Processo de Gestão de Vulnerabilidades de Segurança na UFBA

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.

Agenda

- Gestão de Vulnerabilidade:
  - O que é?
  - Normas
- O fluxo da UFBA
  - Papéis
  - Fases
    - Descoberta
    - Verificação
    - Classificação
    - Notificação
    - Acompanhamento e Validação
- Cases
- Resultados
- Trabalhos futuros
- Conclusão

O que é

- Conhecer fraquezas e brechas de segurança;
- Avaliação de risco ao negócio;
- Corrigir ou aceitar os riscos;

Importância

- *Menor risco de incidentes;*
- ***Salvaguarda!***

Antecipação

- Vulnerabilidade (e correção) divulgadas antes dos exploits;
  - 2017:
    - Universo: 732
    - NVD: 469
    - ExploitDB: 263

  - RODRIGUEZ, Luis Gustavo Araujo et al. Analysis of Vulnerability Disclosure Delays from the National Vulnerability Database. Workshop de Segurança Cibernética em Dispositivos Conectados (WSCDC_SBRC), [S.l.], v. 1, may 2018. Disponível em: < https://portaldeconteudo.sbc.org.br/index.php/wscdc/article/view/2394>. Acesso em: 18 may 2018.

Exemplos :(


Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy

Exemplos :(

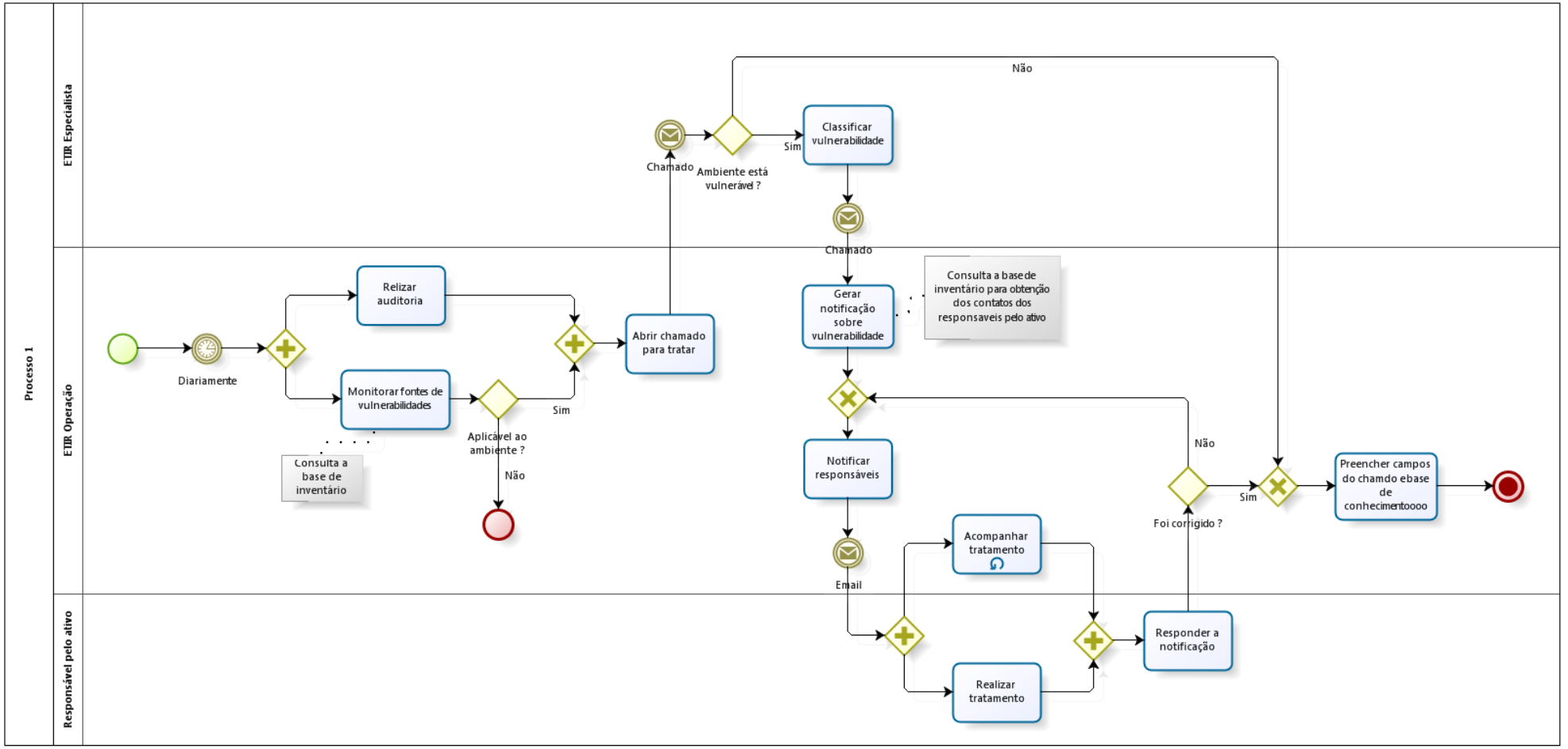
ABNT NBR ISO/IEC 27002:2013

- 12.6 Gestão de vulnerabilidades técnicas
  - Objetivo: Prevenir a exploração de vulnerabilidades técnicas.
  - Controle:
    - *Vulnerabilidades obtidas em tempo hábil;*
    - *Exposição a vulnerabilidades seja avaliada;*
    - *Medidas para lidar com os riscos.*

ABNT NBR ISO/IEC 27002:2013

- Diretrizes:
  - Funções e responsabilidades;
  - Inventário completo e atualizado;
  - SLAs;
  - Análise de priorização;
  - Virtual patching;
  - Base de conhecimento;
  - Métricas.

