
HEMOVITA CAXIAS | GRUPO VITA

HEMATOLOGISTAS ASSOCIADOS GRUPO VITA

Clínica de Hemoterapia GRUPO VITA

Hemobanco GRUPO VITA

vita HEMOTERAPIA GRUPO VITA

CTN GRUPO VITA

Centro de Hematologia e Hemoterapia GRUPO VITA

HEMOVITA POA | GRUPO VITA

Instituto Pasquini GRUPO VITA

UHHS Hemoterapia e Hematologia GRUPO VITA

Procélula TERAPIA CELULAR GRUPO VITA

GRUPO VITA

vita SÃO PAULO GRUPO VITA

vitabahia GRUPO VITA

# TREINAMENTO

## PRO_10.002-Procedimento de Registro de Não Conformidades (RNC)

Comitê de Segurança da Informação

Informação Interna

2023 - Versão 1

# Procedimento de Registro de Não Conformidades

- **PRO_10.002-Procedimento de Registro de Não Conformidades**

**1. INTRODUÇÃO**

1.1. Este procedimento deve ser usado quando for detectada uma não conformidade real ou potencial que afete a segurança da informação do Grupo Vita.

**2. PROPÓSITO**

2.1. O objetivo deste procedimento é estabelecer uma sistemática para executar ações corretivas e/ou preventivas para eliminar as causas de não conformidades reais e potenciais que possam afetar o Sistema de Segurança da Informação do Grupo Vita, garantindo o cumprimento das suas Políticas e Procedimentos.

# Procedimento de Registro de Não Conformidades

- **PRO_10.002-Procedimento de Registro de Não Conformidades**

**4. PROCEDIMENTOS**

**4.1. Registro de Não-Conformidade:**

4.1.1 Todo colaborador, ao detectar uma não conformidade real ou potencial, deve imediatamente emitir um RNC (Registro de Não Conformidade) para a tratativa do problema, utilizando o formulário publicado na Plataforma OneTrust do Grupo Vita. O formulário preenchido será encaminhado ao Comitê de Segurança da Informação.

4.1.2 O Gerente do Comitê delibera sobre o assunto e indica a área/responsável para a tratativa do problema. Caso o assunto não seja procedente em relação ao Sistema de Segurança da Informação implantado, o Gerente notificará o emitente e o Comitê para o cancelamento do RNC.

# Procedimento de Registro de Não Conformidades

- **PRO_10.002-Procedimento de Registro de Não Conformidades**

4.1.3 Quando procedente, o Comitê encaminha o RNC, via e-mail, ao endereço do responsável da investigação da causa da não-conformidade, que deverá também determinar as ações corretivas ou preventivas para a eliminação do problema e quando se tratar de reclamações de clientes, fornecedores ou titulares de dados, posicioná-los sobre a solução aplicada.

4.1.4 Após as ações executadas pelo responsável da investigação, o RNC deverá ser reencaminhado via Plataforma OneTrust ao Comitê de Segurança da Informação, com a descrição da solução aplicada e, se for o caso, com arquivo de documentos complementares anexados.

# Não Conformidades

- **Tipos de não conformidades:**

  1) **Não Conformidade Real**: é tratada com ações corretivas, ou seja, o problema já ocorreu.

  2) **Não Conformidade Potencial**: é tratada com ações preventivas, ou seja, prevenir antes que ocorra.

- **Exemplos do que pode originar não conformidades reais ou potenciais:**

  - Descumprimento das diretrizes e dos procedimentos do Sistema de Segurança da Informação;

  - Incidentes nas atividades do dia-a-dia, como: vazamento de informações, extravio de documentos, armazenamento indevido, roubo/furto/extravio de ativos de informação, etc.;

  - Requisição ou reclamação de clientes, colaboradores ou de titulares de dados;

  - Problemas técnicos, problemas nos serviços, instabilidade da internet, alerta de vírus, etc.;

