	Título	Código
	<b>METODOLOGIA DE RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO</b>	<b>EMAP-PC-73</b>
		Versão
		<b>2</b>
	Data	<b>18/09/2020</b>

Elaborado Por	Aprovado por
Ruan Louzeiro Santos	Thiago Drummond

## ÍNDICE

<b>1.0 OBJETIVO.....</b>	<b>1</b>
<b>2.0 DOCUMENTOS DE REFERÊNCIA.....</b>	<b>2</b>
<b>3.0 DEFINIÇÕES.....</b>	<b>2</b>
<b>4.0 RESPONSABILIDADES .....</b>	<b>4</b>
<b>5.0 DESCRIÇÃO DO PROCEDIMENTO.....</b>	<b>6</b>
<b>6.0 CATÁLOGO DE SERVIÇOS.....</b>	<b>10</b>
<b>7.0 ANEXOS.....</b>	<b>10</b>
<b>8.0 REGISTROS.....</b>	<b>11</b>
<b>9.0 HISTORICO DE REVISÃO .....</b>	<b>11</b>

### 1.0 OBJETIVO

O Gerenciamento de Incidentes, conforme descrito pela ITIL, é o processo cujo propósito é restaurar a operação normal do serviço o mais rápido possível de modo a minimizar o impacto adverso nas operações de negócio, garantindo que os níveis acordados de qualidade do serviço sejam mantidos. A operação normal do serviço é definida como a operação de serviço dentro dos limites estabelecidos no SLA (Acordo de Nível de Serviço). Com isso, o gerenciamento de incidentes visa contribuir para melhorar a satisfação dos usuários com a qualidade dos serviços de TI.

O Gerenciamento de Incidentes deve estar alinhado às seguintes políticas e diretrizes:

- Todos os incidentes devem ser registrados, inclusive os incidentes reportados por telefone;
- Toda informação relevante durante o ciclo de vida do incidente deve ser registrada;
- Os incidentes e seu estado devem ser comunicados ao usuário.

- A Equipe de Suporte deve solicitar mais informações do usuário quando o chamado não dispuser de informação suficiente para o atendimento.
- Os chamados devem ser categorizados e priorizados pela Equipe de Suporte, dentro do prazo acordado.
- Incidentes devem ser resolvidos na Equipe de Suporte somente quando existir uma solução documentada.
- O banco de dados de erros conhecidos deve ser atualizado constantemente.
- Ações corretivas, preventivas e oportunidade de melhorias no processo devem ser registradas e encaminhadas ao dono do processo.

## 2.0 DOCUMENTOS DE REFERÊNCIA

- ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação
- ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação
- ITIL V3 Library – Edição 2011 - Service Operation
- ITIL V3 Library – Edição 2011 - Service Transition
- ITIL V3 Library – Edição 2011 - Service Improvement
- ITIL V3 Library – Edição 2011 - Service Design
- ITIL V3 Library – Edição 2011 - Service Strategy
- Glossário ITIL® de Português do Brasil, v1.0, 29 de julho de 2011
- Decreto nº 9.637 de 26 e dezembro de 2018
- Instrução Normativa GSI nº 1 de 13 de junho de 2008
- Norma Complementar nº 02/IN01/DSIC/GSIPR
- Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo
- Norma Complementar nº 08/IN01/DSIC/GSIPR
- Norma Complementar nº 13/IN01/DSIC/GSIPR

## 3.0 DEFINIÇÕES

- **Central de Serviços:** A Central de Serviços serve como ponto único de contato para os usuários de TI e restaurar a operação normal dos serviços com o mínimo de impacto nos negócios do cliente. (FREITAS, 2010, p. 290). Conhecida também como Service Desk, tem como função, de acordo com a ITIL, “Restabelecer os serviços a sua operação normal o mais rapidamente possível, seja instalando, configurando ou removendo itens de hardware e software”. E atendendo às solicitações de serviços.