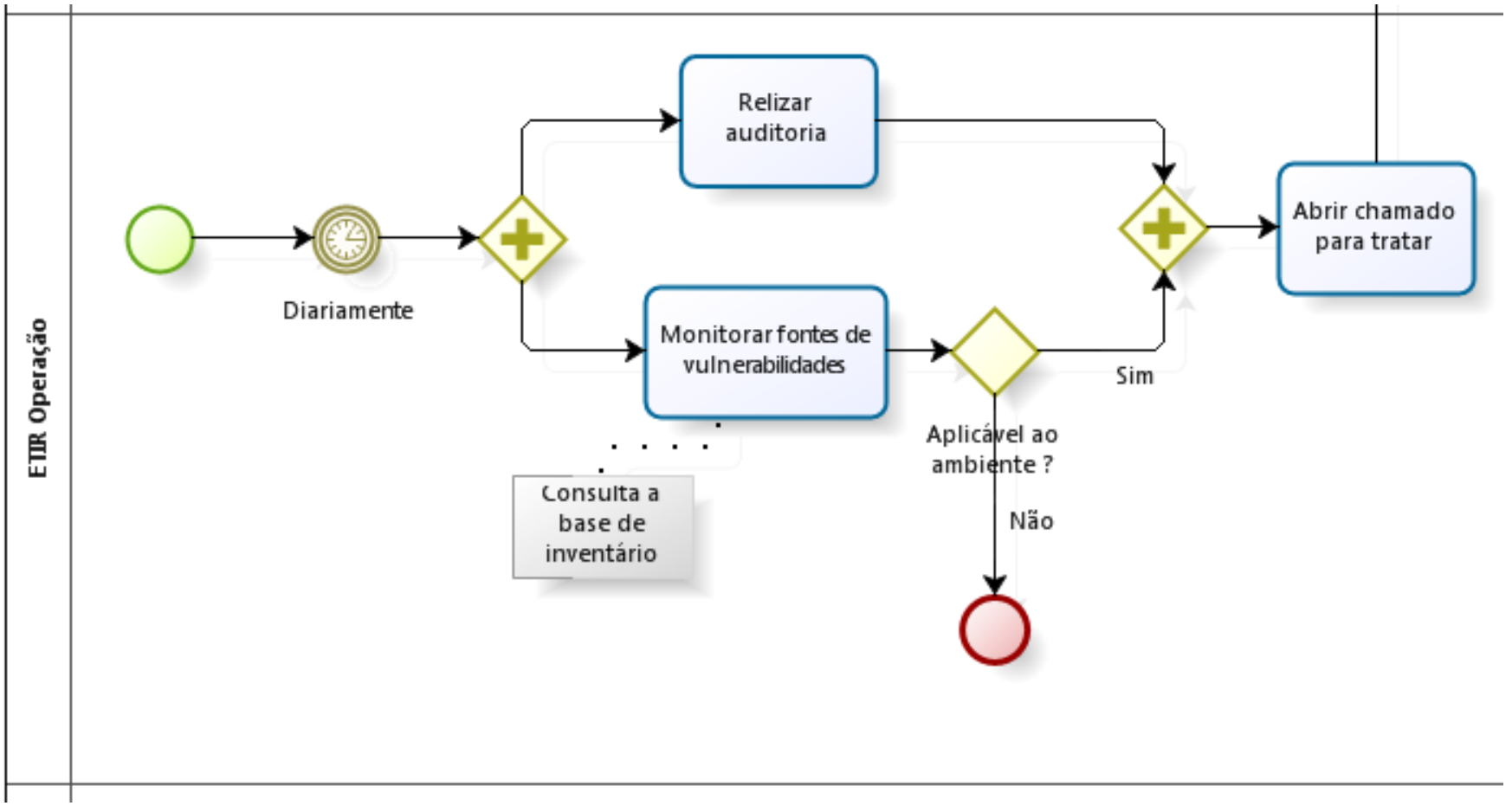
Fluxo do Processo da UFBA



Papéis

- ETIR:
  - Operação;
  - Especialista;
- Responsável pelo ativo;
- Gestor de Configuração;
- Gestor de Mudanças;
- Gestor de SIC e Superintendente de TI;
- Fabricantes e fornecedores.

Descoberta

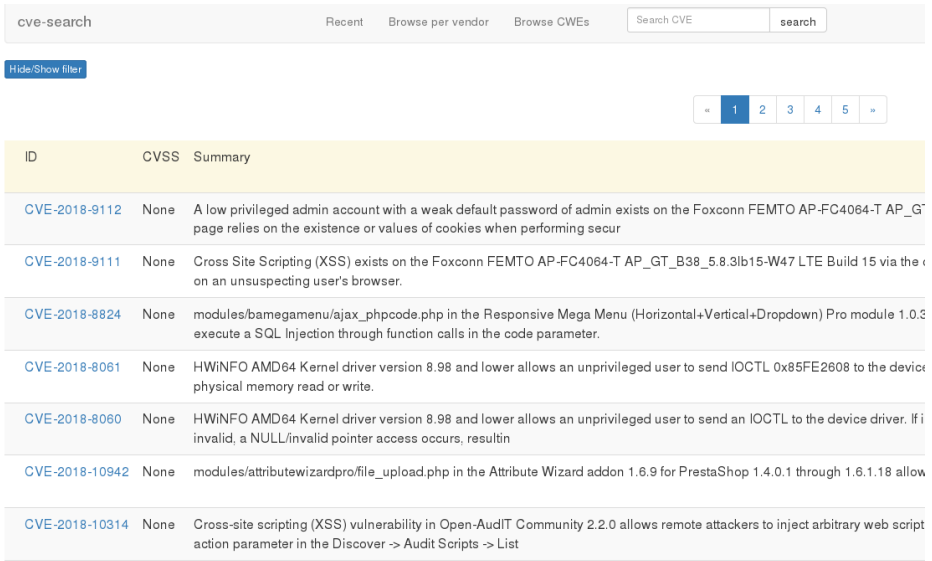

ETIR Operação
Diariamente
Relizar auditoria
Monitorar fontes de vulnerabilidades
Consulta a base de inventário
Aplicável ao ambiente ?
Sim
Não
Abrir chamado para tratar

Auditoria

- OpenVAS – Preocupações:
  - Overhead;
  - Agressividade;
  - Criticidade dos alertas;
  - Efetividade, falsos positivos...
  - Tempo /24, /64
    - RFC 4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6

Fontes de Vulnerabilidades

- Mail Lists:
  - BugTraq, FullDisclosure…
  - US-Cert, CAIS, Cert.Bahia...
  - Fabricantes, comunidades e projetos;
- CVE-Search

