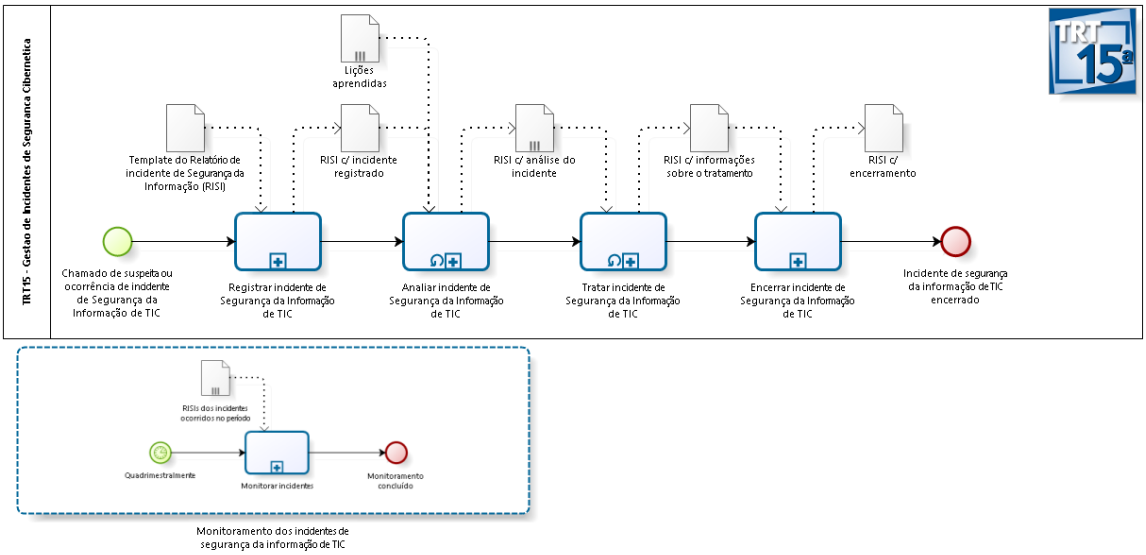
TRT15-Gestão de Incidentes de Segurança Cibernética

Índice

1 FLUXO GERAL



Versão: 1.1

1.1 PROCESSO PRINCIPAL

1.1.1 ELEMENTOS DO PROCESSO

1.1.1.1 Monitoramento dos incidentes de segurança da informação de TIC

Ver detalhes

1.2 TRT15 - GESTAO DE INCIDENTES DE SEGURANCA CIBERNETICA

1.2.1 ELEMENTOS DO PROCESSO

1.2.1.1 Lições aprendidas

Descrição

Conjunto de informações relevantes sobre a gestão de outros incidentes de segurança da informação de TIC

1.2.1.2 Template do Relatório de incidente de Segurança da Informação (RISI)

Descrição

Modelo de documento para registro de todo o clico de vida da gestão de um incidente de segurança da informação de TIC

Presentation Action

https://docs.google.com/spreadsheets/d/1z-n5L6f-ZX8WD4N-4-giOHCVP_zQ3ybSHKEpbT3utB4/edit#gid=0

1.2.1.3 RISI c/ incidente registrado

Descrição

Documento RISI preenchido com as informações preliminares sobre o incidente

1.2.1.4 RISI c/ análise do incidente

Descrição

Documento RISI preenchido com as informações de detalhamento do incidente e as ações de tratamento

1.2.1.5 RISI c/ informações sobre o tratamento

Descrição

Documento RISI preenchido com as informações relativas à aplicação das ações de tratamento do incidente

1.2.1.6 RISI c/ encerramento

Descrição

Documento RISI preenchido com formalização de encerramento do incidente

1.2.1.7 Registrar incidente de Segurança da Informação de TIC

Descrição

Objetivo

Formalizar em documento próprio o comunicado da ocorrência ou suspeita de um incidente de segurança da informação de TIC, a fim de iniciar o ciclo de vida da Gestão do incidente.