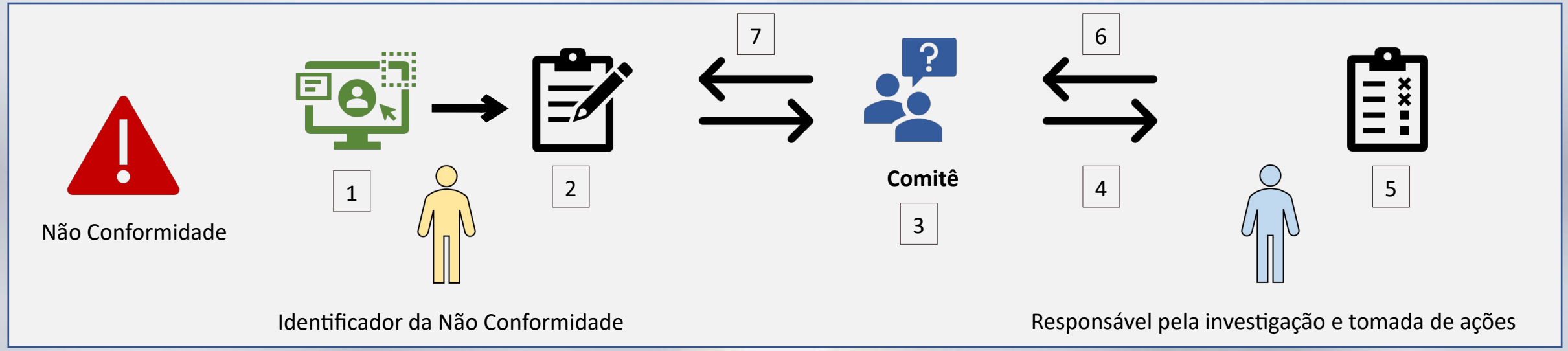
  - Auditorias internas e externas; e

  - Notificação de órgãos públicos.