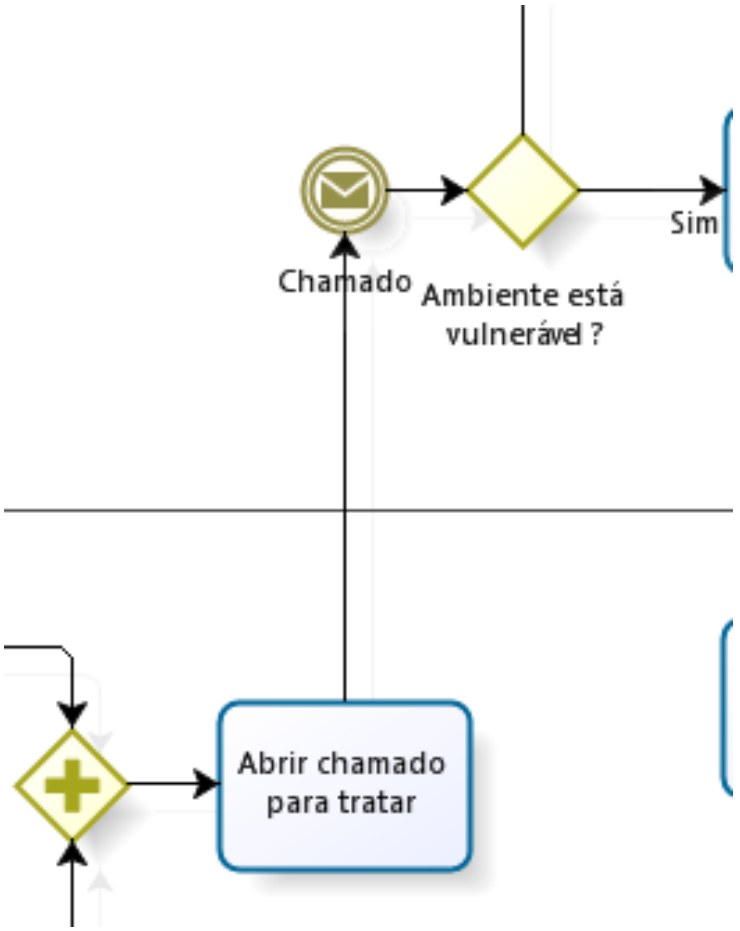


Aplicabilidade

- Gestão de inventário:
  - API para consultas;
  - Deploy simples;
  - Costumização da solução;
  - Histórico de mudanças;
- Nomenclaturas.

