - Redes IPv6.

Auditoria

- Integração do OpenVAS com L2M
  - L2M - https://certbahia.pop-ba.rnp.br/projects/l2m/
  - Mantém o histórico da tabela ARP dos equipamentos;
  - Permite a detecção de novos *hosts* na rede e a execução de *scans* com OpenVAS destes *hosts*;
  - Permite criar *scans* para conjunto de endereços IPv6 ativos na rede;

Verificação e Classificação



Verificação

- Papel do especialista;
- Verificar se a vulnerabilidade afeta o ambiente;
- Realização de PoCs;
- Avaliar a necessidade de criar Ambiente de Teste;
- Avaliar o custo de aplicar o *patch versus* o custo de fazer uma PoC;

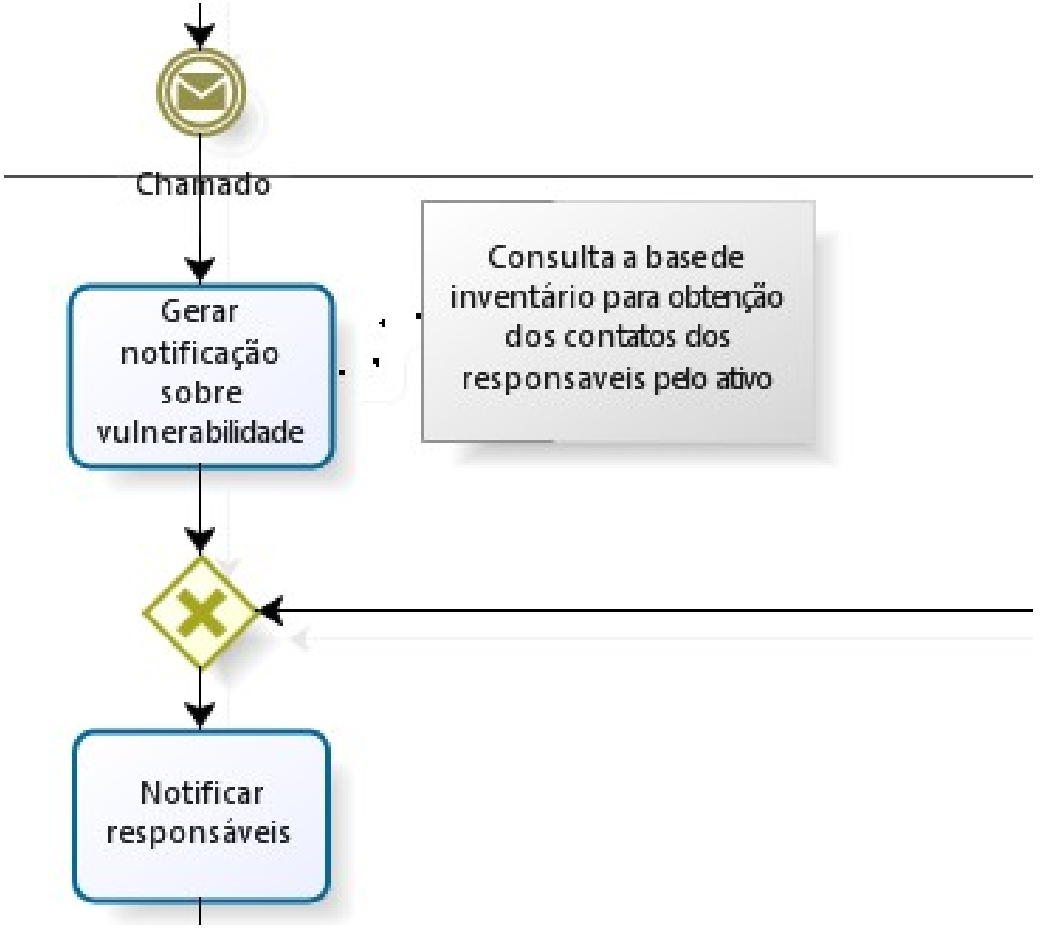
Classificação

- Permite priorizar os esforços para as vulnerabilidades mais críticas;
- CVSS: Common Vulnerability Scoring System;

IMPACTO À ORG.	Score CVSS		
	BAIXA	MÉDIA	ALTA
ALTO	3	2	1
MÉDIO	4	3	2
BAIXO	4	4	3

Prioridade	**Tempo Máximo para Solução (TMS)**
1	Em até 8hs úteis
2	Em até 16hs úteis
3	Em até 5 dias úteis
4	Em até 10 dias úteis ou em data posterior específica ou programada