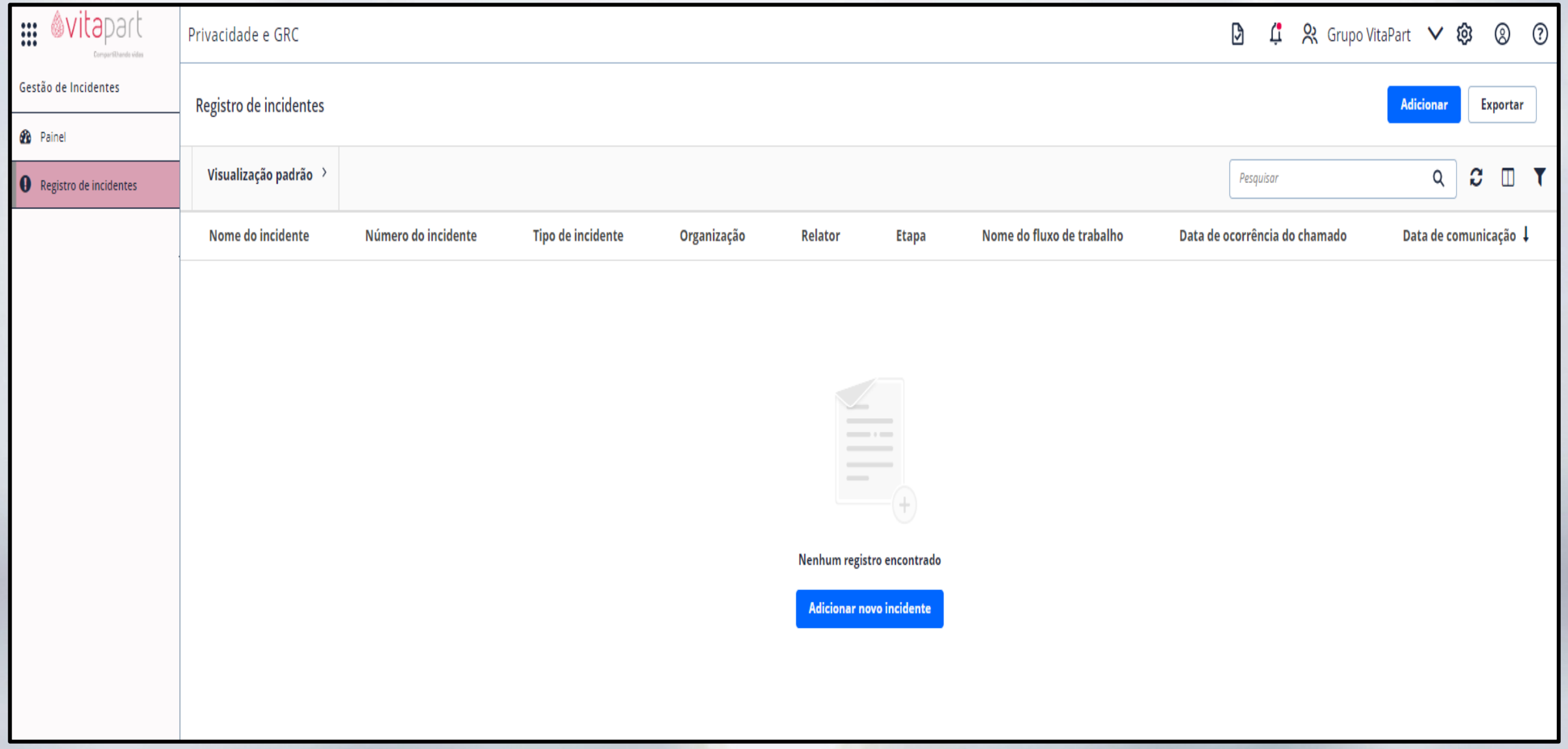
# Registro de Não Conformidades

- **O que deve ser feito após a identificação de uma Não Conformidade?**

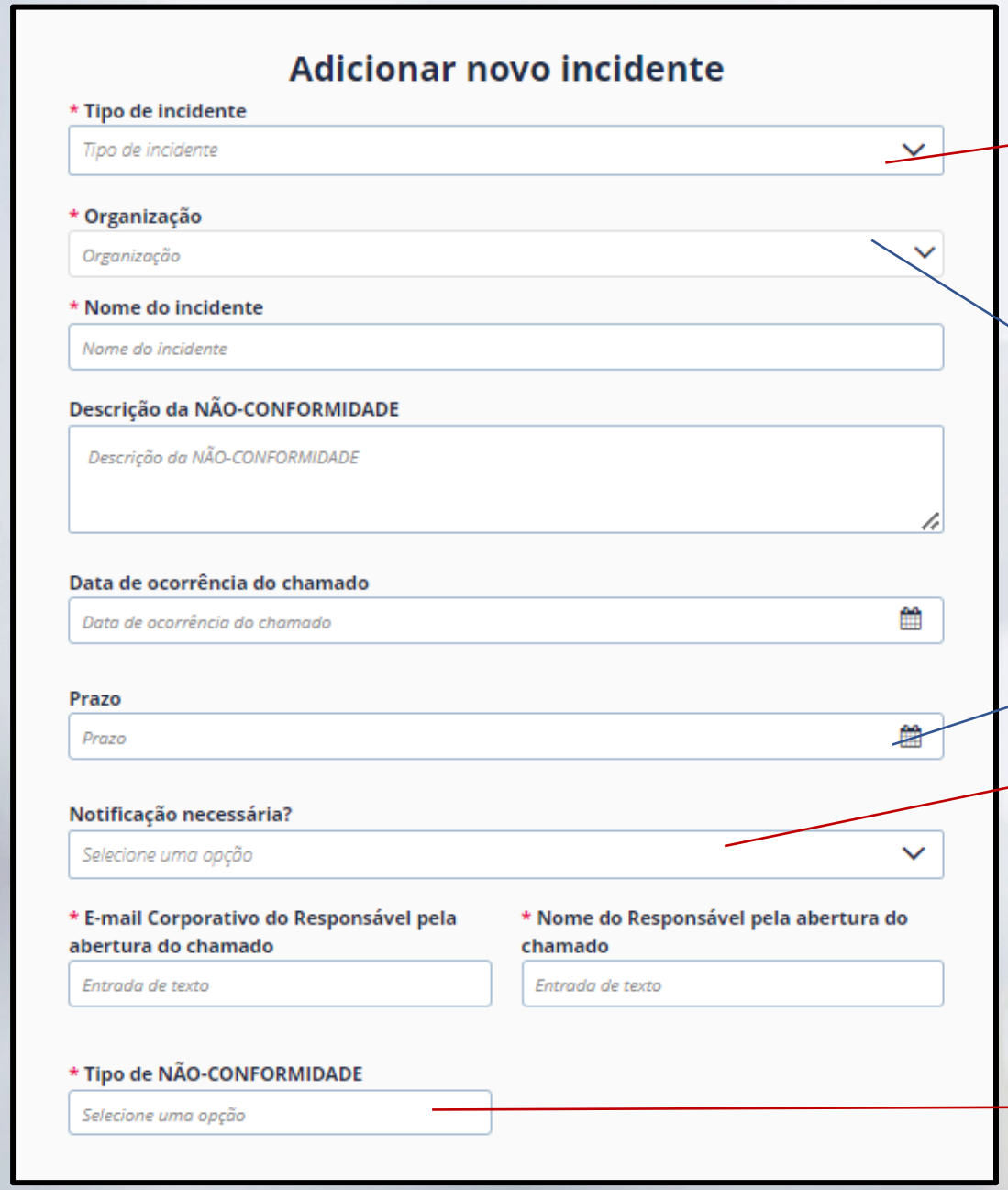
1. Acessar o formulário de Registro de Incidente na plataforma OneTrust;
2. Preencher e encaminhar o formulário para o Comitê de Segurança da Informação clicando em “Salvar”;
3. O Comitê fará a deliberação sobre o assunto e indicará o responsável para a tratativa do problema, através da criação de tarefa.
4. O Comitê encaminha via fluxo de trabalho para o responsável pela investigação da Não Conformidade;
5. O responsável investiga a causa do problema ou do potencial problema e toma as ações corretivas, preventivas ou de melhorias, conforme o caso;
6. O responsável pela investigação devolve o formulário preenchido para avaliação do Comitê; e
7. O Comitê envia o RNC para o identificador da Não Conformidade verificar a eficácia das ações tomadas e informa a todos os envolvidos.