- iTop
- Wiki

Verificação

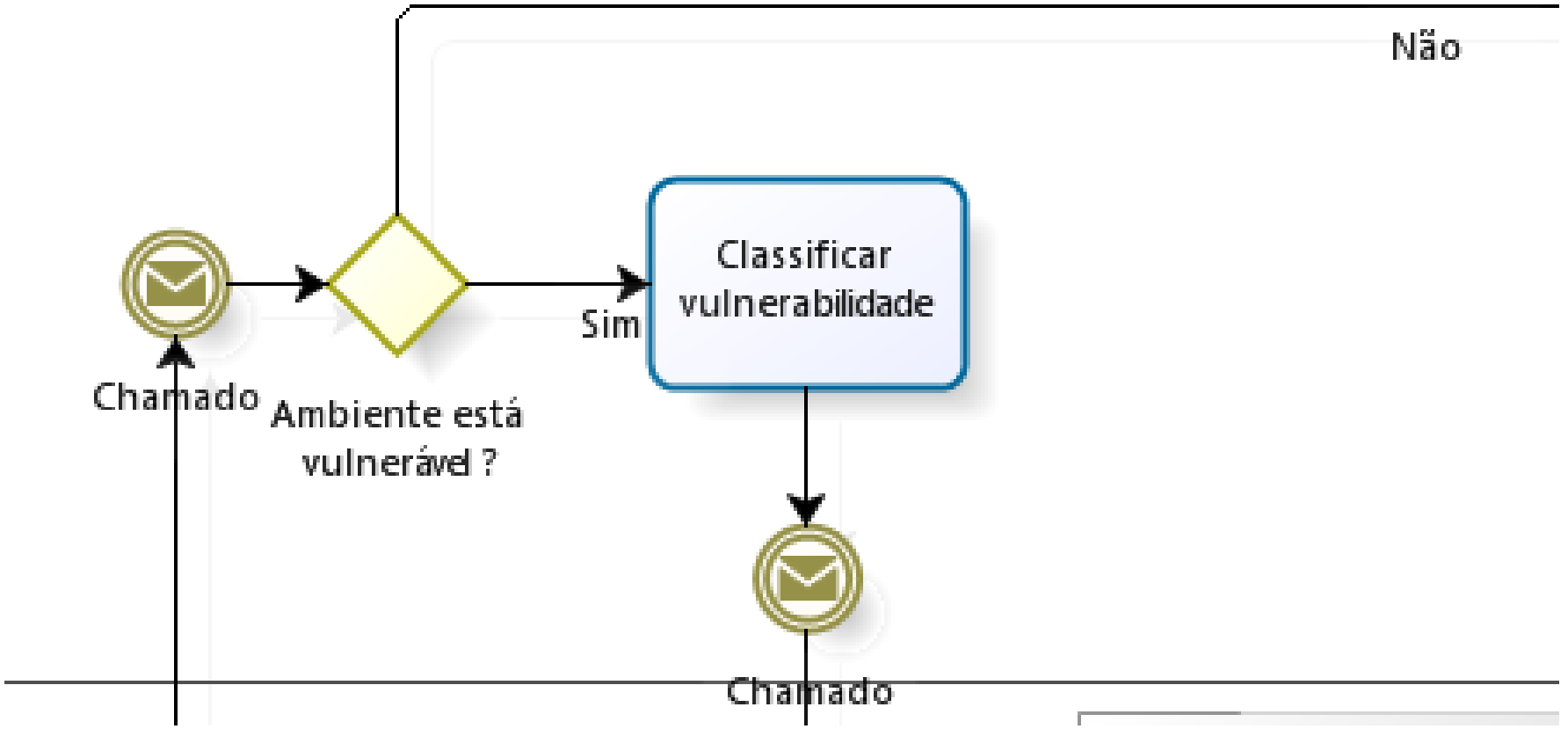


Verificação

- PoCs, PoCs e mais PoCs…
- Ambiente controlado vs Ambiente de produção
- **Documentar!**

