GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

ARTEFATO GERENCIAMENTO DE INCIDENTES E PROBLEMAS (CENTRAL DE SERVIÇOS)

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO

SECRETARIA DE COORDENAÇÃO E GOVERNANÇA DAS EMPRESAS ESTATAIS

DIRETORIA DE ORÇAMENTO DE ESTATAIS

COORDENAÇÃO-GERAL DE GESTÃO DA INFORMAÇÃO DE ESTATAIS

BRASÍLIA - 2018

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO
SECRETARIA DE COORDENAÇÃO E GOVERNANÇA DAS EMPRESAS ESTATAIS

Fernando Antonio Ribeiro Soares
Secretário

André Nunes
Diretor do Departamento de Orçamento de Estatais

Gerson Batista Pereira
Coordenador-Geral de Gestão da Informação de Estatais

EQUIPE TÉCNICA
Natal Henrique Troz Guglilhermi – SEST
Otávio Porto Barbosa – SEST

UNIVERSIDADE DE BRASÍLIA

Márcia Abrahão Moura
Reitora

Sanderson Cesar Macedo Barbalho
Diretor do Centro de Apoio ao Desenvolvimento Tecnológico – CDT

Rafael Timóteo de Sousa Júnior
Coordenador do Laboratório de Tecnologias da Tomada de Decisão – LATITUDE

EQUIPE TÉCNICA
Georges Daniel Amvame Nze (Pesquisador Sênior)
Claudia Jacy Barrenco Abbas (Pesquisador Sênior)
Edna Dias Canedo (Pesquisador Sênior)
Rodrigo de Souza Goncalves (Pesquisador Sênior)
Adyr Andrade de Menezes
Amanda Aline Figueiredo Carvalho
Bruno Justino Garcia Praciano
Demétrio Antônio da Silva Filho
Fabricio de Oliveira Taguatinga
Glauber Luiz Lopes da Silva
Jean Victor Ribeiro Vieira
João Batista Alves Diniz
Jorge Guilherme Silva dos Santos
José Maria dos Reis Lisboa
Leomar Camargo de Souza
Marcus Vinicius Bomfim Guimaraes Barbalho
Moramay Coutinho Guimarães Coelho
Pedro Thiago Rocha de Alcântara
Priscilla Gonçalves da Silva e Souza
Rafaella Aparecida Rosa Lima
Rosa Cristina Portela Dias Jácome
Ruyther Parente da Costa
Victor Matheus da Silva

B823g
Brasil. Ministério do Planejamento, Desenvolvimento e Gestão.

Governança de tecnologia da informação : artefato gerenciamento de incidentes e problemas (Central de Serviços) / Ministério do Planejamento, Desenvolvimento e Gestão, Secretaria de Coordenação e Governança das Empresas Estatais, Coordenação-Geral de Gestão da Informação de Estatais; Universidade de Brasília. -- Brasília : MP, 2018.
23 p.

1. Governança Digital 2. Tecnologia da Informação 3. Empresa Estatal 4. Administração Pública I. Título II. Universidade de Brasília.

CDU 658.115:004

HISTÓRICO DE VERSÕES

15/03/2018 | Versão 1.0

Descrição: Inclusão dos artefatos, definição do processo, adequação do passo-a-passo, objetivos e capa ao processo.

Autor: Edna Dias Canedo e Pedro Thiago Rocha de Alcântara.

Revisor: Natal Henrique Troz Guglilhermi e Otávio Porto Barbosa.

SUMÁRIO

INTRODUÇÃO

Em observância às normas e diretrizes de Tecnologia da Informação (TIC) do Poder Executivo Federal, disseminadas pela Secretaria de Tecnologia da Informação e Comunicação do Ministério do Planejamento, Desenvolvimento e Gestão (SETIC/MP), na condição de Órgão Central do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) e, conforme preconiza o Decreto Presidencial nº 7.579, de 11 de outubro de 2011, o Ministério do Planejamento, Desenvolvimento e Gestão (MP), como Órgão Setorial integrante do SISP, vincula-se aos preceitos definidos pelo Sistema relativamente à governança e gestão de tecnologia da informação.

Diante do tema e também em decorrência de orientação do TCU, conforme Acórdão 3051/2014 a SEST deve atuar no desenvolvimento de ações que promovam a disseminação da cultura de Governança de TIC nas Empresas Estatais, para facilitar o cumprimento dos objetivos definidos e exigidos no planejamento estratégico, como também na racionalização de recursos e retorno financeiro/operacional.

VISÃO GERAL

2.1. Objetivo

Identificar e apontar os passos necessários, de acordo com as práticas listadas na literatura e conhecimento prático, para a Gerenciamento de Incidentes e Problemas (Central de Serviços) nas diferentes Empresas Estatais.