Processo

Registrar incidente de SI-TIC - Registrar incidente de SI-TIC

1.2.1.8  Analiar incidente de Segurança da Informação de TIC

Descrição

Objetivo

Proceder com uma investigação técnica detalhada sobre o incidente, permitindo compreendê-lo e, por fim, definir medidas saneadoras para tratá-lo

Tipo de loop

Padrão

Máximo ciclo

0

Tempo de teste

Depois

Processo

Analisar incidente de SI-TIC - Analisar incidente de SI-TIC

1.2.1.9  Tratar incidente de Segurança da Informação de TIC

Descrição

Objetivo

Aplicar esforços para implantar as medidas saneadoras/ações elencadas na fase anterior, com o intuito de tratar o incidente de segurança.

Tipo de loop

Padrão

Máximo ciclo

0

Tempo de teste

Depois

Processo

Tratar incidente de Segurança da Informação de TIC - TRT15 - Tratar incidente de Segurança da Informação de TIC

1.2.1.10  Chamado de suspeita ou ocorrência de incidente de Segurança da Informação de TIC

Descrição
Qualquer usuário do TRT15 pode abrir chamado na Central de Serviços

1.2.1.11  Incidente de segurança da informação de TIC encerrado

1.2.1.12  Encerrar incidente de Segurança da Informação de TIC

Descrição

Objetivo

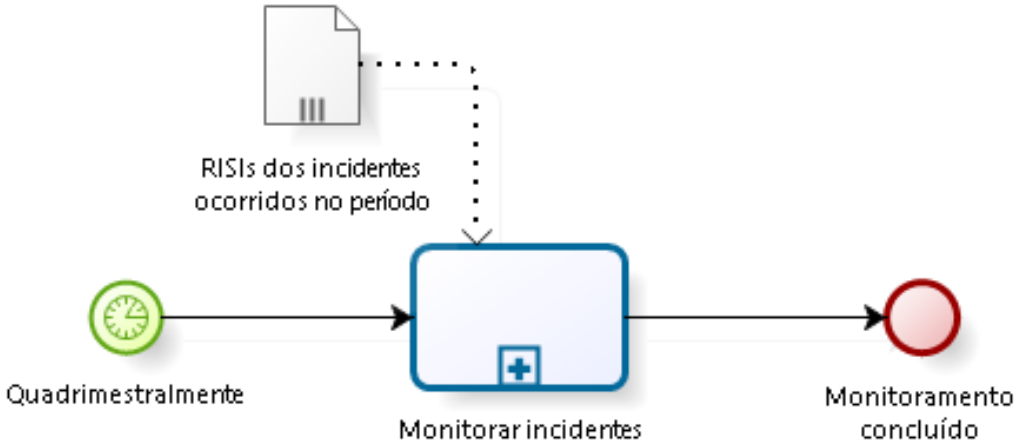
Formalizar e documentar o encerramento do incidente de segurança da informação de TIC

Processo

Encerrar incidente de Segurança da Informação de TIC - TRT15 - Encerrar incidente de Segurança da Informação de TIC