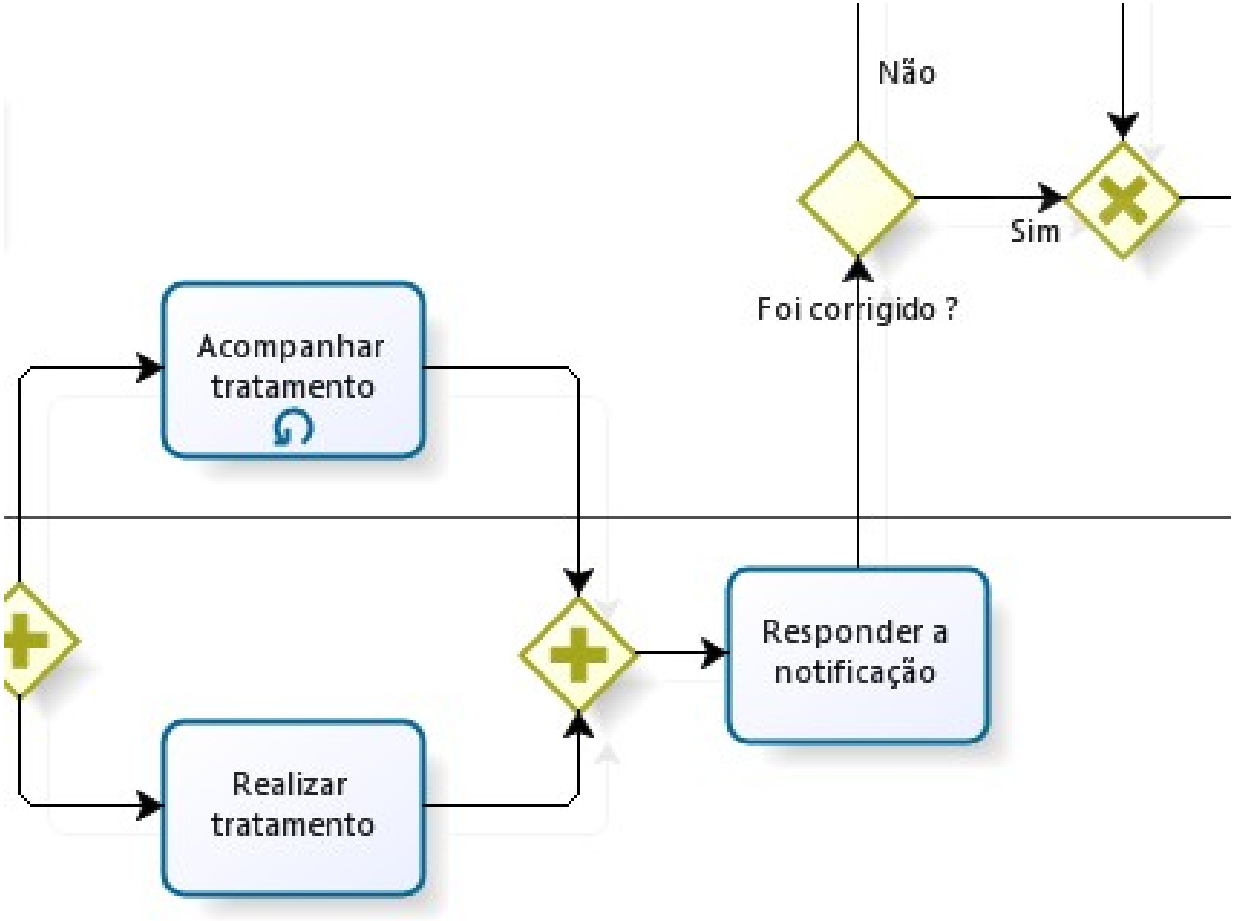
Notificação



Notificação

- Gestão de Inventários registra os contatos responsáveis dos ativos e sistemas;
- Sistema de Chamados para registro e acompanhamento;
  - Resquest Tracker (RT)
  - *Templates* de mensagem;
- Intervenção da ETIR em casos críticos.