2.2. Justificativa

A SEST, institucionalmente, como órgão de Coordenação e Governança das Empresas Estatais, deve promover e orientar a Governança de TIC dessas entidades. As iniciativas nesse sentido devem ser planejadas e priorizadas a partir do alinhamento dos investimentos de TIC aos objetivos estratégicos das organizações.

GERENCIAMENTO DE INCIDENTES E PROBLEMAS (CENTRAL DE SERVIÇOS)

3.1. Definição

O Gerenciamento de Incidentes e Problemas (Central de Serviços) visa fornecer resposta rápida e eficaz às solicitações dos usuários e resolver todos os tipos de incidentes e problemas.

Para isso, faz-se necessário restaurar serviços de forma eficiente, identificar e classificar os problemas e suas causas raízes, fornecer resolução oportuna para evitar incidentes recorrentes e recomendações para melhorias.

3.2. Passo a passo

Para implantação do Gerenciamento de Incidentes e Problemas (Central de Serviços) é preciso executar as seguintes atividades:

1 - Definir um esquema de classificação de registros de incidentes de serviços de TIC e estabelecer uma Base de Conhecimento na Estatal, na qual devem ser registrados todos os incidentes e soluções adotadas.

2 - Estabelecer e manter uma abordagem para resolução e prevenção de incidentes na Estatal.

4 - Identificar incidentes e as suas causas e registrar as informações para registro na Base de Conhecimento da Estatal.

5 - Classificar e priorizar os incidentes e solicitações de serviços de TIC da Estatal.

6 - Definir os critérios de atendimento de solicitações de serviços da Estatal.

7 - Analisar as solicitações de serviços, aprova-las e atende-las com base nos critérios estabelecidos pela Estatal.

8 - Investigar, diagnosticar e definir um plano de ações para os incidentes registrados na Estatal.

9 - Aplicar o plano de ações definido para resolução e recuperar as operações e serviços após incidentes na Estatal.

10 - Monitorar e comunicar às partes interessadas o status dos incidentes até o encerramento.

11 - Gerar relatórios de incidentes contendo seus status e disponibilizar a toda a Estatal.

12 – Identificar, classificar, investigar e diagnosticar Problemas e determinar as ações corretivas a serem adotadas pela Estatal.

13 - Gerenciar a execução das ações corretivas determinadas pela Estatal.

14 - Finalizar a ocorrência de problema ou incidentes, quando encontrada resolução, e registrar a solução na Base de Conhecimento da Estatal.

15 - Identificar Erros Conhecidos e documenta-los em um formulário apropriado.

16 - Executar o gerenciamento proativo de Problemas na Estatal.

ARTEFATOS

4.1. Documentos

Os modelos dos documentos para o Gerenciamento de Incidentes e Problemas (Central de Serviços), estão disponíveis para download no endereço eletrônico http://www.planejamento.gov.br/acesso-a-informacao/institucional/unidades/sest, conforme lista a seguir:

Planejar Gerenciamento de Incidentes e Problemas	
 Plano de Gerenciamento de Incidentes	Nome: Plano de Gerenciamento de Incidentes
	Objetivo: Descrever as condições para que a Estatal gerencie todas as fases de um incidente.
 Plano de Gerenciamento de Problemas	Nome: Plano de Gerenciamento de Problemas
	Objetivo: Prevenir a ocorrência de problemas e seus incidentes resultantes, eliminando incidentes recorrentes e assim minimizando o impacto dos incidentes que não podem ser prevenidos.

Relatar Gerenciamento de Incidentes e Problemas	
 Relatório das Requisições de Serviços e Incidentes	Nome: Relatório das Requisições de Serviços e incidentes
	Objetivo: Registrar as requisições de serviços e os incidentes.
 Relatório de Ações Corretivas	Nome: Relatório de Ações Corretivas
	Objetivo: Registrar as ações corretivas a serem tomadas na resolução de um determinado incidente ou problema.
 Relatório dos Incidentes e seu Status	Nome: Relatório dos Incidentes e seu status
	Objetivo: Registrar a lista de incidentes ocorridos e seus respectivos status.
Documentar Base de Conhecimento	
 Base de Conhecimento	Nome: Base de Conhecimento
	Objetivo: Registrar os incidentes e problemas já resolvidos com suas devidas soluções e as lições aprendidas no processo de resolução.