1.2.1.13 

1.3 MONITORAMENTO DOS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO DE TIC



1.3.1 ELEMENTOS DO PROCESSO

1.3.1.1 RISIs dos incidentes ocorridos no período

Descrição

"Relatórios de incidentes de segurança da informação" gerados

1.3.1.2 Quadrimestralmente

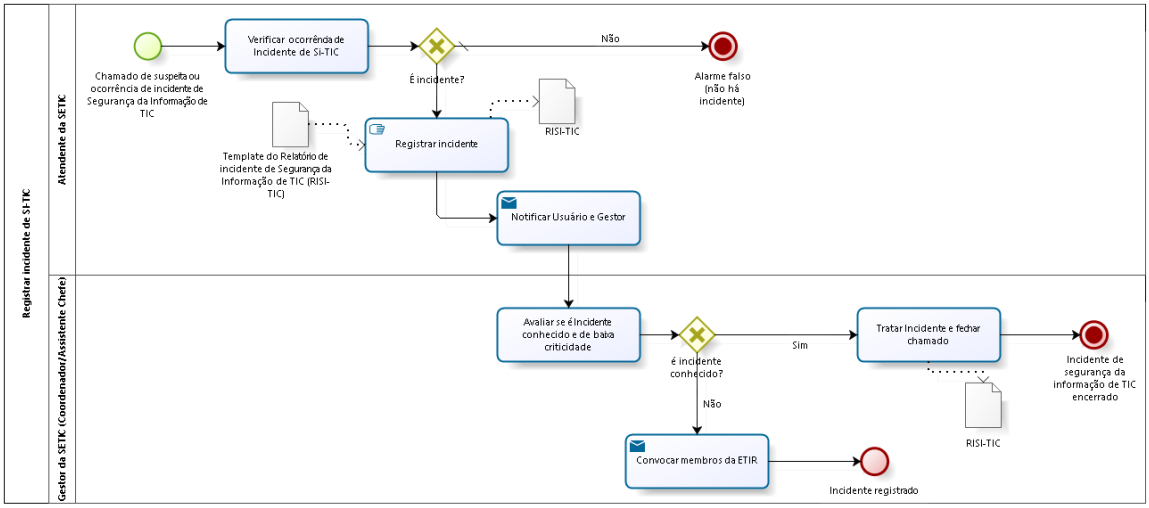
1.3.1.3 Monitorar incidentes

Processo

Monitorar incidentes - TRT15 - Monitorar incidentes

1.3.1.4  Monitoramento concluído

2 REGISTRAR INCIDENTE DE SI-TIC



Versão: 1.0

Autor: heitorfaria

2.1 REGISTRAR INCIDENTE DE SI-TIC

2.1.1 ELEMENTOS DO PROCESSO

2.1.1.1 RISI-TIC

Descrição

Documento RISI preenchido com as informações preliminares sobre o incidente

2.1.1.2 Template do Relatório de incidente de Segurança da Informação de TIC (RISI-TIC)

Descrição

Modelo de documento para registro de todo o clico de vida da gestão de um incidente de segurança da informação de TIC

2.1.1.3 RISI-TIC

2.1.1.4 Chamado de suspeita ou ocorrência de incidente de Segurança da Informação de TIC

Descrição

Qualquer usuário do TRT15 pode abrir chamado na Central de Serviços

2.1.1.5 Incidente registrado

2.1.1.6 Registrar incidente

Descrição

Objetivo

Identificado a ocorrência de incidente, o atendente da SETIC registra o RISI-TIC (Relatório de Incidente de de Segurança da Informação de TIC).

2.1.1.7  Verificar ocorrência de Incidente de Si-TIC

Descrição

Objetivo

Recebida uma suspeita ou ocorrência de incidente Cibernética, de SI-TIC, o atendente faz um primeiro filtro se há realmente um incidente. Por exemplo, um e-mail suspeito pode ser avaliado como oficial ou realmente suspeito.

2.1.1.8  É incidente?

Portões

Registrar incidente

Não

Tipo de Condição

Padrão

2.1.1.9  Alarme falso (não há incidente)

2.1.1.10  Notificar Usuário e Gestor

Descrição

Objetivo

Notificar o respectivo Gestor para iniciar o tratamento do incidente.

Deve-se notificar o usuário também, avisando que o incidente está sendo tratado. Esta notificação pode ser automática ou manual, de acordo com característica do chamado.

Implementação

Serviço Web

2.1.1.11  Avaliar se é Incidente conhecido e de baixa criticidade

Descrição

Objetivo

Avaliar impacto do Incidente, de forma a convocar ou não a ETIR. Há incidentes que são conhecidos e de baixo impacto, sendo resolvidos sem necessidade de acionamento da ETIR.

2.1.1.12  é incidente conhecido?

Portões

Sim

Não

2.1.1.13  Tratar Incidente e fechar chamado

Descrição

Objetivo

Tratar o incidente conhecido e registrar no RISI-TIC (Relatório de Incidente de de Segurança da Informação de TIC) sua resolução.