# Formulário de Registro de Incidentes



# Formulário de Registro de Incidentes




Unidade onde foi identificada a Não Conformidade

Informar caso haja algum prazo a ser cumprido

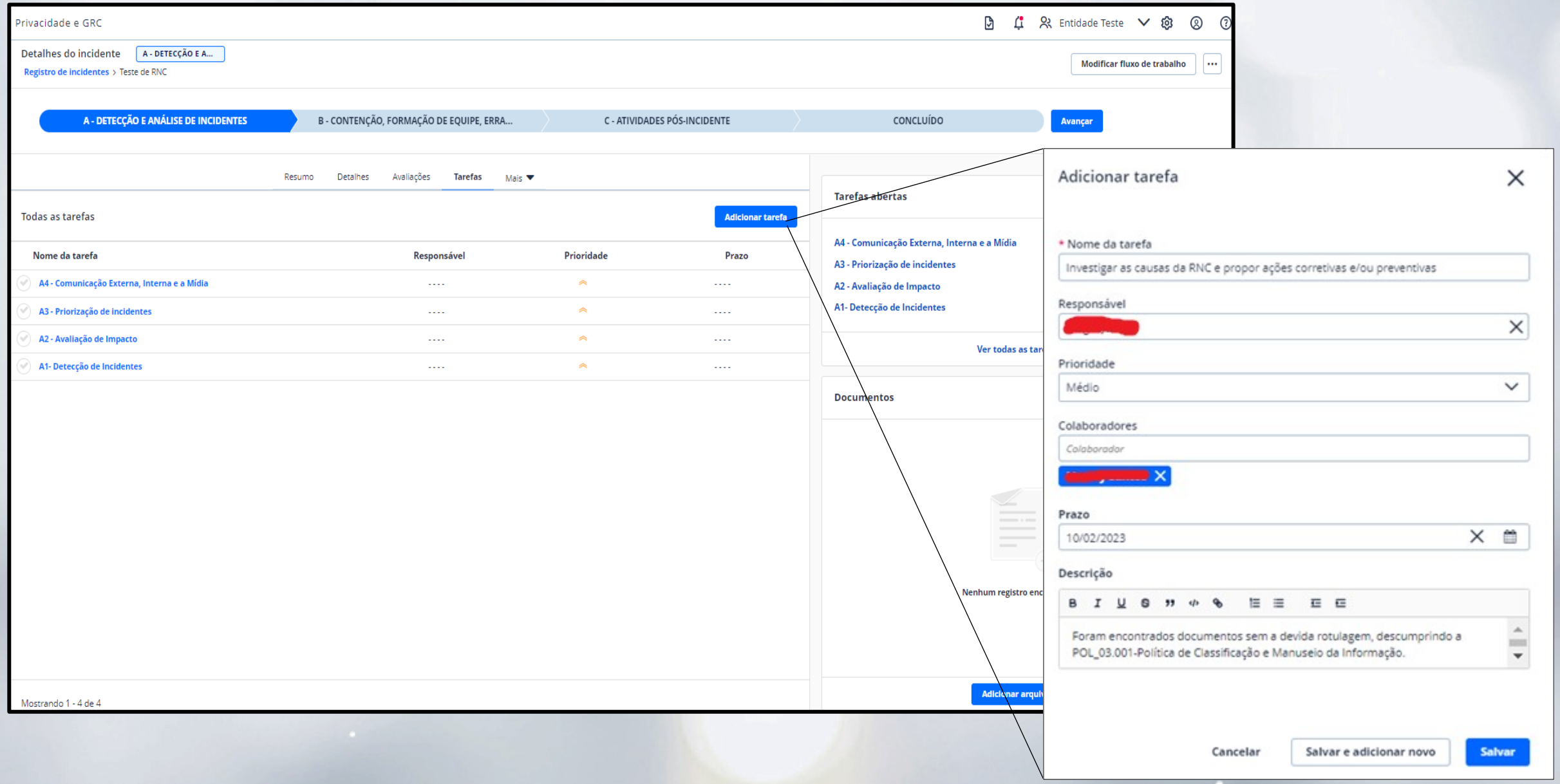
**Notificação de órgãos reguladores**

- Não tenho certeza
- Sim
- Não

- CORRETIVA
- PREVENTIVA

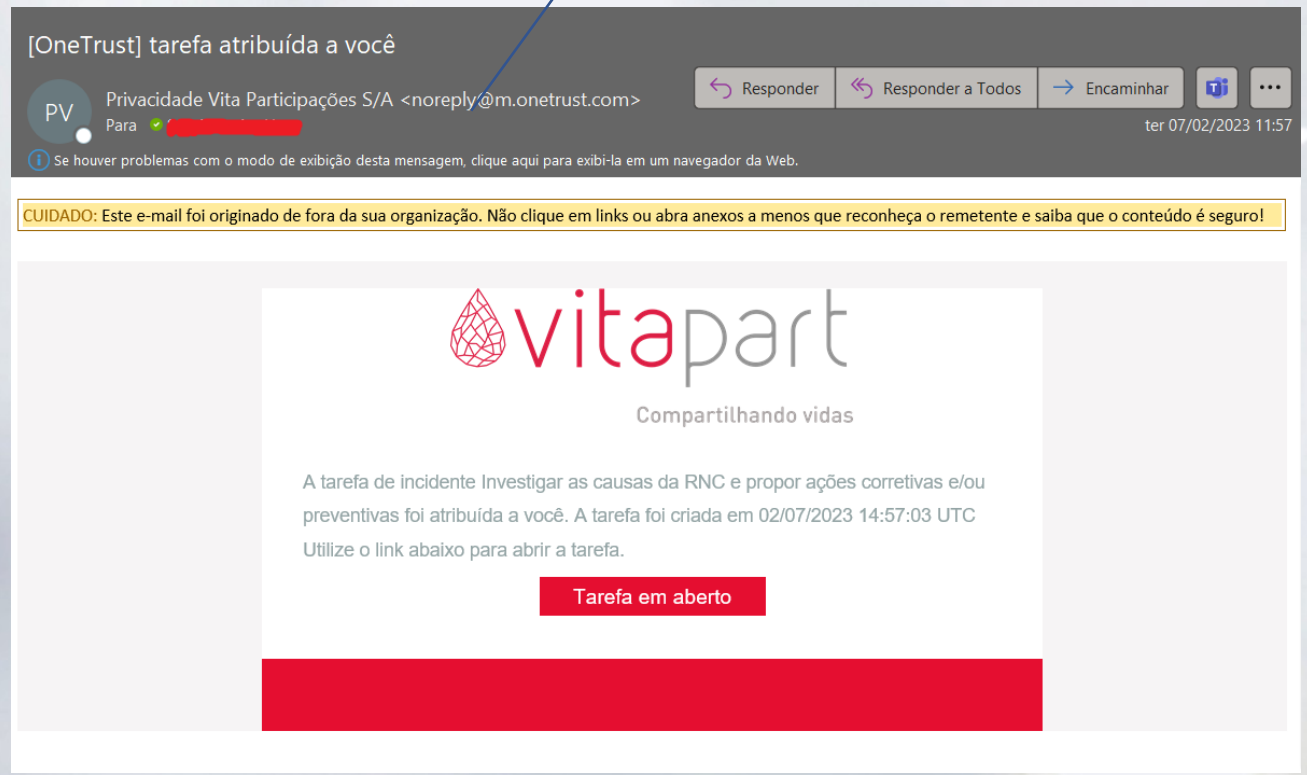
- Descumprimento de política/procedimento
- Farsa
- Identificação de possível risco à segurança das informações ou à infraestrutura
- Intrusão
- Perda/roubo
- Extravio de e-mail
- Análise/pesquisa de rede
- Raiz comprometida
- Engenharia social (por exemplo, phishing)
- Abuso do sistema
- Vulnerabilidade técnica
- Alteração não autorizada
- Divulgação de informações não autorizada
- Conta de usuário comprometida
- Vírus/ Código malicioso
- Degradação do website