4.1.1 Plano de Gerenciamento de Incidentes

Plano de Gerenciamento de Incidentes da <Sigla da estatal>

Controle de Versões

<Inserir os dados das versões.>

Versão	Data	Autor	Notas da Revisão

1. Objetivo do Plano de Gestão de Incidentes

<Descrever o objetivo do Plano de Gestão de Incidentes.>

2. Gestão de Incidentes

<Usar as seções seguintes para identificar os componentes do Plano de Gestão de Incidentes.>

2.1. Processos de Incidentes

<Descrever o(s) Processo(s) de Gestão dos Incidentes a serem adotados.>

2.2. Documentos Padronizados de Incidentes

<Descrever os documentos padronizados a serem usadas nos processos dos incidentes. Indique onde estão armazenados, como serão usados, e os responsáveis envolvidos.>

2.3. Responsabilidades da Equipe de Incidentes

<Descrever as responsabilidades referentes aos processos dos incidentes de cada membro do projeto, mesmo que já citados em outros tópicos do documento. Ressaltar as divisões de responsabilidade entre compras, projetos e jurídico.>

Membro da Equipe	Responsabilidades

2.4. Ferramentas Usadas

<Listar as ferramentas que o projeto empregará. Descrever como serão usadas e o responsável por isso.>

Ferramenta	Descrição	Quando aplicar	Responsavel

3. Indicadores de Desempenho

<Descrever indicadores de desempenho de incidentes. >
Exemplo:

Indicador	Descrição	Periodicidade

Aprovado em ___ de _____ de _____.

<nome completo da autoridade máxima da Estatal >
<cargo da autoridade máxima da Estatal >

Observações:

O Gerenciamento de Incidentes tem o objetivo de restabelecer serviços interrompidos o mais rápido possível minimizando o impacto negativo no negócio.

A Gestão dos incidentes garante que os melhores níveis de disponibilidade e de qualidade dos serviços, sejam mantidos conforme os acordos de nível de serviço.

É importante que o Gerenciamento de Incidentes conheça e seja informado de quaisquer mudanças.

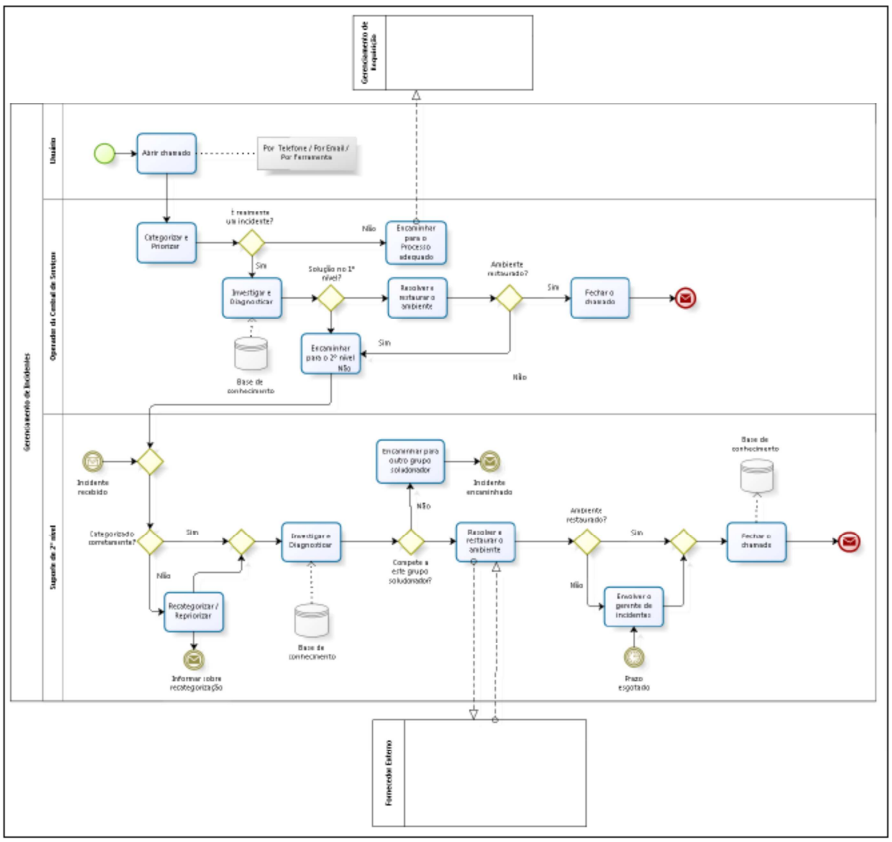
Um plano de gerenciamento de incidentes cria condições para que a organização gerencie todas as fases de um incidente.

É imprescindível que gerenciamento de incidentes descreva como será feita a gestão de incidentes na organização, relatando os processos de relacionados a incidentes e os indicadores de desempenho.

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 Central de Serviços deve solicitar mais informações do usuário quando o chamado não dispuser de informação suficiente para o atendimento.