2.1.1.14  Incidente de segurança da informação de TIC encerrado

2.1.1.15  Convocar membros da ETIR

Descrição

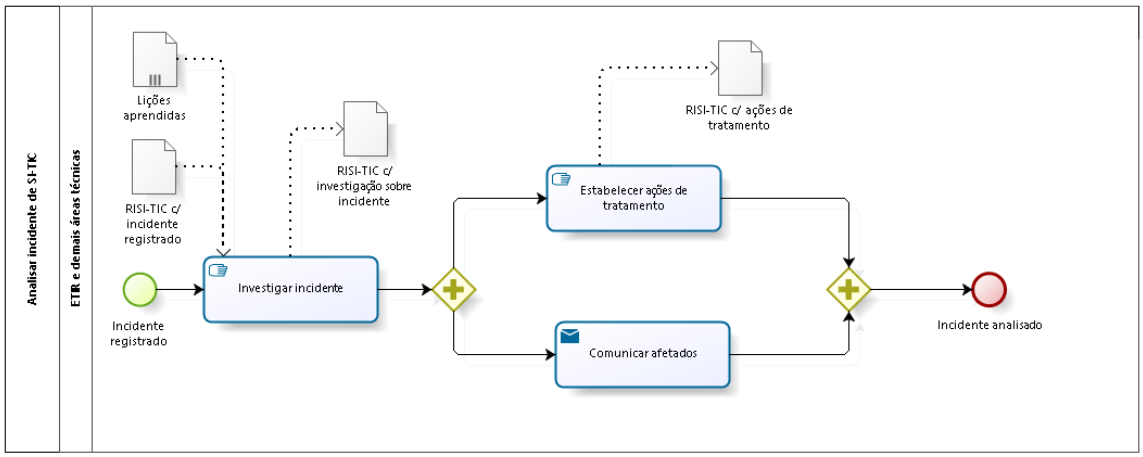
Objetivo

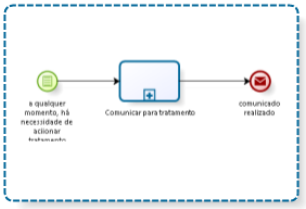
Convocar a ETIR, notificando quem for necessário.

Implementação

Serviço Web

3 ANALISAR INCIDENTE DE SI-TIC





Comunicar para tratamentos específicos

Versão: 1.0

Autor: heitorfaria

3.1 PROCESSO PRINCIPAL

3.1.1 ELEMENTOS DO PROCESSO

3.1.1.1 Comunicar para tratamentos específicos

Ver detalhes

3.2 ANALISAR INCIDENTE DE SI-TIC

3.2.1 ELEMENTOS DO PROCESSO

3.2.1.1 RISI-TIC c/

3.2.1.2 ações de tratamento

Descrição

Documento RISI preenchido com as ações de tratamento

3.2.1.3 Lições aprendidas

Descrição

Conjunto de informações relevantes sobre a gestão de outros incidentes de segurança da informação de TIC

3.2.1.4 RISI-TIC c/ incidente registrado

Descrição

Documento RISI preenchido com as informações preliminares sobre o incidente

3.2.1.5 RISI-TIC c/ investigação sobre incidente

Descrição

Documento RISI preenchido com as informações de detalhamento do incidente

3.2.1.6 Incidente registrado

3.2.1.7 Gateway

3.2.1.8 Gateway

3.2.1.9 Incidente analisado

3.2.1.10 Investigar incidente

Descrição

Objetivo

Investigar as possíveis causas, extensão e impacto do incidente, a fim de subsidiar as decisões e ações para sua contenção ou para seu encaminhamento. Essas informações serão registradadas no respectivo RISI do incidente.

3.2.1.11 Estabelecer ações de tratamento

Descrição

Objetivo

Propor ações para tratar o incidente, com base nas informações levantadas na fase de investigação. Tais ações devem ser registradas no respectivo RISI do incidente.

3.2.1.12  Comunicar afetados

Descrição

Objetivo

Comunicar àqueles (pessoas, áreas) eventualmente afetados pelo incidente sobre a sua ocorrência.

O usuário do chamado também deve ser notificado neste momento.

Detalhamento

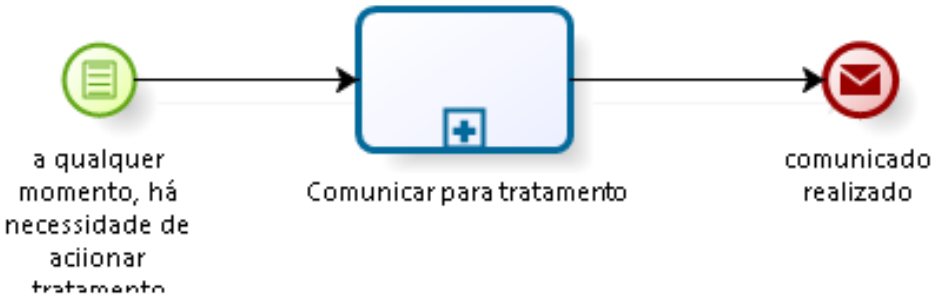
Pode ser necessário solicitar alguma autorização para o tratamento, devendo, para isso, utilizar o fluxo "Acionar Gerenciamento de Crises Cibernéticas" ou "Acionar Investigação para Ilícitos Cibernéticos"ou "Acionar Tratamento de Dados (LGPD)".