**Figura 1:** Ilustração de funcionamento da Central de Serviço.

- **Incidente:** Uma interrupção não planejada ou uma redução da qualidade de um serviço de TI.
- **Gerenciamento de Incidentes:** O processo responsável por gerenciar o ciclo de vida de todos os incidentes. O gerenciamento de incidente garante que a operação normal de um serviço seja restaurada tão rapidamente quanto possível e que o impacto no negócio seja minimizado.
- **Operação Normal do Serviço:** A operação de serviço dentro dos limites estabelecidos no SLA (Acordo de Nível de Serviço).
- **Acordo de Nível de Serviço (ANS OU SLA):** Acordo de Nível de Serviço (ANS ou SLA, do inglês Service Level Agreement) é um acordo firmado entre as áreas de negócio e a unidade de TI que descreve as metas de nível de serviço. O acordo que deve equilibrar demandas e ofertas, benefícios e custos entre TI e a área de negócio, com obrigações e direitos de ambas as partes, como a medição da disponibilidade dos serviços e a medição do tempo de atendimento de um chamado.
- **Equipe de Suporte:** O ponto único de contato entre o provedor de serviço e os usuários. Uma central de serviço típica gerencia incidentes, requisições de serviço e também a comunicação com os usuários. A Equipe de Suporte é primeiro nível na hierarquia dos grupos de suporte envolvidos na resolução de incidentes. No contexto da Empresa Maranhense de Administração Portuária.
- **Suporte de 2º nível (ou grupo solucionador de 2º nível):** O segundo nível na hierarquia dos grupos de suporte envolvidos na resolução de incidentes e investigação de problemas. Cada nível contém especialistas com maiores

habilidades, mais tempo disponível ou outros recursos necessários para solução do incidente.

- **Erro conhecido:** Um problema que possui causa raiz e solução de contorno documentadas. Erros conhecidos são criados e gerenciados durante todo o seu ciclo de vida pelo gerenciamento de problema. Erros conhecidos também podem ser identificados pelo desenvolvimento ou fornecedores.
- **Base de conhecimento (BDC):** Um banco de dados que contém todos os registros de erros conhecidos. Este banco de dados é criado pelo gerenciamento de problema e é usado pelo gerenciamento de incidente e pelo próprio gerenciamento de problema.
- **Problema:** A causa raiz de um ou mais incidentes. A causa geralmente não é conhecida no momento em que o registro de problema é criado e o processo do gerenciamento de problema é responsável pela investigação a ser conduzida.
- **Requisição de serviço:** É uma requisição formal de um usuário por algo a ser fornecido, por exemplo, uma requisição de informações ou aconselhamento, solicitações para redefinir uma senha ou para instalar uma estação de trabalho para um novo usuário.
- **Solução de Contorno:** meio de resolver um Incidente, voltando o serviço ao estado normal, sem resolver o problema definitivamente
- **Solução Definitiva:** meio identificado de resolver um Problema por meio de uma Requisição de Mudança para eliminar definitivamente a falha da infraestrutura de TI que causou o problema e seus incidentes.
- **Prioridade:** é definida como a sequência em que os Problemas devem ser tratados, baseada no impacto sobre o negócio e na urgência.

#### 4.0 RESPONSABILIDADES

Os papéis e responsabilidades dos envolvidos no processo de Gerenciamento de Incidentes são definidos conforme a tabela abaixo.

Papel	Responsabilidade
Dono do processo	<ul style="list-style-type: none"><li>• Garantir que o processo esteja adequado aos propósitos da Empresa Maranhense de Administração Portuária e realizar as melhorias necessárias;</li><li>• Garantir que a documentação do processo esteja atualizada e acessível a todos os envolvidos.</li><li>• Garantir que os envolvidos sejam informados das mudanças</li></ul>

Papel	Responsabilidade
	<p>efetuadas no processo;</p> <ul style="list-style-type: none"> <li>• Definir e revisar periodicamente os indicadores de desempenho utilizados para aferir a eficácia e eficiência do processo;</li> <li>• Garantir que relatórios com os indicadores de desempenho sejam produzidos e distribuídos entre os interessados;</li> <li>• Auditar periodicamente o processo para garantir que esteja sendo seguido conforme o especificado;</li> <li>• Garantir que o processo seja automatizado na ferramenta Central de Serviços da GETIN;</li> <li>• Garantir que os envolvidos recebam os treinamentos adequados para a fiel execução do processo;</li> <li>• Garantir a autoridade necessária a todos os papéis do processo.</li> </ul>
Gerente do Processo	<ul style="list-style-type: none"> <li>• Indicar as pessoas adequadas aos papéis definidos no processo;</li> <li>• Promover e garantir que o processo seja seguido conforme o especificado;</li> <li>• Gerenciar os recursos alocados ao processo (pessoal, financeiros, etc.) de forma otimizada;</li> <li>• Medir e analisar criticamente os indicadores de desempenho do processo;</li> <li>• Registrar e informar ao Dono do Processo as sugestões de melhorias no processo e no sistema da Central de Serviços da GETIN;</li> <li>• Garantir que os usuários sejam mantidos informados sobre seus incidentes;</li> <li>• Decidir sobre a alocação de incidentes aos Operadores da Equipe de Suporte que tratam incidentes;</li> <li>• Decidir sobre as escalas hierárquicas de incidentes;</li> <li>• Garantir a inclusão e atualização dos erros conhecidos na base de conhecimento;</li> <li>• Conduzir reuniões periódicas com a equipe da Equipe de Suporte e com as equipes de atendimento do 2º nível;</li> <li>• Auxiliar os operadores na solução de incidentes;</li> </ul>
Operador da Equipe de Suporte	<ul style="list-style-type: none"> <li>• Garantir o registro de todos os incidentes reportados na Central de Serviços da GETIN;</li> <li>• Realizar a categorização dos incidentes no prazo acordado no SLA;</li> <li>• Buscar mais informações do usuário quando o chamado não estiver suficientemente descrito;</li> <li>• Realizar o atendimento dos incidentes cuja solução esteja na base de conhecimento;</li> <li>• Apoiar na atualização dos erros conhecidos na base de conhecimento;</li> </ul>