Exemplo de um processo de gerenciamento de incidentes:



Ferramentas Usadas:

Action/Response: Um script, comando ou qualquer tipo de resposta gerada na maioria das vezes automaticamente que representa um evento necessário alertando sobre um determinado incidente ou iniciando uma tarefa diária, como a inicialização de um aplicativo, por exemplo.

Alert: Uma notificação de que algo aconteceu, gerada quando as ferramentas de monitoramento detectam algo no ambiente que necessite de atenção.

Event Correlation: Procedimento para avaliar a relação entre objetos com o intuito de determinar o quanto uma alteração feita em um pode afetar o outro.

Control: Uma resposta ou conjunto de respostas automáticas, os três tipos de controle são: Diagnostic, Notification e Interoperability.

Event: Uma ocorrência, geralmente um incidente, no ambiente de TI descoberta pela ferramenta de monitoramento.

Reporting: Uma coleção de informações sobre o nível e a qualidade do serviço, deverá ser utilizado pelas SMFs Capacity, Availability e Service Level Management.

Resolution Completion: Ponto no processo de controle em que todas as ações para o gerenciamento de incidentes foram executadas com sucesso.

Exemplo de Responsabilidade da Equipe:

Papel	**Responsabilidades**
Gestor do Processo	Garantir que o processo esteja adequado aos propósitos da estatal e realizar as melhorias necessárias; • Garantir que a documentação do processo esteja atualizada e acessível a todos os envolvidos. • Garantir que os envolvidos sejam informados das mudanças efetuadas no processo; • Definir e revisar periodicamente os indicadores de desempenho utilizados para aferir a eficácia e eficiência do processo; • Garantir que relatórios com os indicadores de desempenho sejam produzidos e distribuídos entre os interessados.
Gerente do Processo	Indicar as pessoas adequadas aos papéis definidos no processo; • Promover e garantir que o processo seja seguido conforme o especificado; • Gerenciar os recursos alocados ao processo (pessoal, financeiros, etc.) de forma otimizada;

Indicadores de Desempenho:

Os indicadores de desempenho, são métricas que quantificam a performance de acordo com os objetivos organizacionais. Para que esses **indicadores de desempenho** tenham uma contribuição significativa no controle da estatal, primeiro é necessário entender o planejamento estratégico e ter objetivos claros na hora da definição das metas que devem ser alcançadas. A partir daí, a elaboração e a gestão dos indicadores de desempenho podem ser direcionadas para o monitoramento da evolução dos resultados da estatal e servir como referência para o processo de tomada de decisão e a criação de estratégias de melhoria.

4.1.2 Plano de Gerenciamento de Problemas

Plano de Gerenciamento de Problemas da <Sigla da estatal>

Controle de Versões

<Inserir os dados das versões.>

Versão	Data	Autor	Notas da Revisão

1. Objetivo do Plano de Gestão de Problemas

<Descrever o objetivo do Plano de Gestão de Problemas.>

2. Gestão de Problemas

<Usar as seções seguintes para identificar os componentes do Plano de Gestão de Problemas.>

2.1. Processos de Problemas

<Descrever o(s) Processo(s) de Gestão dos Problemas a serem adotados.>

2.2. Documentos Padronizados de Problemas

<Descrever os documentos padronizados a serem usadas nos processos dos incidentes. Indique onde estão armazenados, como serão usados, e os responsáveis envolvidos.>

2.3. Responsabilidades dos Problemas

<Descrever as responsabilidades referentes aos processos dos problemas de cada membro do projeto, mesmo que já citados em outros tópicos do documento. Ressaltar as divisões de responsabilidade entre compras, projetos e jurídico.>

Membro da Equipe	Responsabilidades

2.4. Ferramentas Usadas

<Listar as ferramentas que o projeto empregará. Descrever como serão usadas e o responsável por isso.>

Ferramenta	Descrição	Quando aplicar	Responsavel

3. Rastreamento de Problemas

<Identifique as categorias de problemas e onde elas serão armazenadas e rastreadas.>

Aprovado em ___ de _____ de _____.

<nome completo da autoridade máxima da Estatal >
<cargo da autoridade máxima da Estatal >

Observações:

O Gerenciamento de Problemas tem como objetivo prevenir a ocorrência de problemas e seus incidentes resultantes, eliminando incidentes recorrentes e assim minimizando o impacto dos incidentes que não podem ser prevenidos.

Pode-se elencar como atividades do Gerenciamento de Problemas:

- Detecção e Registro do Problema: análise de incidentes recorrentes ou incidentes não identificados pela Central de Serviços ou pelo Gerenciamento de Incidentes. Todos os problemas devem conter informações importantes para o atendimento do problema e quando partir de um registro de incidentes, o problema deve herdar as informações relevantes do registro de incidentes como todo o histórico anterior;

- Categorização do Problema: os problemas devem ser categorizados da mesma forma que os incidentes, podendo ser categorizados em grupos ou projetos.