Acompanhamento

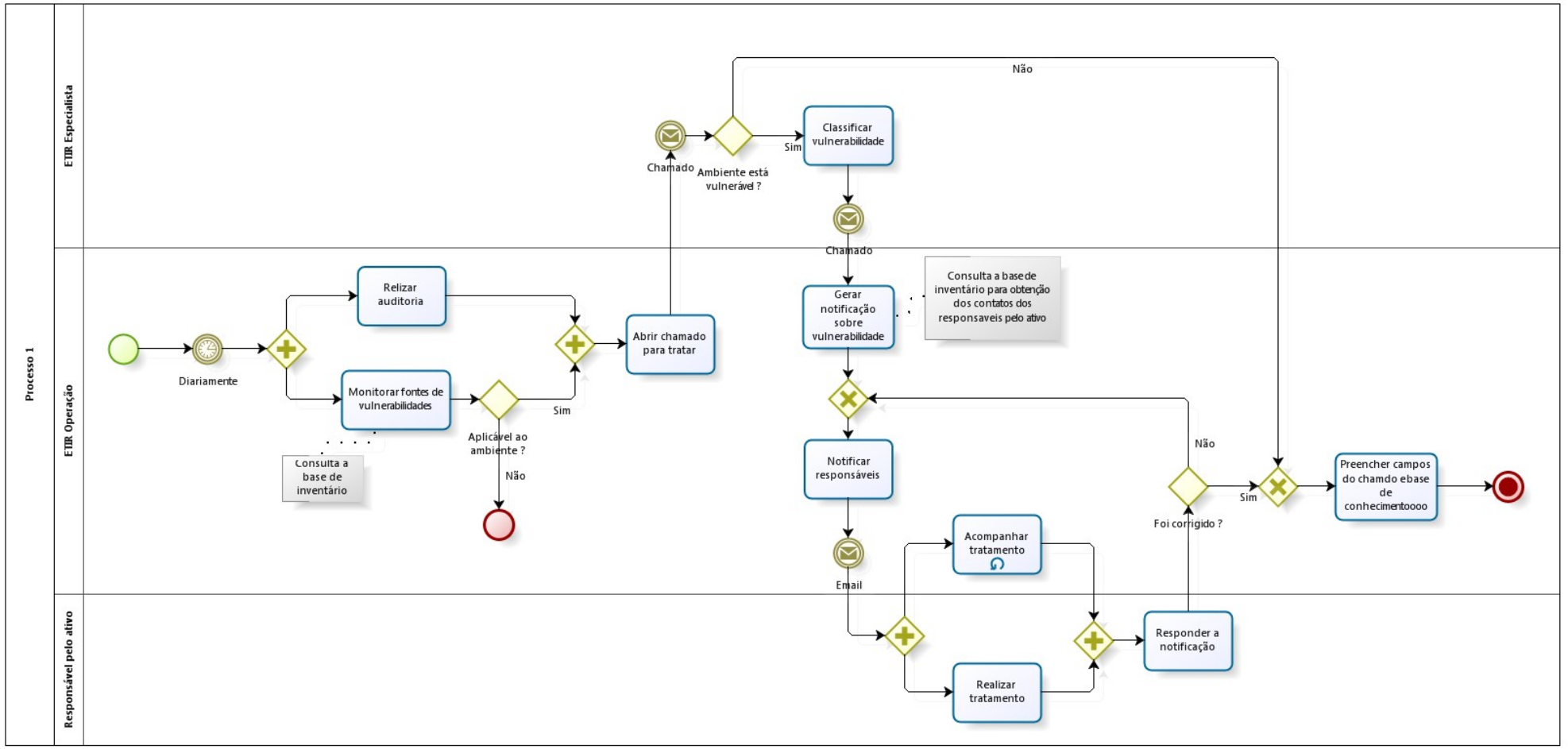


Acompanhamento e Validação

- Acompanhamento e suporte ao Responsável do Ativo na correção da vulnerabilidade;

- Verificar se a medida aplicada realmente corrige a vulnerabilidade.