Implementação

Serviço Web

3.2.1.13  ETIR e demais áreas técnicas

3.3 COMUNICAR PARA TRATAMENTOS ESPECÍFICOS



Powered by bizagi Modeler

3.3.1 ELEMENTOS DO PROCESSO

3.3.1.1 a qualquer momento, há necessidade de aciionar tratamento

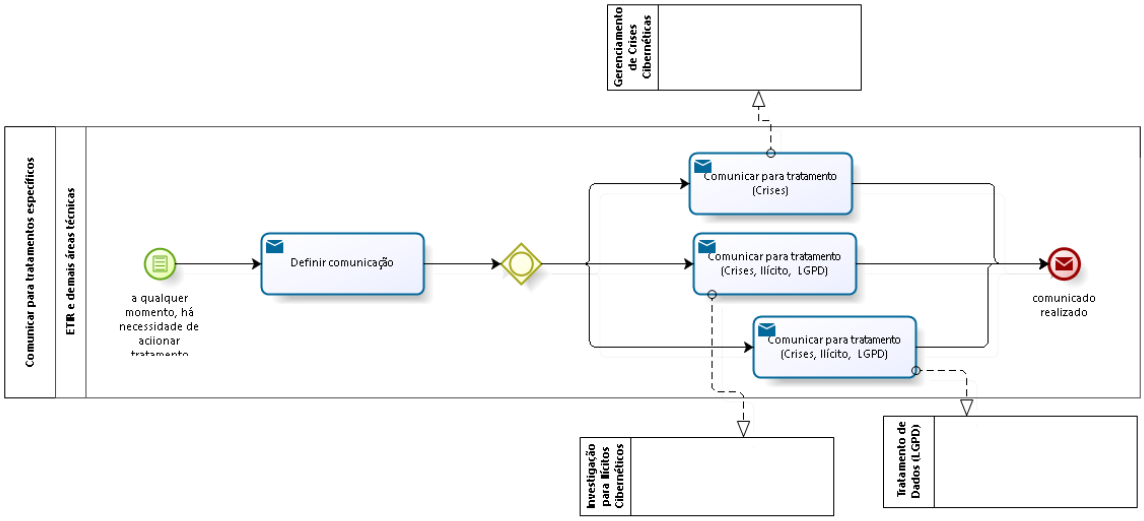
3.3.1.2 comunicado realizado

3.3.1.3 Comunicar para tratamento

Processo

Comunicar para tratamentos específicos - Comunicar para tratamentos específicos

4 COMUNICAR PARA TRATAMENTOS ESPECÍFICOS



Versão: 1.0

Autor: wagne

4.1 COMUNICAR PARA TRATAMENTOS ESPECÍFICOS

4.1.1 ELEMENTOS DO PROCESSO

4.1.1.1  a qualquer momento, há necessidade de aciionar tratamento

4.1.1.2  comunicado realizado

4.1.1.3  Definir comunicação

Implementação

Serviço Web

4.1.1.4  Gateway

Portões

Comunicar para tratamento (Crises)

Comunicar para tratamento (Crises, Ilícito, LGPD)

Comunicar para tratamento (Crises, Ilícito, LGPD)