- Priorização do Problema: os problemas devem ser classificados quanto ao seu impacto sobre o negócio assim como a urgência de sua solução;

- Investigação e Diagnóstico: a atividade de investigação e diagnóstico consiste em identificar a causa raiz dos problemas. Muitas vezes as causas dos problemas residem em procedimentos errados;

- Registro de Erro Conhecido: assim que a causa for identificada e a solução for encontrada, um erro Conhecido deve ser registrado na Base de Dados de Erros Conhecidos para posterior utilização das equipes de Gerenciamento de Incidentes;

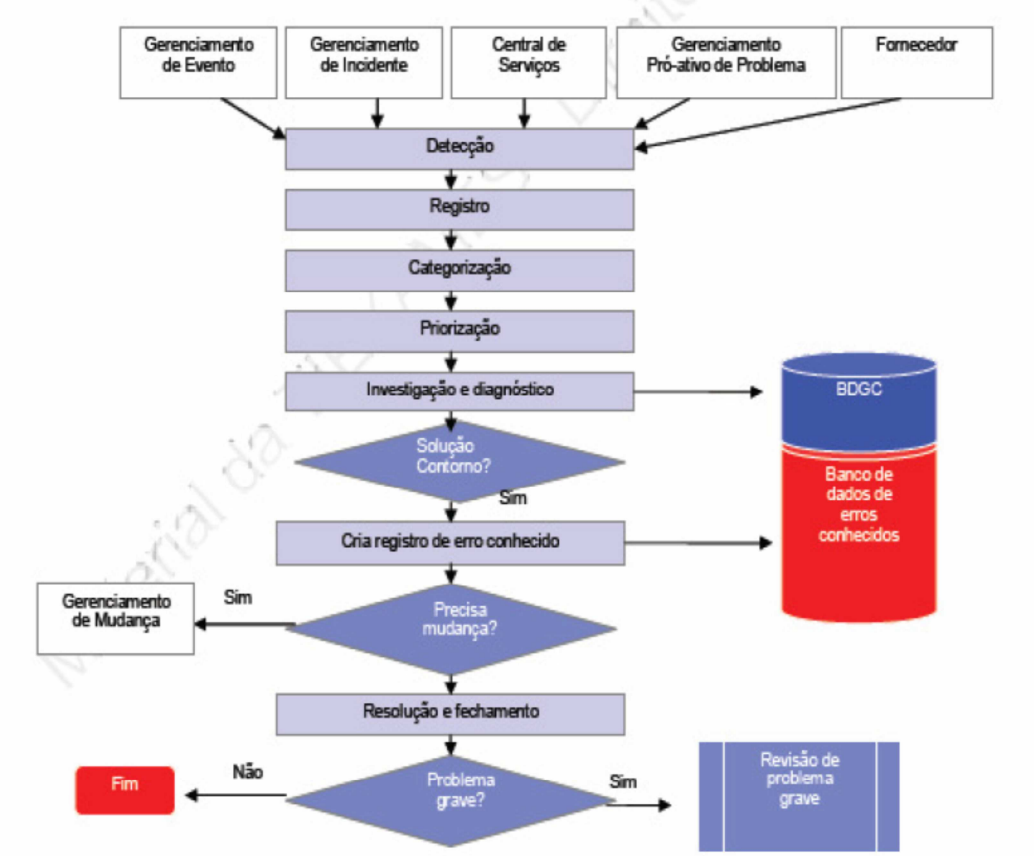
- Resolução do Problema: consiste na análise sobre como resolver o problema;

Fechamento do Problema: após aplicar a solução, o Registro de Problema é fechado, assim como os Registros de Incidentes relacionados ao problema.

É imprescindível que o plano de gerenciamento de problemas descreva como será feita a gestão de problemas na estatal, relatando os processos de relacionados a problemas e o rastreamento de problemas.

O Gerenciamento de Problema foca a identificação da causa-raiz do problema e o desenvolvimento de uma proposta para remover definitivamente o erro da infraestrutura. Os problemas são a causa de um ou mais incidentes. Um incidente nunca vira problema: sempre teremos dois registros separados, um para cada processo. Podemos ter 1.000 registros de incidentes referentes ao travamento da tela de determinado sistema e apenas um registro de problema. É importante separar o registro de incidente do registro de problema. Ao implantar um software na Central de Serviços, recomenda-se que este tenha o recurso de poder vincular a ID (identificação) do incidente no formulário de cadastro do problema.

Ciclo do processo de Gerenciamento de Problema.