# Fluxo de Tratamento de Incidentes do Comitê

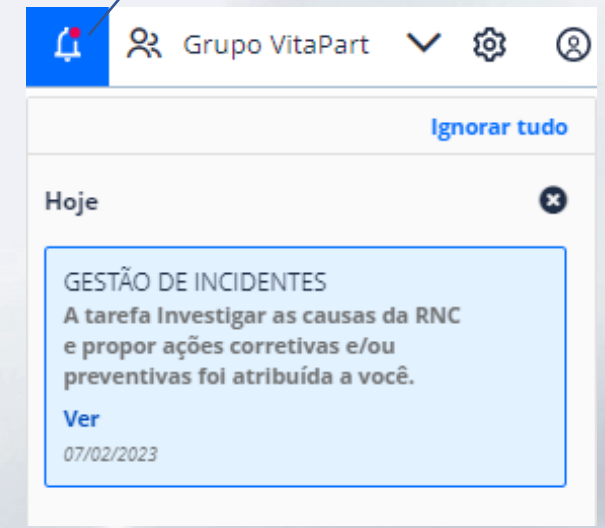


# Notificação para o Responsável pela Investigação do RNC

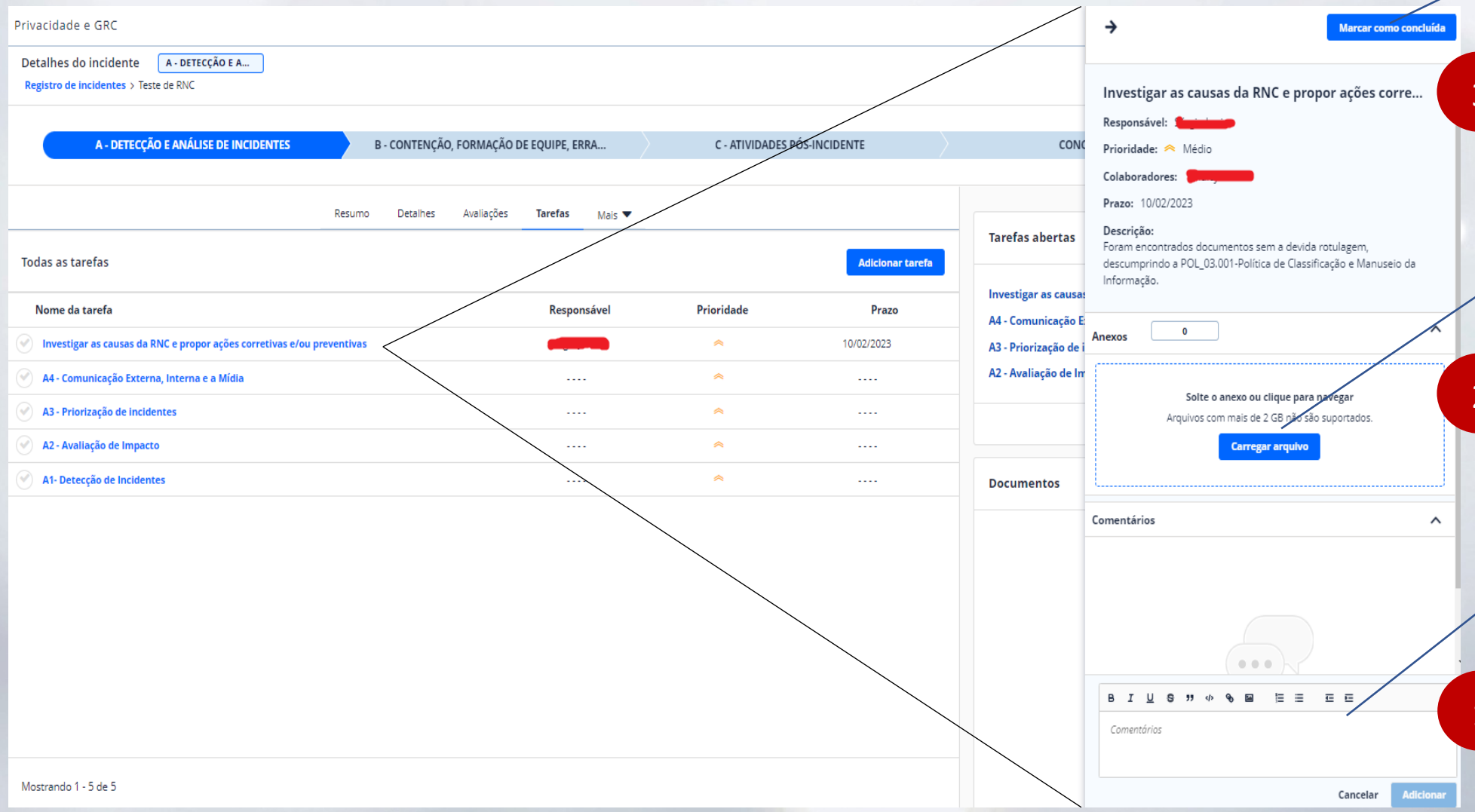
Receberá notificação por e-mail para acessar a Plataforma OneTrust