Fluxo do Processo



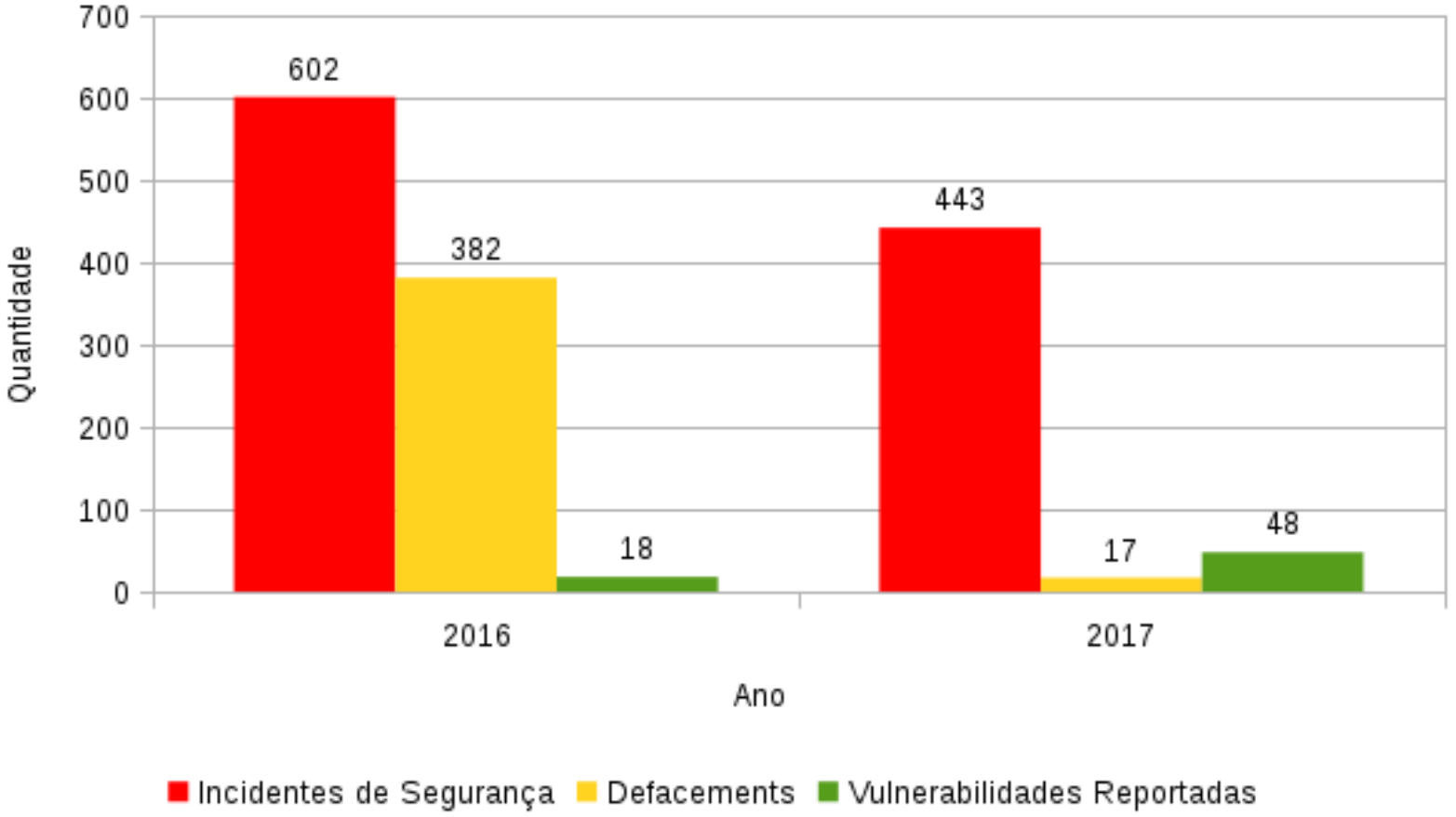
- Vulnerabilidade crítica (CVSS Score 9.8);
- Amplamente divulgada;
- *Exploit* disponível publicamente após 2 semanas.

- Sistemas críticos vulneráveis;
- ETIR atuou e *patch* foi aplicado em menos de 2h;
- Virtual Patching foi aplicado aos sistemas de terceiros e intensificou-se o monitoramento;
- Baixo número de incidentes.

Resultados

- 48 vulnerabilidades reportadas em 2017;
- Tempo para correção: de 1 a 6 meses;
- Redução de 25% no total de incidentes;
- Redução de 95% nos incidentes de desfiguração de páginas web.

Resultados


700
600
500
400
300
200
100
0
Quantidade
602
382
18
443
17
48
2016
2017
Ano
Incidentes de Segurança
Defacements
Vulnerabilidades Reportadas

Conclusão

- Maior conhecimento das vulnerabilidade que afetam a Instituição;
- Melhor capacidade de planejar e priorizar as ação de correção e/ou contenção das vulnerabilidades;
- Redução da quantidade de incidentes;
- Salvaguarda da equipe de segurança em relação à alta gestão.

Obrigado

Rogerio Bastos

https://sti.ufba.br/cosic
https://certbahia.pop-ba.rnp.br

POP-BA

Superintendência de Tecnologia da Informação | UFBA