Sumário

[1. INTRODUÇÃO 2](#_Toc12366838)

[2. OBJETIVO 2](#_Toc12366839)

[3. METODOLOGIA 5W2H 2](#_Toc12366840)

[4. WHY – POR QUÊ? 2](#_Toc12366841)

[4.1. Evidências 2](#_Toc12366842)

[5. WHAT – O QUE? 2](#_Toc12366843)

[5.1. Evidências 2](#_Toc12366848)

[6. WHEN – QUANDO? 2](#_Toc12366849)

[6.1. Evidências 2](#_Toc12366851)

[7. WHERE – ONDE? 3](#_Toc12366852)

[7.1. Evidências 3](#_Toc12366853)

[8. WHO – QUEM? 3](#_Toc12366854)

[8.1. Evidências 3](#_Toc12366855)

[9. HOW – COMO? 3](#_Toc12366856)

[9.1. Evidências 3](#_Toc12366857)

[10. HOW MUCH – QUANTO? 3](#_Toc12366858)

[10.1. Evidências 3](#_Toc12366859)

[11. MELHORIAS 3](#_Toc12366860)

# INTRODUÇÃO

Esse documento tem como objetivo detalhar o incidente de segurança da informação ocorrido e como o mesmo foi respondido.

# OBJETIVO

Com os dados contidos nesse relatório será possível mensurar tempo de resposta de um incidente, criar novos procedimentos e processos para que em futuros incidentes semelhantes a equipe de CSIRT possa responder ao incidente mais rápido e com isso mitigar os danos causados.

# METODOLOGIA 5W2H

A ferramenta 5W2H nada mais é do que um checklist de atividades, que devem ser respondidos com o máximo de clareza e eficiência por todos os envolvidos na resposta do incidente tratado nesse relatório.

# WHY – POR QUÊ?

*O “por quê” do incidente pode se resumir a pergunta “por quê, isso é considerado um incidente?”. Tal ação é considerada pois, ... (comprometeu um serviço ou usuário, causou indisponibilidade...)*

### Evidências

# WHAT – O QUE?

*Detalhar o que aconteceu (houve um vazamento de informação, uma máquina foi invadida, detectado um malware...) com a maior riqueza de detalhes possíveis.*



### Evidências

# WHEN – QUANDO?

*Descrever quando ocorreu o incidente, principalmente o momento que a ferramenta identificou, independente do momento que foi identificado pelo analista ou colaborador, o mais importante e identificar o momento que o incidente iniciou.*



### Evidências

# WHERE – ONDE?

*Especificar onde ocorreu o incidente, desde solução (servidor X, ferramenta Y, estação Z...) até localidade (prédio 123, Datacenter, Sede...).*

### Evidências

# WHO – QUEM?

*Identificar o “pivô” do incidente, pode ser a pessoa que realizou a ação e deu origem ao incidente ou a pessoa que foi vítima de um incidente, dependendo do incidente o pivô pode ser o “atacante” ou a vítima.*

### Evidências

# HOW – COMO?

*Descriminar o como o incidente ocorreu (através de um phishing, um colaborador malicioso, um malware não identificado...).*

### Evidências

# HOW MUCH – QUANTO?

*Informar se houve danos financeiros ou gastos além do tempo usado na resposta do incidente (o serviço X ficou indisponível por Y minutos e isso causou prejuízo estimado em R$..., foi solicitado que a estação presenta na loja X fosse enviada para sede para analise forense...)*

### Evidências

# MELHORIAS

*Identificar melhorias na rede, processo, procedimento, solução... que possa ser melhorado com o viés de melhorar respostas futuras ou até mesmo evitar incidente futuros.*