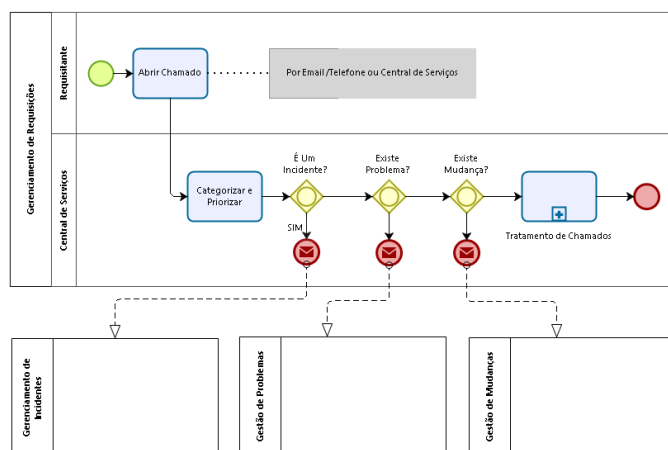
Papel	Responsabilidade
Operador do 2º nível	<ul style="list-style-type: none"> <li>Recategorizar os chamados categorizados de forma equivocada e comunicar os operadores da central sobre o equívoco.</li> <li>Solucionar os incidentes que não possuem solução documentada na base de conhecimento ou que não foram solucionados pela Equipe de Suporte no prazo definido pelo SLA.</li> <li>Atualizar ou adicionar novos registros de erros conhecidos na base de conhecimento.</li> </ul>
Fornecedor Externo	<ul style="list-style-type: none"> <li>Garantir a execução das atividades relacionadas ao contrato existente para resolução de incidentes;</li> <li>Fornecer informações gerenciais e de acompanhamento;</li> </ul>

## 5.0 DESCRIÇÃO DO PROCEDIMENTO

O Gerenciamento de Incidentes é aplicável a todos os serviços que são prestados pela Empresa Maranhense de Administração Portuária e que estão descritos no Catálogo de Serviços de TI.

Incidentes podem ser reportados à Central de Serviços da GETIN pelos usuários, pelo próprio pessoal de TI ou, automaticamente, pelas ferramentas de monitoramento. Alguns exemplos de incidentes são: falta de acesso à Internet, problemas de hardware ou problemas de impressão.

Não faz parte do escopo do gerenciamento de incidentes investigar a causa raiz dos incidentes (isso faz parte do escopo do gerenciamento de problemas). O objetivo do gerenciamento de incidentes é restaurar a operação do serviço o mais rápido possível. Para tanto, deverá utilizar as soluções de contorno disponíveis nas bases de conhecimento da Central de Serviços da GETIN.



**Figura 2:** Abertura de Chamado e Avaliação de Chamados.

## 5.1 ABRIR CHAMADO

- O chamado deve ser registrado pelo usuário (através de e-mail ou do sistema de chamados) ou pela Equipe de Suporte (quando o chamado é aberto por telefone ou quando o próprio operador identifica algum incidente).
- Todos os chamados devem ser registrados no sistema de gerenciamento de chamados, inclusive os chamados provenientes de ligações telefônicas. Além disso, toda nova informação relevante durante o ciclo de vida do chamado, tais como tentativa de contato com usuário, ligações recebidas e atividades realizadas, deve ser registrada no histórico do chamado.