Membro da Equipe	Responsabilidades
Gestor de Problemas	É responsável por gerenciar o ciclo de vida de todos os problemas. Seus principais objetivos são prevenir que incidentes aconteçam e minimizar o impacto de incidentes que não podem ser evitados. Para este fim, ele mantém informações sobre erros conhecidos e soluções adotadas em uma base própria dessa gestão.

4.1.3 Relatório das Requisições de Serviços e incidentes

Relatório das Requisições de Serviços e Incidentes da < estatal>

Controle de Versões

<Inserir os dados das versões.>

Versão	Data	Autor	Notas da Revisão

1. Requisições de Serviços

<Listar e identificar as requisições de serviços e suas características >

ID	Categoria	Descrição	Data	Responsável

2. Incidentes

< Listar e identificar os incidentes e suas características >

ID	Categoria	Descrição	Data	Responsável

Aprovado em ___ de _____ de _____.

<nome completo da autoridade máxima da Estatal >
<cargo da autoridade máxima da Estatal >

Observações:

INCIDENTE: É qualquer acontecimento que ocorre com algum componente que tenha alguma ligação com um serviço já prestado pelo departamento de TI e que não faça parte do comportamento padrão de usabilidade causando assim a redução na qualidade do serviço de TI ou até mesmo a interrupção do serviço como um todo. Abaixo alguns exemplos:

- Internet Lenta;
- Indisponibilidade para acessar uma pasta na rede;
- E-mail não enviando mensagens;
- Impressora com problema para imprimir.

REQUISIÇÃO: É quando tudo está funcionando perfeitamente nos serviços de TI, porem o usuário precisa da mão de obra do departamento de tecnologia para a criação de um recurso ou desenvolvimento de uma nova ferramenta de trabalho. Abaixo, novamente alguns exemplos:

- Criação de um e-mail;
- Mudança na instalação de um computador;
- Desenvolvimento de um novo relatório no sistema.

EVENTO: Normalmente o setor de TI possui algum tipo de sistema ou tecnologia que é capaz de realizar o monitoramento dos ativos e dos equipamentos de informática. É muito comum que esse sistema também faça alguns avisos, seja por e-mail, SMS ou até mesmo numa televisão mostrando os itens que estão sendo monitorados e, quando apresentado algum problema, destacando eles dos demais. O evento normalmente é qualquer requisição que é feita de uma maneira automática para o setor de TI, ou seja, para ser considerado evento, não se pode haver qualquer intervenção seja de um usuário ou até mesmo de um técnico especializado. Abaixo, segue alguns exemplos:

- Link de Internet com consumo próximo ao contratado junto a operadora;
- Disco rígido de um servidor cheio;
- Sessões trancadas no servidor do banco de dados.

4.1.4 Relatório de Ações Corretivas

Relatório de Ações Corretivas <estatal>

Controle de Versões

<Inserir os dados das versões.>

Versão	Data	Autor	Notas da Revisão

1. Descrição da Não Conformidade

<Descrever motivo, real ou potencial, das ações corretiva. >

1.1. Áreas Envolvidas

1.1.1. Responsáveis pelas Áreas Envolvidas

2. Descrição da Correção

<Descrever de ações tomadas para sanar o problema.>

2.1.1. Áreas Envolvidas
2.1.2. Responsáveis pela Correção
2.1.3. Data

3. Resultados das Ações Tomadas

<Descrever resultados, esperados e obtidos, com as ações corretivas tomadas.>

3.1.1. Responsáveis pela Verificação da Correção
3.1.2. Data

4. Origem da Não Conformidade

<Indicar a origem da não conformidade.>

5. Investigação da Causa da não Conformidade

<Descrever os resultados da investigação da causa da não conformidade.>

6. Descrição das Ações Corretivas

<Descrever ações corretivas.>

7. Verificação da Eficácia das Ações Corretivas

<Descrever como é verificada a eficácia das ações corretiva. >

Aprovado em ___ de _____ de _____.

<nome completo da autoridade máxima da Estatal >
<cargo da autoridade máxima da Estatal >

Observações:

É imprescindível ter procedimentos para registrar, avaliar e investigar acidentes, incidentes e não conformidades. O principal propósito do procedimento é prevenir a repetição da situação, identificando e documentando suas causas raízes. Além disso, é recomendado que os procedimentos possibilitem detectar, analisar e eliminar as causas potenciais de não conformidades.

As entradas típicas desse processo incluem:

- Procedimentos (em geral);
- Plano de emergência;
- Relatórios de identificação de perigos e de avaliação e controle de riscos;
- Relatórios de acidentes, incidentes e/ou perigos;
- Relatórios de manutenção e de serviços.

No processo é necessário que a organização prepare procedimentos documentados, a fim de assegurar que acidentes, incidentes e não conformidades estão sendo investigados e que as ações corretivas e preventivas foram iniciadas. É recomendado que seja monitorado o progresso da implementação das ações corretivas e preventivas, e analisada criticamente a eficácia de tais ações.