- Papel do especialista!

Classificação



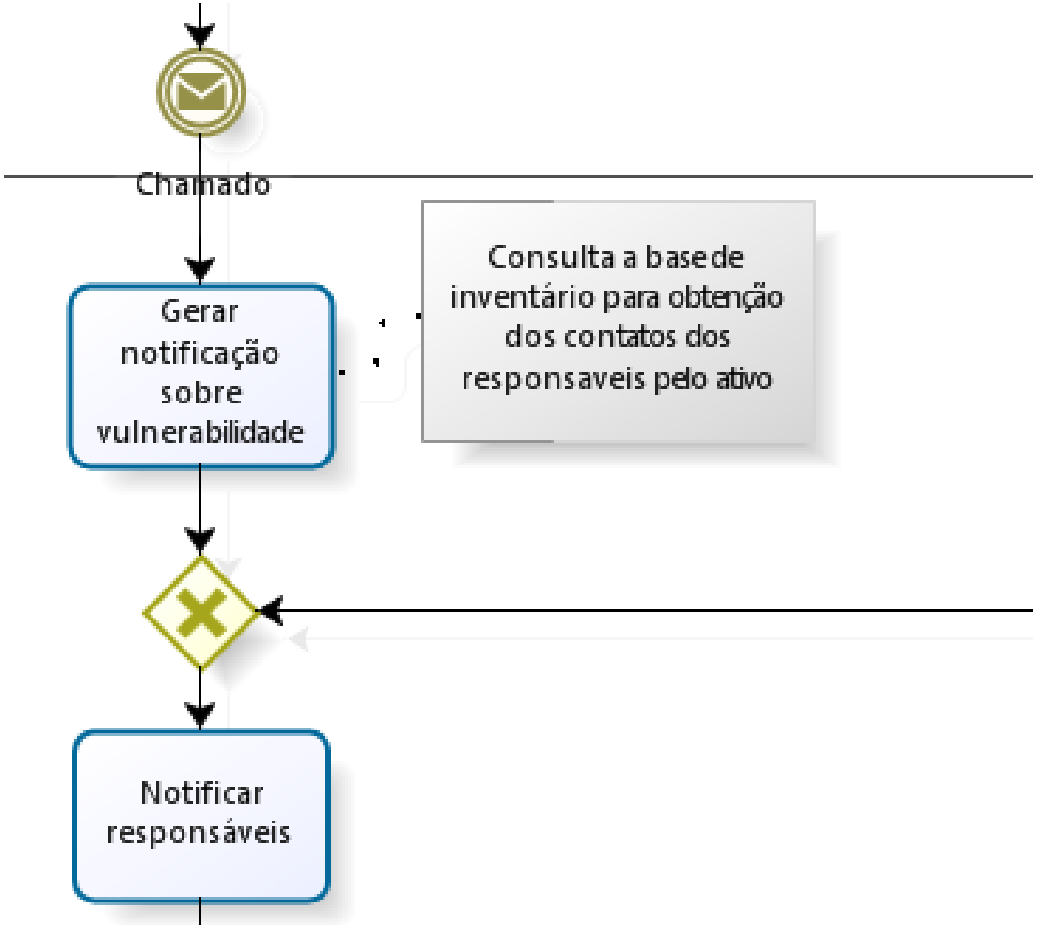
Classificação

- CVSS: Common Vulnerability Scoring System;
- Impacto à UFBA;
- Impacto vs CVSS → SLA