## 5.2 CATEGORIZAR E PRIORIZAR CHAMADO

- Os chamados devem ser categorizados e priorizados pela Equipe de Suporte, dentro do prazo acordado. Categorizar um chamado consiste em definir o tipo do chamado, além de analisar se o chamado é um incidente ou uma requisição normal.
- As requisições (incidente ou não) devem também ser priorizadas, levando em consideração o impacto causado sobre o negócio. Os incidentes que causarem maior impactos nos serviços prestados aos usuários deverão ter maior prioridade. Os incidentes devem ter a prioridade definida como 'Muito Baixa', 'Baixa', 'Média', 'Alta', 'Muito Alta' e 'Crítica'. Incidentes de maior prioridade terão precedência no atendimento.
- Os incidentes que causarem impacto no faturamento e na operação portuária deverão ter a prioridade definida como 'Alta' 'Muito Alta', ou 'Crítica'. Os demais como 'Muito Baixa', 'Baixa' ou 'Média'.
- O sistema poderá ser configurado para alterar a prioridade automaticamente de acordo com a categoria.
- O Gerente do Processo poderá ser consultado a respeito da prioridade caso exista dúvida a respeito do grau da prioridade.
- Caso o chamado não seja um incidente, deverá ser resolvido pelo processo de tratamento de chamados.
- A requisição também deve ser analisada com o objetivo de identificar se o chamado está relacionado a um problema, que será tratado pelo processo de Gestão de Problemas, e se está relacionado a uma Mudança, que será tratada pela Gestão de Mudanças.

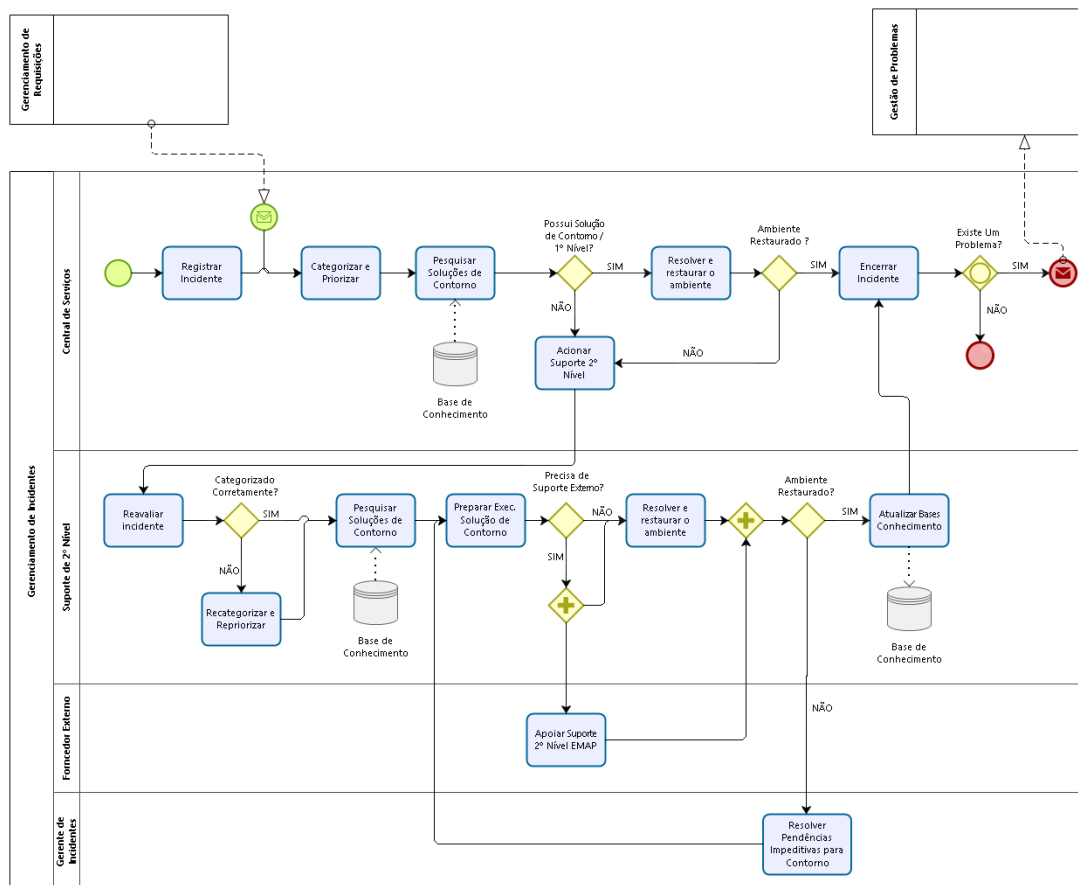


Figura 3: Gerenciamento de Incidentes

### 5.3 REGISTRAR INCIDENTE

- Incidentes podem ser informados à Central de Serviços da GETIN pelos usuários, pelo próprio pessoal de TI ou, automaticamente, pelas ferramentas de monitoramento. Um chamado, ao ser analisado, pode ser reavaliado como um incidente.

