GISA

Gerenciamento de Incidentes de Segurança e Ativos

GER-0003

Gerente de Incidente	Guilherme Bezerra
Técnicos RSTI	Camilla Nogueira e Fabrício Leão

Ministério Público do Estado do Tocantins
Departamento de Modernização de TI
Área de Redes, Telecomunicações e Segurança da Informação

Para verificar a autenticidade, acesse o site do MPE/TO e use a chave: dbe8a0d6 - e1e5bef6 - 683fa76d - ccf75f7b

HISTÓRICO DE REVISÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
29/01/2018	1.0	Elaboração do documento.	Diego Silva
26/07/2018	1.1	Revisão	Diego Silva
03/06/2019	1.2	Inclusão da CPSI no fluxo do processo de incidente de segurança, item 6 e 7.2.	Diego Silva

Para verificar a autenticidade, acesse o site do MPE/TO e use a chave: dbe8a0d6 - e1e5bef6 - 683fa76d - ccf75f7b

Sumário

Para verificar a autenticidade, acesse o site do MPE/TO e use a chave: dbe8a0d6 - e1e5bef6 - 683fa76d - ccf75f7b

1. INTRODUÇÃO

Considerando as recomendações da resolução nº 171/2017 do CNMP que institui o Plano Nacional de Tecnologia da Informação (PNTI-MP), a seção VIII no art. 27 aponta dentre outras importantes gestões, a necessidade da área de Segurança da Informação regulamentar o controle efetivo dos incidentes de segurança nos ativos de TI.

Este documento descreve as diretrizes e políticas que envolvem o fluxo no tratamento dos incidentes de segurança, bem como dos ativos de infraestrutura.

2. OBJETIVO

Este documento tem por objetivo estabelecer o processo de Gerenciamento de Incidentes no Ministério Público de Estado de Tocantins e garantir controles efetivos de monitoramento, identificação e registros dos incidentes de segurança e ativos de infraestrutura de modo a mitigar os impactos no negócio.

3. ESCOPO

O Gerenciamento de Incidentes deve ser entendido por todas as áreas do DMTI e abrange o controle dos eventos de incidentes reportados por usuários ou sistema de monitoramento. Os tipos de incidentes estão descritos no Catálogo de Serviços do RTSI e limitam-se a:

3.1 Incidentes de Segurança

Segurança

- Erro humano;
- Mudanças descontroladas de sistemas;
- Não-Conformidade com a Política de Segurança e Diretrizes;
- Propagação de Virus/Malware;
- Violação da Disponibilidade, Confidencialidade e/ou Integridade da Informação;
- Violação de acesso.

Para verificar a autenticidade, acesse o site do MPE/TO e use a chave: dbe8a0d6 - e1e5bef6 - 683fa76d - ccf75f7b

3.2 Incidentes Ativos de Infraestrutura

Rede/Internet

- Falha/erro de equipamento de rede;
- Indisponibilidade de serviço e/ou sistema;
- Problemas com link/equipamento de Internet.

Os incidentes são tratados de forma diferenciada das requisições habituais de um usuário do MPTO, sendo registradas por áreas distintas. As requisições recebem tratamento pela Central de Serviço e os incidentes pelas Área de Rede de Dados e Segurança da Informação.

4. DEFINIÇÕES E ABREVIAÇÕES

Termo	Definição
DMTI	Departamento de Modernização da Tecnologia da Informação.
Incidente	Qualquer evento que causa uma interrupção ou redução na qualidade do serviço.
ITSM	Gerenciamento de Serviços de TI
NIS	Núcleo de Inteligência e Segurança Institucional.
RTSI	Área de Rede de Dados e Segurança da Informação.

5. DIRETRIZES E POLITICAS

O Gerenciamento de Incidentes deve estar alinhado às diretrizes e políticas descritas a seguir:

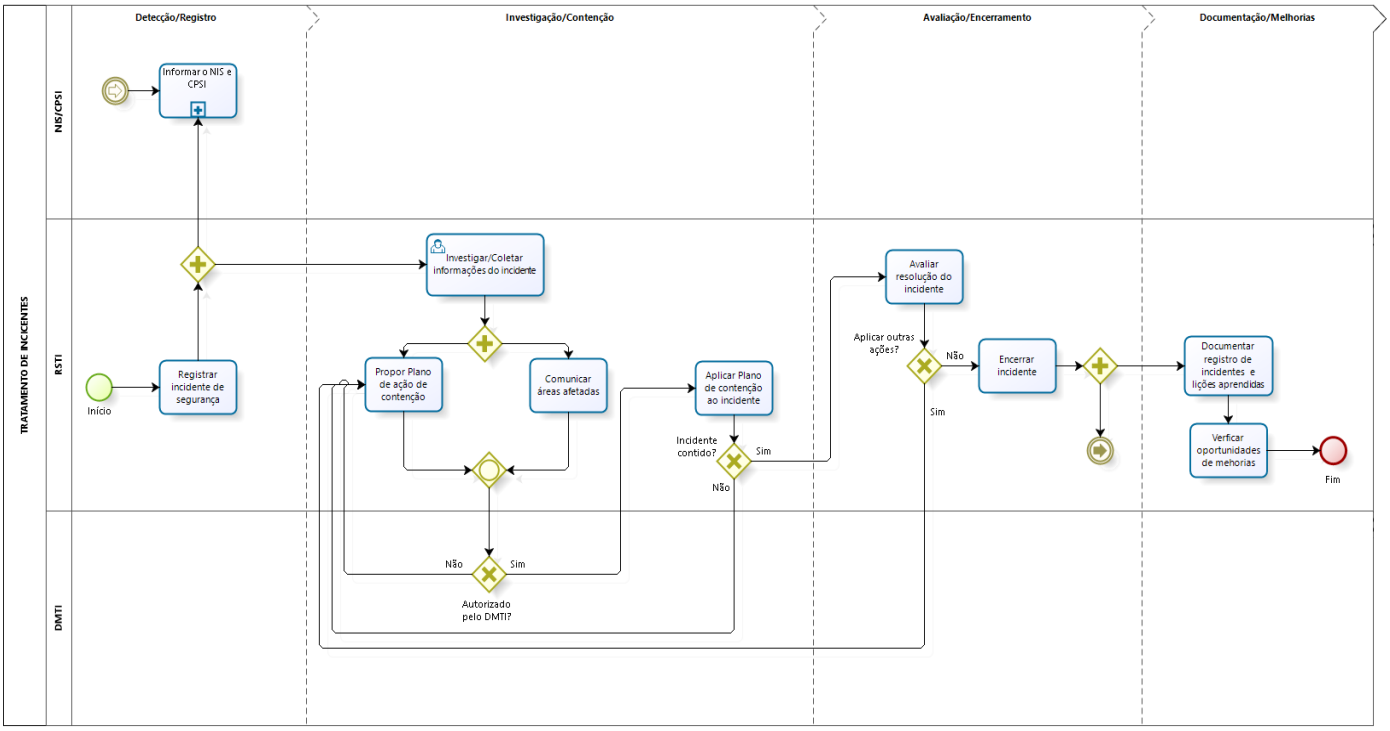
- Registrar todos os incidentes reportados por telefone, monitoramento ou e-mail;
- Comunicar áreas/pessoas afetadas;
- A Área de Rede de Dados e Segurança da Informação deve documentar soluções ou atualizar as existentes caso necessário, mantendo a base de conhecimento;
- Registrar oportunidades de melhorias e informar ao Gerente de Incidente.
- No caso de incidente de segurança, preencher Formulário de Registro de Incidente de Segurança e anexar ao registro de encerramento.

Para verificar a autenticidade, acesse o site do MPE/TO e use a chave: dbe8a0d6 - e1e5bef6 - 683fa76d - ccf75f7b

Acesso ao formulário:
smb://10.113.1.241/rtsi/Restrito/Documentação/Temporario/Formulários

6. FLUXO INCIDENTE DE SEGURANÇA

O fluxo abaixo mostra como funciona o processo de Gerenciamento de Incidentes de Segurança:



7. ATIVIDADES DO PROCESSO INCIDENTE DE SEGURANÇA

7.1. Registrar incidente de segurança

Os eventos de incidentes de segurança reportados pelos usuários ou ferramenta de monitoramento devem ser registrados no ITSM pelo técnico do RTSI. As informações pertinentes ao andamento ou encerramento devem ser registradas de forma detalhada para resguardar quaisquer situações adversas e gerar histórico completo e minucioso do ciclo de vida do incidente.

Para verificar a autenticidade, acesse o site do MPE/TO e use a chave: dbe8a0d6 - e1e5bef6 - 683fa76d - ccf75f7b

7.2. Informar ao NIS e CPSI

De acordo com definições de escopo estabelecidas entres as áreas DMTI, NIS e CPSI, os incidentes de segurança devem ser informados ao Núcleo de Inteligência e Segurança Institucional e Comitê de Políticas de Segurança Institucional. As ações ocorrerão seguindo as politicas internas de investigação.