4.1.1.5  Comunicar para tratamento (Crises)

Implementação

Serviço Web

4.1.1.6  Comunicar para tratamento (Crises, Ilícito, LGPD)

Implementação

Serviço Web

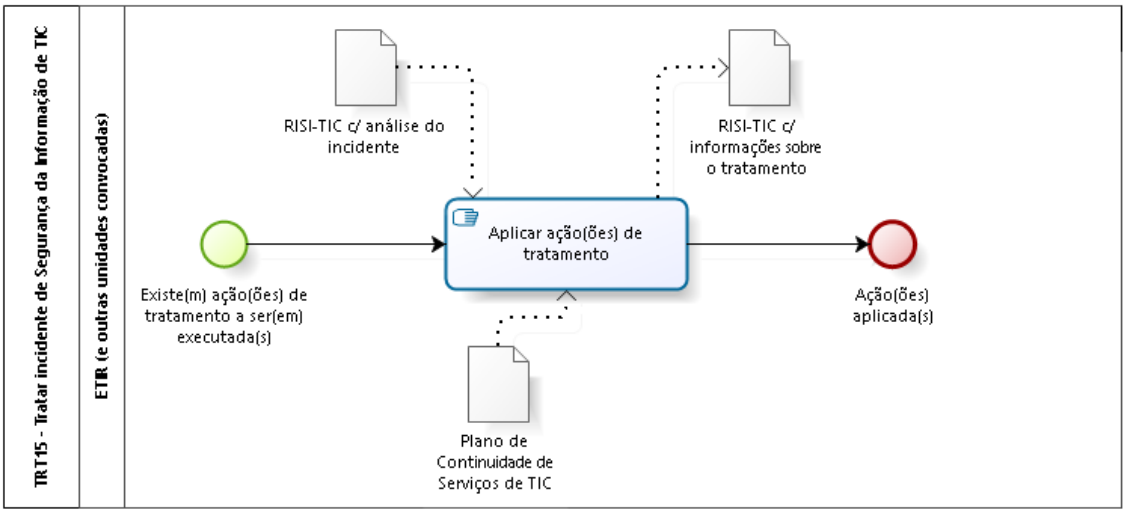
4.1.1.7  Comunicar para tratamento (Crises, Ilícito, LGPD)

Implementação

Serviço Web

4.1.1.8  ETIR e demais áreas técnicas

5 TRATAR INCIDENTE DE SEGURANÇA DA INFORMAÇÃO DE TIC



Versão: 1.0

Autor: heitorfaria

5.1 TRT15 - TRATAR INCIDENTE DE SEGURANÇA DA INFORMAÇÃO DE TIC

5.1.1 ELEMENTOS DO PROCESSO

5.1.1.1 RISI-TIC c/ análise do incidente

Descrição

Documento RISI preenchido com as informações de detalhamento do incidente e as ações de tratamento

5.1.1.2 RISI-TIC c/ informações sobre o tratamento

Descrição

Documento RISI preenchido com as informações relativas à aplicação das ações de tratamento do incidente

5.1.1.3 Plano de Continuidade de Serviços de TIC

5.1.1.4 Existe(m) ação(ões) de tratamento a ser(em) executada(s)

5.1.1.5 Ação(ões) aplicada(s)

5.1.1.6 Aplicar ação(ões) de tratamento

Descrição

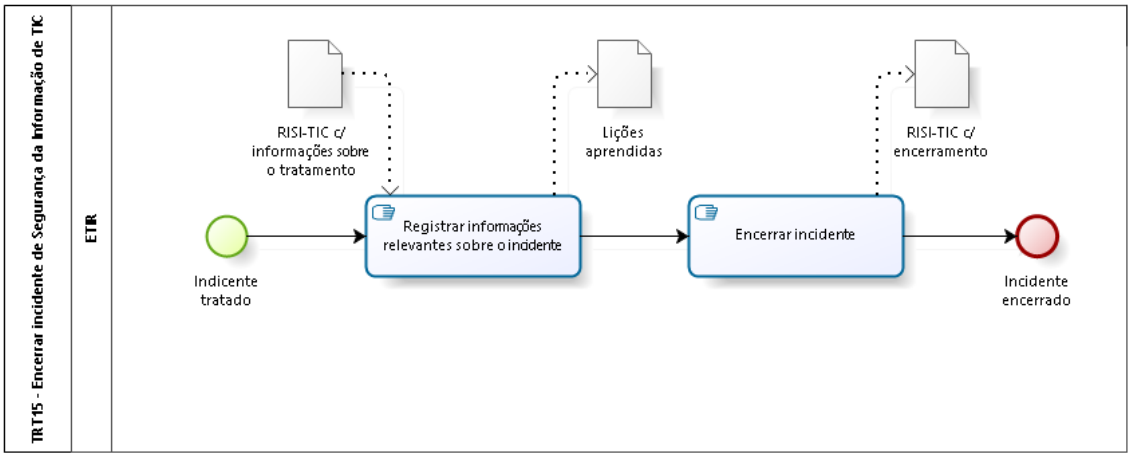
Objetivo

Implantar as ações de tratamento do respectivo incidente.