### 5.4 CATEGORIZAR E PRIORIZAR INCIDENTE

- Os incidentes não registrados pelos usuários (e, portanto, não categorizados ainda) devem ser analisados, categorizados e priorizados, exatamente como feito com as requisições normais.



## 5.5 PESQUISAR SOLUÇÕES DE CONTORNO

- Durante esta atividade, o operador deverá analisar todas as informações registradas no chamado a fim entender melhor o incidente. O operador poderá utilizar de vários meios que auxiliem na identificação da melhor solução de contorno, dentre os quais, citam-se:
  - Base de conhecimento e chamados semelhantes;
  - Procedimentos e outros documentos técnicos da organização;
  - Consulta a especialistas;
  - Fornecedores externos;
- Se existir um erro conhecido na base de conhecimento, o incidente deverá ser resolvido pela Equipe de Suporte. Caso contrário, deverá ser encaminhado imediatamente para o segundo nível de suporte (ver atividade **Acionar Suporte de 2º Nível**).

## 5.6 ACIONAR SUPORTE DE 2º NÍVEL

- Caso não exista na base de conhecimento um registro com a solução para o incidente ou o operador não consiga resolver o incidente no SLA definido, o operador da Equipe de Suporte deverá encaminhar o chamado para o 2º nível de suporte.
- É importante que o operador da Equipe de Suporte se certifique de que o chamado possui as informações suficientes para o atendimento. Caso o chamado não possua informações suficientes para o atendimento, a Equipe de Suporte deve solicitar mais informações ao usuário, utilizando a ferramenta ou através do telefone.

## 5.7 RESOLVER E RESTAURAR O AMBIENTE

- Esta atividade pode ser realizada tanto pela Equipe de Suporte quanto pelo suporte de 2º nível, conforme mostra o fluxo do processo. Em ambos os casos, o operador deverá atuar na resolução do incidente conforme solução descrita na base de erros conhecidos e registrar, no histórico do chamado, as ações realizadas. Depois, deverá certificar-se, juntamente com o usuário, de que o ambiente foi realmente restaurado.
- É importante ressaltar que na Equipe de Suporte o atendimento deverá ser por telefone, via acesso remoto ao computador ou presencial, devendo o chamado ser encaminhado para o segundo nível somente quando o suporte nível primeiro não conseguir resolver ou restaurar o ambiente.

- Para alguns incidentes, a solução de contorno pode depender de um fornecedor externo. Nesses casos, o suporte de segundo nível será apoiado por essa equipe externa.

## **5.8 RESOLVER PENDÊNCIA IMPEDITIVAS PARA SOLUÇÃO DE CONTORNO**

- Caso o incidente não seja resolvido no prazo definido no SLA, o Gerente de Incidentes deverá atuar na definição um plano de ação e acompanhamento da resolução do incidente.

## **5.9 ATUALIZAR BASES DE CONHECIMENTO**

- Ao constatar que o ambiente foi restaurado, a Equipe de Suporte deverá registrar a solução de contorno aplicada ao incidente utilizada ou a Equipe de Suporte de 2º Nível deverá atualizar a base de conhecimentos.

## **5.10 ENCERRAR CHAMADO**

- Como o gerenciamento de incidentes não trata as causas do mesmo, caso haja necessidade, o processo de gestão de Problemas deve ser iniciado.
- O chamado referente ao incidente pode ser finalizado no sistema e o usuário que registrou o chamado é notificado automaticamente a respeito do seu encerramento e restauração do serviço.

## **6.0 CATÁLOGO DE SERVIÇOS**

- A lista dos serviços de TI e suas características (nome, descrição, tarefas), assim como o SLA das tarefas estão definidos no documento **EMAP-DSGSI-15 Catálogo de Serviços de TI**.

## **7.0 ANEXOS**

Não há.

## 8.0 REGISTROS

Identificação	Local do Arquivo	Armazenamento	Proteção	Recuperação	Tempo de Retenção		Descarte
					Tempo	Base legal	
Registro de Tratamento de Incidente	Servidor	Central de Serviços da GETIN	Usuário e senha. Acesso restrito à GETIN	Ordem cronológica	Permanente	Não há	Não há
Base de Erros Conhecidos	Servidor	Central de Serviços da GETIN	Usuário e senha. Acesso restrito à GETIN	Ordem cronológica	Permanente	Não há	Não há

## 9.0 HISTORICO DE REVISÃO

Versão	Data	Item	Revisões
0	25/09//2019		Publicação do procedimento
1	18/09/2020	2	Documentos de referência atualizados
1	18/09/2020	5.2	Atualizada nomenclatura das prioridades