Para isso é imprescindível descrever a não conformidade, relatando as áreas envolvidas, descrever a correção e seus resultados, indicar as origens da não conformidade, relatar a investigação das causas da não conformidade.

E também, indicar e descrever as ações corretivas que serão tomadas e como elas serão verificadas.

Ação corretiva: Ações corretivas são medidas tomadas para eliminar a (s) causa (s) raiz de não-conformidades, acidentes ou incidentes identificados, a fim de prevenir sua repetição. Exemplos de elementos a serem considerados ao se estabelecer e manter procedimentos para ação corretiva incluem:

- Identificação e implementação de medidas corretivas e preventivas tanto a curto como a longo prazo (isso pode incluir também o uso de fontes de informação apropriadas, tais como recomendações de funcionários especializados em incidentes);
- Avaliação de qualquer impacto nos resultados da identificação de perigos e da avaliação de riscos (e de quaisquer necessidades de atualização do (s) relatório (s) de identificação de perigos e de avaliação e controle de riscos);
- Registro de qualquer alteração requerida nos procedimentos, resultante da ação corretiva ou da identificação de perigos e da avaliação e controle de riscos;
- Aplicação de controles de riscos ou modificação dos controles de riscos existentes, a fim de assegurar que as ações corretivas são tomadas e que são eficientes.

Ação preventiva: Exemplos de elementos a serem considerados ao se estabelecer e manter procedimentos para ação preventiva incluem:

- Uso de fontes de informação apropriadas (tendências dos "incidentes sem perdas", relatórios de auditorias do Sistema de Gestão da TI, registros, atualização das análises de riscos, novas informações sobre materiais perigosos, "rondas" de segurança, recomendações de funcionários especializados em SI, etc.);
- Identificação de quaisquer problemas que requeiram ação preventiva;
- Iniciação e implementação da ação preventiva e aplicação de controles para assegurar a eficiência da ação preventiva;
- Registros de quaisquer alterações nos procedimentos resultantes da ação preventiva, e submissão para aprovação.

Acompanhamento

É recomendado que as ações corretivas e preventivas tomadas sejam as mais permanentes e eficientes possíveis. É recomendado que se façam verificações da eficácia das medidas corretivas/preventivas tomadas. É recomendado que as ações pendentes/atrasadas sejam relatadas à alta Administração na primeira oportunidade.

Análise de não-conformidades, acidentes e incidentes

É recomendado que as causas de não-conformidades, acidentes e incidentes sejam classificadas e analisadas regularmente. É recomendado que as taxas de frequência e de gravidade de acidentes sejam calculadas de acordo com a prática aceita para fins de comparação.

É recomendado que seja realizada a classificação e a análise dos seguintes itens:

- Taxas de frequência ou gravidade de doenças/lesões com perda de tempo;
- Localização e tipo da lesão, parte do corpo atingida, atividade envolvida, unidade envolvida, dia, hora (todos os itens apropriados);
- Tipo e gravidade dos danos à propriedade;
- Causas diretas e causas-raiz.

Monitoramento e comunicação de resultados

É recomendado que a eficácia das investigações e notificações de incidentes seja avaliada. É recomendado que a avaliação seja objetiva e produza um resultado quantitativo, se possível.

Após ser informada sobre a investigação, é recomendado que a estatal:

- Identifique as causas-raiz das deficiências no Sistema de Gestão de TI e na administração geral da organização, onde aplicável;
- Comunique as constatações e recomendações à Administração e às partes interessadas pertinentes;
- Inclua as constatações e recomendações pertinentes das investigações no contínuo processo de análise crítica de incidentes;
- Monitore a implementação oportuna dos controles corretivos e de sua subsequente eficácia ao longo do tempo;
- Aplique as lições aprendidas da investigação das não-conformidades em toda a organização, concentrando-se nos amplos princípios envolvidos, ao invés de se restringir a ações específicas projetadas para evitar a repetição de um evento exatamente similar, na mesma área da organização.

Resultados típicos

Os resultados típicos incluem os seguintes itens:

- Procedimento para acidentes e não-conformidades;
- Relatórios de não-conformidades;
- Cadastro de não-conformidades;
- Relatórios de investigações;
- Relatórios atualizados de identificação de perigos e de avaliação e controle de riscos;
- Entradas da análise crítica pela Administração;
- Evidência das avaliações da eficácia das ações corretivas e preventivas tomadas.

4.1.5 Relatório dos Incidentes e seu status

Relatório dos Incidentes e seu Status da <Sigla da estatal>

Controle de Versões

<Inserir os dados das versões.>

Versão	Data	Autor	Notas da Revisão

1. Incidentes

< Listar incidentes e seus status >

ID do Incidente	Categoria	Descrição da Incidente	Data	Status

Aprovado em ___ de _____ de _____.