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

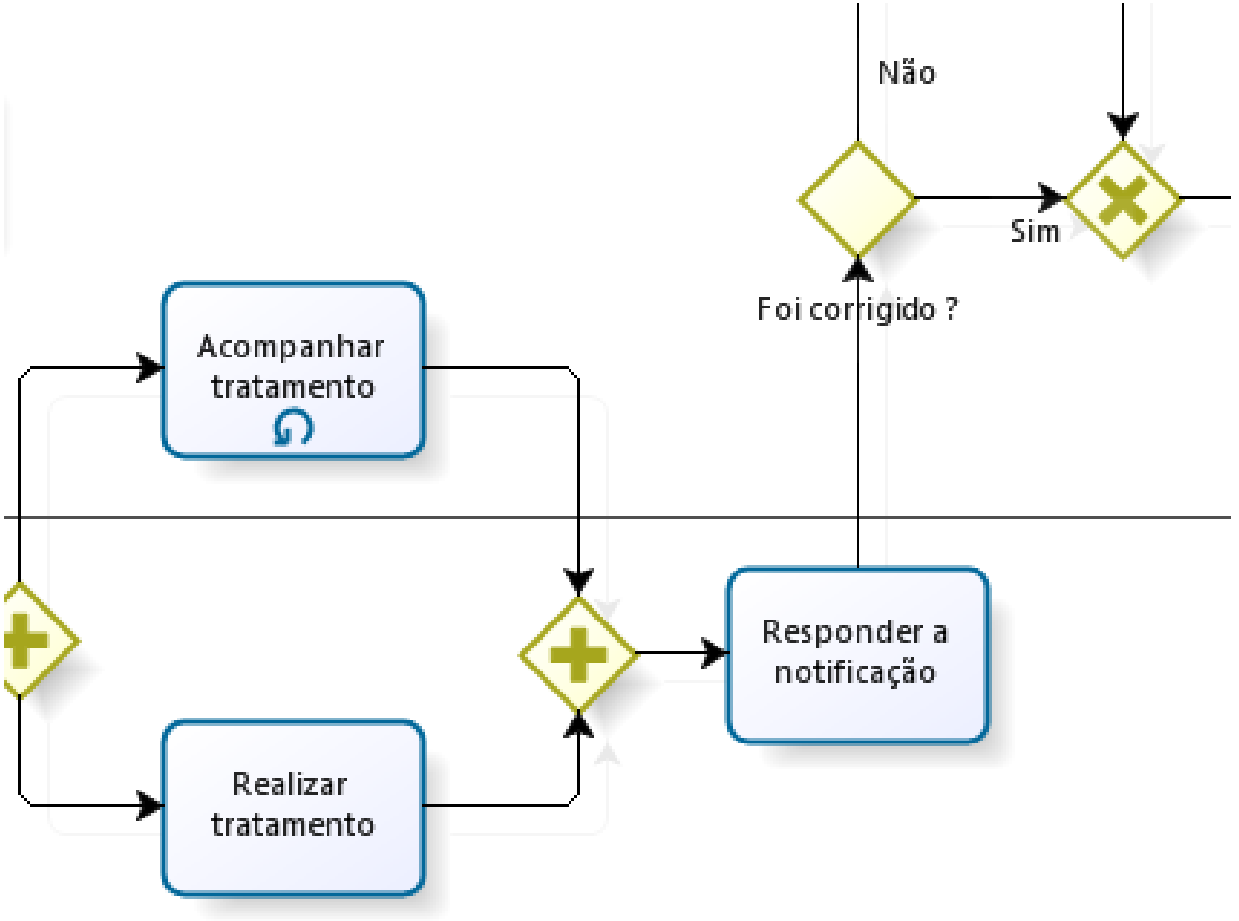
Notificação



Notificação

- Mais uma vez: Gestão de Inventários
  - **Atualizada constantemente!!**
- Templates de mensagem;
- Acompanhamento.