O fluxo mostra que paralelamente ocorre a tratativa dos incidentes nos níveis de atuação do RTSI, como: coleta de informações, plano de ação, contenção e avaliação.

7.3. Investigar/Coletar informações

Durante esta atividade, o técnico deve analisar todas as informações relevantes que apoiem na investigação a fim de reproduzir diagnostico preciso. Vários meios e fontes podem ser exploradas pelo técnico:

- Base de conhecimento ou documentação existente;
- Fontes externas e/ou documentos técnicos;
- Outras áreas do DMTI;
- Ferramentas de monitoramento;
- Logs e reports;
- Fornecedores e parceiros.

7.4. Propor plano de ação

O impacto é classificado de acordo com o nível de interrupção ou redução das atividades do negócio em um departamento, serviço ou pessoa. Independente da abrangência do impacto, uma equipe de resposta ao incidente de segurança deve ser constituída a fim de agregar ações conjuntas na contenção e/ou solução dos incidentes. A equipe pode ser formada por:

- Analista/técnicas do DMTI;
- Fornecedores e parceiros;
- Especialistas de outros órgãos.

Para verificar a autenticidade, acesse o site do MPE/TO e use a chave: dbe8a0d6 - e1e5bef6 - 683fa76d - ccf75f7b

7.5. Comunicar áreas afetadas

As áreas afetadas devem ser comunicadas sobre o estado do incidente, deve-se registrar todos os contatos realizados no ITSM, gerando histórico da comunicação. Desta forma resguarda-se quaisquer situações adversas.

7.6. Autorização DMTI

Considerando o ambiente do MPTO e sua estrutura organizacional bem definida, todas as ocorrências de incidentes de segurança que impactam nas atividades da área-fim, devem ser reportadas a chefia do DMTI, assim também os planos de contenção.

Nesta etapa o plano apresentado será previamente analisado e toma-se a decisão de aplicá-lo como medida de contenção adequada ao negócio. Em caso de não autorizado, apresenta-se um novo plano à chefia até alcançar o desejado.

7.7. Aplicar plano de contenção

O técnico deve atuar conforme descrito no plano de contenção e seguir rigorosamente todos os passos descritos. Depois registrar todas as ações no ITSM.

7.8. Avaliar resolução

Deve-se avaliar com as áreas afetadas a efetividade da solução aplicada e se realmente o resultado esperado foi alcançado trazendo a normalidade ao ambiente.

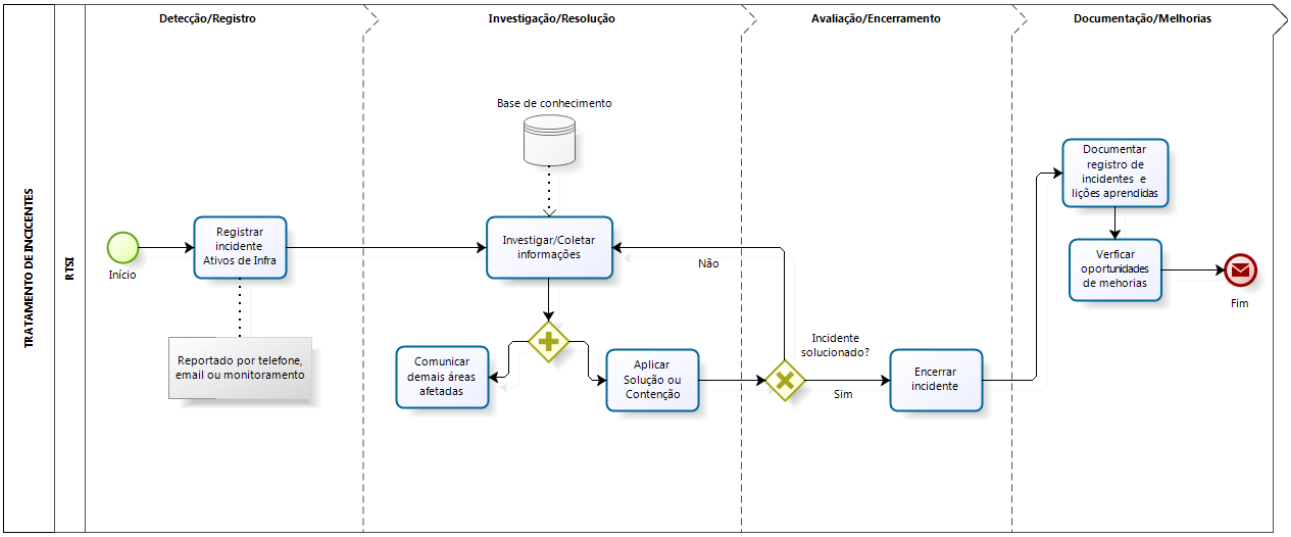
7.9. Encerrar incidente

O técnico deve encerrar o incidente com a anuência das áreas afetadas resguardando o registro de todos os contatos realizados.