Lista de Notificações dentro da Plataforma OneTrust



# Tarefa atribuída ao responsável por investigar as causas do RNC




3 Marcar como Concluído quando finalizar a investigação

2 Anexar as evidências das ações corretivas e/ou preventivas

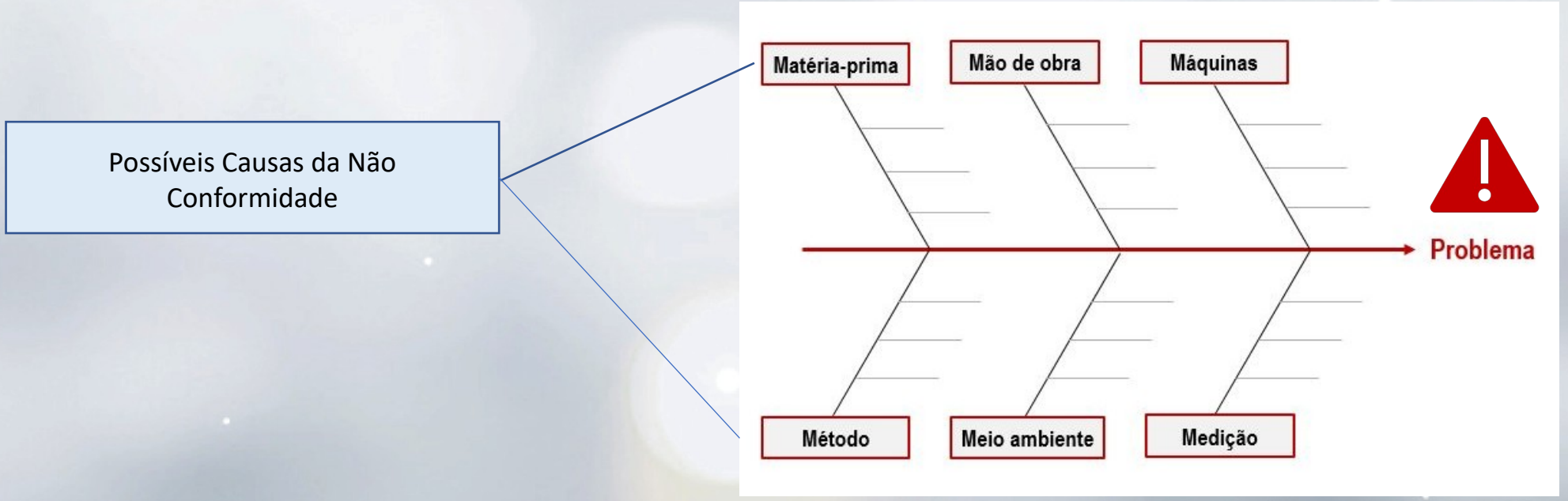
1 Preencher com o descritivo da investigação e as ações corretivas e/ou preventivas

# Procedimento de Registro de Não Conformidades

- **PRO_10.002-Procedimento de Registro de Não Conformidades**

## 4.2 DETECÇÃO E ANÁLISE DE INCIDENTES

Através das investigações de um RNC, um incidente pode ser detectado de várias maneiras e através de várias fontes diferentes, dependendo da natureza e localização do incidente. Alguns incidentes podem ser detectados através de softwares usados dentro do Grupo Vita ou por colaboradores que notam atividades incomuns. Outros podem ser notificados por terceiros, como um cliente, fornecedor ou autoridade que tomou conhecimento de uma violação, talvez porque as informações violadas foram usadas de alguma forma para fins maliciosos.



# Procedimento de Registro de Não Conformidades

- **PRO_10.002-Procedimento de Registro de Não Conformidades**

**4.3 AVALIAÇÃO DE IMPACTO**

A avaliação inicial de impacto deve ser realizada pelo Comitê para decidir a resposta apropriada.

Esta avaliação de impacto deve estimar:

- A extensão do impacto na infraestrutura de TI, incluindo computadores, redes, equipamentos e acomodações;
- Os ativos de informação que podem estar em risco ou foram comprometidos;
- A provável duração do incidente, ou seja, quando pode ter começado;
- As áreas de negócios afetadas e a extensão do impacto para elas; e
- Indicação inicial da provável causa do incidente.