Acompanhamento



Acompanhamento

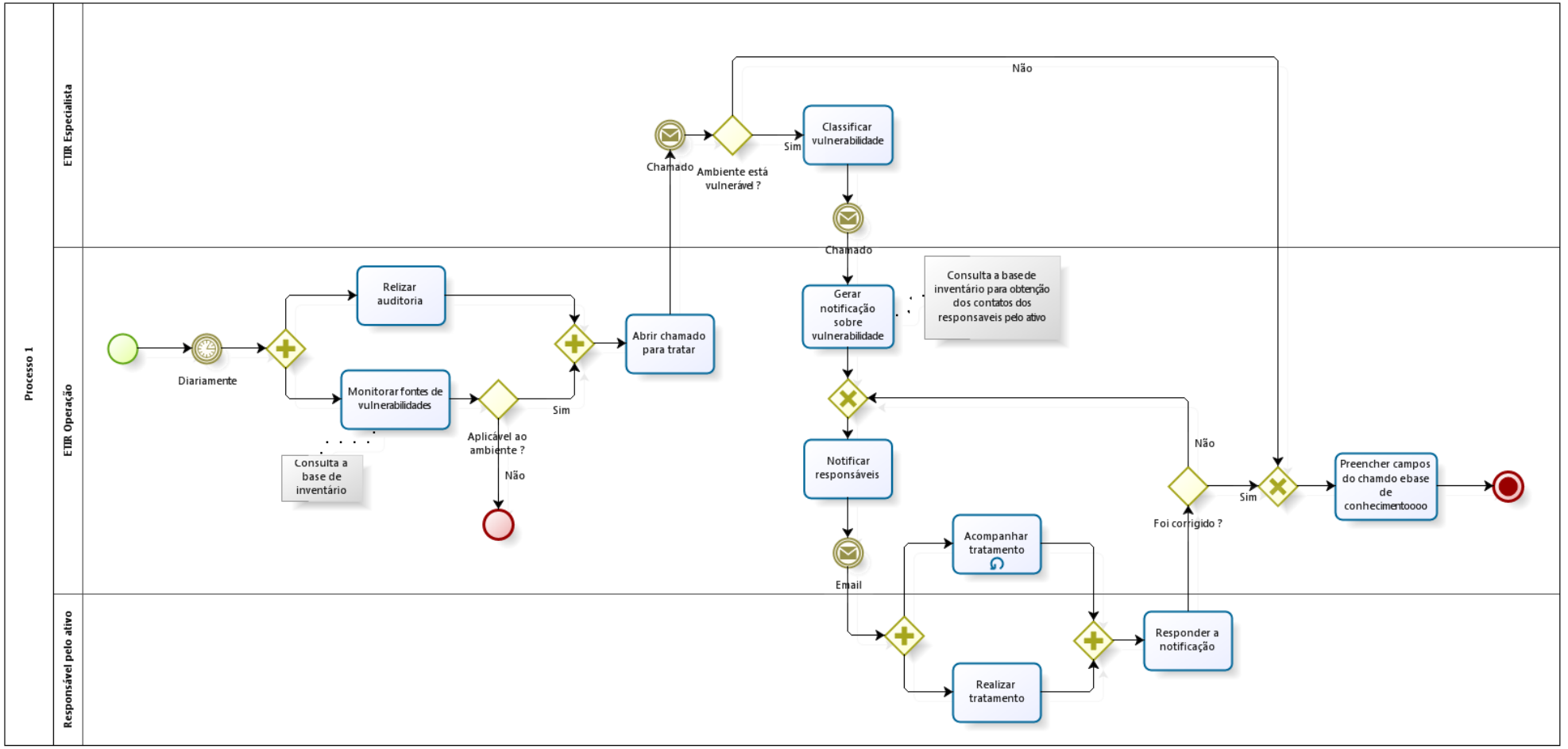
- Definição de formato:
  - E-mail;
  - Telefone;
- Definição de prazo: SLAs
  - Diariamente? Semanalmente?
  - O que fazer caso não seja cumprido?
    - Bloquear ativo?
    - Equipe agir?

Validação

- Execução dos testes feitos:
  - Seguir documentação feita na **Verificação**;

- Prosseguir com fechamento do chamado; ou
- Voltar à fase de notificação e acompanhamento.