Para verificar a autenticidade, acesse o site do MPE/TO e use a chave: dbe8a0d6 - e1e5bef6 - 683fa76d - ccf75f7b

8. FLUXO ATIVOS DE INFRAESTRUTURA

O fluxo abaixo mostra como funciona o processo de Gerenciamento de Incidentes de Ativos de Infraestrutura:



9. ATIVIDADES DO PROCESSO ATIVOS DE INFRAESTRUTURA

9.1. Registrar incidente Ativos de Infraestrutura

Os eventos de incidentes em ativos de Infraestrutura reportados por usuários ou ferramenta de monitoramento devem ser registrados no ITSM pelo técnico do RTSI. As informações pertinentes ao andamento ou encerramento devem ser registradas de forma detalhada para resguardar quaisquer situações adversas e gerar histórico completo e minucioso do ciclo de vida do chamado.

9.2. Investigar/Coletar informações

Durante esta atividade, o técnico deve analisar todas as informações relevantes que apoiem na investigação a fim de reproduzir diagnostico preciso. Vários meios e fontes podem ser exploradas pelo técnico:

Para verificar a autenticidade, acesse o site do MPE/TO e use a chave: dbe8a0d6 - e1e5bef6 - 683fa76d - ccf75f7b

- Base de conhecimento ou documentação existente;
- Fontes externas e/ou documentos técnicos;
- Ferramentas de monitoramento;
- Logs e reports;
- Fornecedor e parceiros.

9.3. Comunicar áreas afetadas

As áreas afetadas devem ser comunicadas sobre o estado do incidente, deve-se registrar todos os contatos realizados no sistema de chamado, gerando histórico da comunicação. Desta forma resguarda-se quaisquer situações adversas.

9.4. Aplicar Solução ou Contenção

O técnico deve atuar na resolução do incidente conforme soluções descritas na base de conhecimento ou outra fonte segura que descreva a solução. Vale ressaltar a importância de documentar, atualizar e registrar todas as etapas aplicadas na contenção dos incidentes.

9.5. Encerrar incidente

O técnico deve encerrar o incidente com a anuência das áreas afetadas resguardando o registro de todos os contatos realizados.

10. EVOLUÇÃO E CONTINUIDADE

10.1 Do Processo

Este documento deve refletir o funcionamento do processo de Gerenciamento de Incidentes no RTSI e ser mantido revisado periodicamente. As situações seguintes devem representar gatilhos para revisão do processo:

- Decisões estabelecidas em reuniões de melhorias e ajustes do processo;
- Determinação do Gerente de Incidente.

Para verificar a autenticidade, acesse o site do MPE/TO e use a chave: dbe8a0d6 - e1e5bef6 - 683fa76d - ccf75f7b

11. FUNÇÕES E RESPONSABILIDADES

Os papéis definidos neste processo tem como base a ITIL e adaptados a realidade da organização:

Função	Responsabilidade
Gerente de Incidente	• Buscar a eficiência e eficácia dos processos; • Produzir informações gerenciais, como relatórios de atendimento e de tipos de incidentes; • Gerenciar o trabalho da equipe de solução de incidentes; • Desenvolver e manter processos e procedimentos.
Técnicos RTSI	• Registrar Incidentes; • Atualizar e adicionar informações na base de conhecimento; • Solucionar incidentes ou definir contenção; • Estabelecer contato com as áreas afetadas.

12. SUGESTÕES E MELHORIAS IDENTIFICADAS

- Definir e incluir Acordo de Nível de Serviço (ANS).

13. REFERÊNCIAS

- Resolução no 171, de 27 de junho de 2017 http://www.cnmp.mp.br/portal/images/Resolucoes/Resolu%C3%A7%C3%A3o-171.pdf;
- Resolução 156, de 13 de dezembro de 2016 http://www.cnmp.mp.br/portal/images/Normas/Resolucoes/RESOLUO_156.pdf;
- ABNT NBR ISO/IEC 27002;
- ITIL v3 – Fundamentos.

Para verificar a autenticidade, acesse o site do MPE/TO e use a chave: dbe8a0d6 - e1e5bef6 - 683fa76d - ccf75f7b