# Procedimento de Registro de Não Conformidades

- **PRO_10.002-Procedimento de Registro de Não Conformidades**

### 4.3.1. PRIORIZAÇÃO DE INCIDENTES

Como resultado dessa análise inicial, o Comitê ou qualquer membro da equipe tem autoridade para entrar em contato com o Líder da Equipe de Resposta a Incidente a qualquer momento, para pedir que avalie se o procedimento **PRO_10.001-Procedimento de Resposta a Incidentes de Segurança da Informação** deve ser ativado. Este é provavelmente o caso para todos os incidentes de alta prioridade e para incidentes de prioridade média, quando considerado apropriado.

| NÍVEL DE PRIORIDADE | DESCRIÇÃO |
|---|---|
| Alta | Interrupção real ou potencialmente significativa para os negócios.<br>Exemplos:<br>• Um malware foi detectado e está se espalhando pela rede<br>• Um acesso não autorizado a quantidades significativas de dados confidenciais foi detectado<br>• O Site ou o Portal não estão disponíveis para os clientes, devido a um possível problema nos serviços |
| Média | Interrupção localizada, afetando várias áreas de negócio.<br>Exemplos:<br>• Rede única indisponível<br>• Rede executando lentamente<br>• Perda de um disco rígido |
| Baixa | Inconveniência localizada, afetando um único usuário.<br>Exemplos:<br>• Pequena violação da política de segurança da informação<br>• Alerta de vírus em um único computador<br>• Compartilhamento de senha |

# Procedimento de Registro de Não Conformidades

- **PRO_10.002-Procedimento de Registro de Não Conformidades**

**4.3.2. ATIVANDO O PROCEDIMENTO DE RESPOSTA A INCIDENTES**

Uma avaliação inicial de impacto já terá sido feita pelo Comitê, mas antes de decidir se uma resposta formal a incidentes deve ser iniciada, deve avaliar se algum dos seguintes se aplicam:

- Há perda real ou potencial significativa de informações confidenciais
- Há uma interrupção real ou potencial significativa nas operações comerciais
- Há risco significativo para a reputação do negócio
- Qualquer outra situação que possa causar impacto significativo para a organização

Se o incidente for justificado, então o procedimento **PRO_10.001-Procedimento de Resposta a Incidentes de Segurança da Informação** será ativado.

# Procedimento de Resposta a Incidentes originado pelo RNC

- **PRO_10.001-Procedimento de Resposta a Incidentes de Segurança da Informação**

## 4.9.3. NOTIFICAÇÃO

Há situações em que será necessário notificar a Autoridade Nacional de Proteção de Dados (ANPD), quando houver risco ou dano relevante aos titulares (vide previsão do art. 48 da LGPD). A ANPD recomenda que os controladores adotem posição de cautela, de modo que a comunicação seja efetuada mesmo nos casos em que houver dúvida sobre a relevância dos riscos e danos envolvidos. Ressalte-se ainda que, em eventual e comprovada subavaliação dos riscos e danos por parte dos controladores, pode ser considerada descumprimento à legislação de proteção de dados pessoais.

A comunicação à ANPD apenas não será necessária se for possível demonstrar, de forma irrefutável, que a violação da segurança dos dados pessoais não constitui um risco relevante para os direitos e liberdades do titular dos dados.

É recomendável que, após a ciência do evento adverso e havendo risco relevante, a ANPD seja comunicada com a maior brevidade possível, sendo considerado a título indicativo o prazo de 2 (dois) dias úteis, contados da data do conhecimento do incidente.

A comunicação efetuada à ANPD deve ser feita com base no formulário produzido e disponibilizado pela própria entidade, e enviado através dos meios de peticionamento vigentes à época do incidente. O formulário será preenchido pela EQUIPE DE RESPOSTAS A INCIDENTES com o apoio da assessoria jurídica e outros especialistas e com o máximo possível de entendimento do impacto do incidente.

Link do formulário:

- https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis/formulario_cis_anpd1.docx

# Canal de Contato com o Comitê

- **Dúvidas e sugestões sobre o Procedimento de Registro de Não Conformidades:**

E-mail: lgpd@vitapart.com.br

# OBRIGADO!!!

GRUPO VITA

HEMOVITA CAXIAS GRUPO VITA

HEMATOLOGISTAS ASSOCIADOS GRUPO VITA

Clínica de Hemoterapia GRUPO VITA

Hemobanco GRUPO VITA

vita HEMOTERAPIA GRUPO VITA

CTN GRUPO VITA

Centro de Hematologia e Hemoterapia GRUPO VITA

HEMOVITA POA GRUPO VITA

Instituto Pasquini GRUPO VITA

UHHS Hemoterapia e Hematologia GRUPO VITA

Procélula TERAPIA CELULAR GRUPO VITA

GRUPO VITA

vita SÃO PAULO GRUPO VITA

vitabahia GRUPO VITA