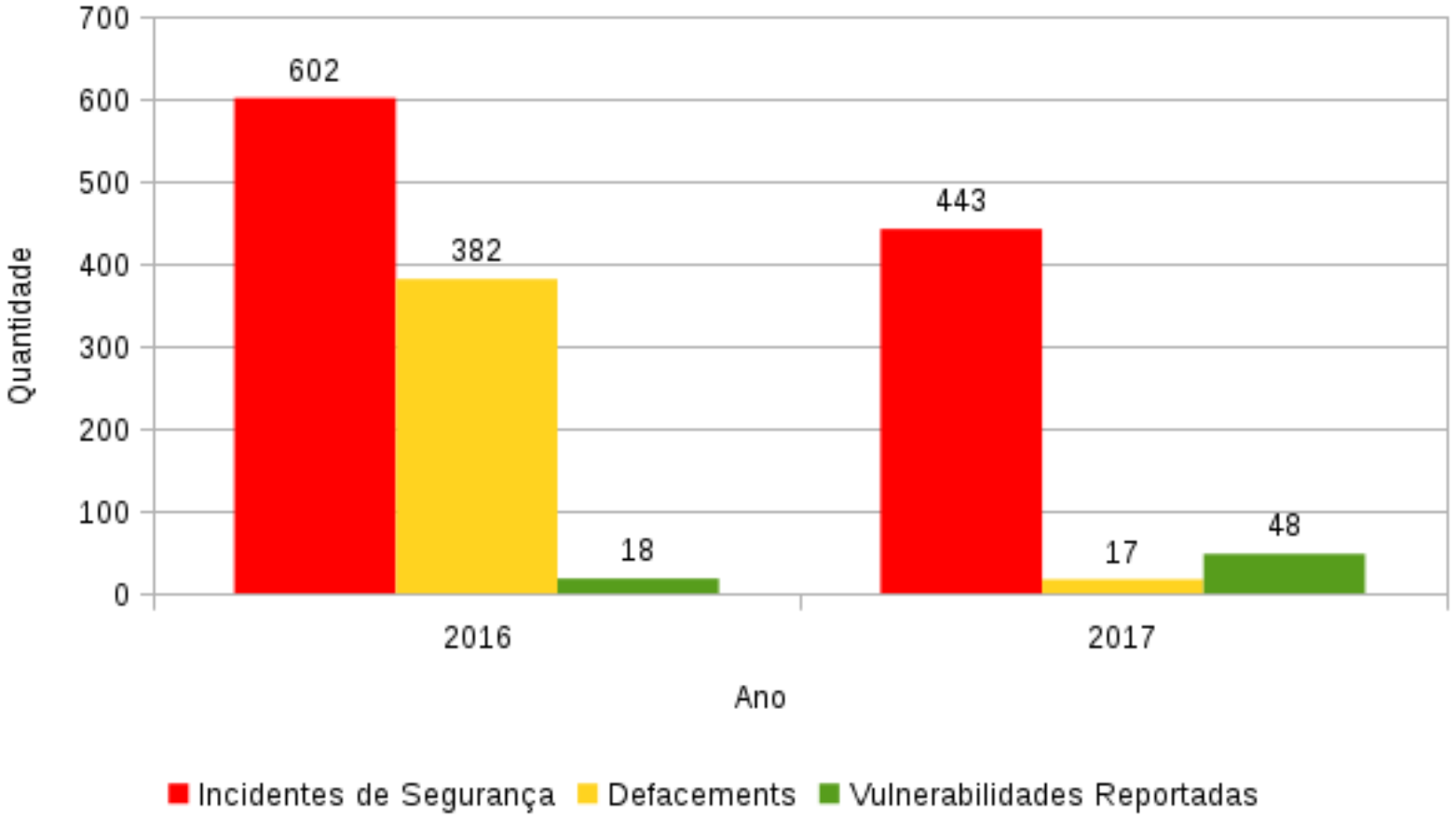
Fluxo do Processo



Cases

- **Salvaguarda**: Incidente de segurança grave;
- **Antecipação**: Vulnerabilidade crítica.

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

Trabalhos Futuros

- Aplicação do Processo de Gestão de Vulnerabilidades;
- Acordo de SLAs com demais setores;
- Consolidação dos indicadores.

- Detecção de vulnerabilidades ativamente;
- Automatização do processo.

Trabalhos Futuros

- Aplicação do Processo de Gestão de Vulnerabilidades;
- Acordo de SLAs com demais setores;
- Consolidação dos indicadores.

- Detecção de vulnerabilidades ativamente;
- Automatização do processo.

Conclusão

- Redução da quantidade de incidentes;
- Melhor documentação e comunicação;
- Respaldo da equipe de segurança em relação à alta gestão.

Obrigado!

Gildásio Júnior <jose.gildasio@ufba.br>

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

POP-BA

STI
Superintendência de
Tecnologia da Informação | UFBA