Neste momento é feito a preservação de evidências para investigar a causa raiz do incidente.

5.1.1.7 ETIR (e outras unidades convocadas)

6 ENCERRAR INCIDENTE DE SEGURANÇA DA INFORMAÇÃO DE TIC



Versão: 1.0

Autor: heitorfaria

6.1 TRT15 - ENCERRAR INCIDENTE DE SEGURANÇA DA INFORMAÇÃO DE TIC

6.1.1 ELEMENTOS DO PROCESSO

6.1.1.1  Lições aprendidas

Descrição

Conjunto de informações relevantes sobre a gestão deste incidente de segurança da informação de TIC

6.1.1.2  RISI-TIC c/ informações sobre o tratamento

Descrição

Documento RISI preenchido com as informações relativas à aplicação das ações de tratamento do incidente

6.1.1.3  RISI-TIC c/ encerramento

Descrição

Documento RISI preenchido com formalização de encerramento do incidente

6.1.1.4  Indicente tratado

6.1.1.5  Incidente encerrado

6.1.1.6  Registrar informações relevantes sobre o incidente

Descrição

Objetivo

Coletar os acontecimentos, experiências, percepções, etc, mais relavantes que se deram ao longo da Gestão do incidente de segurança da informação de TIC, para subsidiar outras necessidades futuras

6.1.1.7  Encerrar incidente

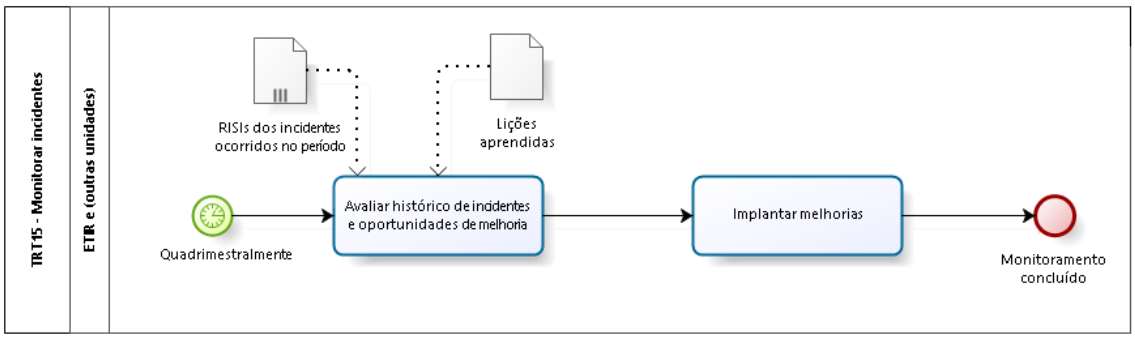
Descrição

Objetivo

Verificar a existência de providências pendentes e providenciar sua execução. Além disso, deve-se registrar as informações pertinentes para o encerramento formal do incidente.

6.1.1.8  ETIR

7 MONITORAR INCIDENTES



Versão: 1.0

Autor: heitorfaria

7.1 TRT15 - MONITORAR INCIDENTES

7.1.1 ELEMENTOS DO PROCESSO

7.1.1.1 RISIs dos incidentes ocorridos no período

Descrição

"Relatórios de incidentes de segurança da informação" gerados

7.1.1.2 Quadrimestralmente

7.1.1.3 Avaliar histórico de incidentes e oportunidades de melhoria

Descrição

Objetivo

Analisar o histórico de incidentes, com o intuito de estudar o cenário de forma mais abrangente, a fim de identificar oportunidades de melhoria, bem como serviços reiteradamente afetados por incidentes

7.1.1.4 Implantar melhorias

Descrição

Objetivo

Identificadas eventuais melhorias, essa atividade se encarrega de implantá-las.

7.1.1.5 Monitoramento concluído

7.1.1.6 Lições aprendidas

Descrição

Conjunto de informações relevantes sobre a gestão deste incidente de segurança da informação de TIC

7.1.1.7 ETIR e (outras unidades)