<nome completo da autoridade máxima da Estatal >
<cargo da autoridade máxima da Estatal >

Observações:

Os incidentes são eventos alheios à operação normal. Quando ocorre um incidente, os processos operacionais normais da organização são interrompidos.

Um relatório de incidentes deve conter os dados essenciais que devem constar em uma notificação para identificar a origem da ação, como por exemplo:

- Logs completos;
- Data, horário e time zone (fuso horário) dos logs ou da atividade sendo notificada;
- Dados completos do incidente ou qualquer outra informação relevante na identificação da atividade.

Campos de Incidente

Os campos a seguir são necessários para criar ou atualizar um incidente:

Número de referência do incidente. Este é um número de referência exclusivo atribuído pelo Service Desk Manager a todos os tickets de incidente. Ele é usado pelos analistas e clientes para fazer referência a um determinado ticket de incidente.

Solicitador. Especifica o nome da pessoa que iniciou o ticket. Essa pessoa deve ser um contato definido. É possível digitar um valor diretamente ou clicar na lupa para pesquisar um nome.

Usuário final afetado. Especifica o nome de contato da pessoa afetada pelo registro. Se o contato for atribuído a um tipo de tratamento especial, indicadores de tratamento especial são exibidos. É possível digitar um valor diretamente ou clicar no ícone de lupa para pesquisar o nome do contato.

Área de incidente. Indica a área geral de seu ambiente de TI afetada pelo incidente. Por exemplo, aplicativos, e-mail, hardware e software. Uma área de incidente fornece valores padrão que são inseridos automaticamente em todos os tickets de incidentes relacionados à área. Além das áreas de incidente predefinidas, seu administrador do sistema pode definir áreas de incidente personalizadas. É possível inserir um valor diretamente, ou pode-se expandir o nó para exibir as áreas de incidente definidas e selecionar uma.

Status

Especifica o código do status do registro. Por exemplo, é possível listar apenas tickets com o código de status Correção em andamento ou Fechamento solicitado. É possível digitar um valor diretamente ou clicar no ícone de lupa para procurar um status. O botão azul (no lado esquerdo do campo Status) permite mudar o status atual para o próximo status padrão.

Nível de prioridade

Especifica a classificação de prioridade do registro. A classificação determina a quantidade de atenção que o ticket recebe. Os níveis de prioridade predefinidos vão de 1 (mais alto) a 5 (mais baixo). O administrador do sistema ou um cálculo de prioridade ativa podem gerar os valores de prioridade adequados para várias instalações e inquilinos. Quando o cálculo de prioridade está ativado, esse campo é atualizado com base nas configurações de Impacto, Urgência, Serviço afetado e Usuário afetado. Quando o administrador desativa o cálculo de prioridade e desinstala a opção, os usuários de autoatendimento veem o campo Prioridade na página Detalhes de solicitação.

Ativo

Indica se o registro está Ativo ou Inativo. Esse valor se aplica apenas ao registro atual, e não ao modelo associado.

Campos de Detalhes

- **Reportado por**
  Especifica o nome da pessoa que reporta o registro do incidente.
- **Responsável**
  Especifica o nome da pessoa com a atribuição de lidar com o registro.
- **Grupo**
  Especifica o grupo responsável por esse registro. Pode ser definido grupos de contatos que serão responsáveis por diferentes tipos de ocorrências, solicitações, incidentes ou problemas. Qualquer contato que é parte do grupo pode lidar com o registro depois que ele está atribuído ao grupo.
- **Serviço afetado**

  Especifica o serviço primário que afeta o problema ou incidente.

  Urgência
  Especifica a urgência do registro. A urgência é determinada pela importância das tarefas de usuário afetadas pelo registro. Os códigos de urgência indicam a importância de um ticket com base no grau em que ele afeta as tarefas de usuário. Por exemplo, uma interrupção de rede é mais

urgente do que uma falha de impressora. O administrador do sistema pode modificar os códigos de urgência padrão. Portanto, eles podem variar de uma instalação para outra. Os valores de urgência podem ser atualizados automaticamente com base em um cálculo de prioridade ativo.

- **Impacto**
  Especifica um código de impacto, como 1 - Toda a organização, que indica como o ticket afeta o trabalho sendo executado. Por exemplo, um ticket que exija uma interrupção de rede durante várias horas terá um impacto maior do que um ticket que desative uma impressora. O administrador do sistema pode modificar os códigos de impacto padrão, portanto, eles podem variar de uma instalação para outra.
- **Incidente principal**
  Especifica que o incidente é principal ou significativo. Em vista da sua importância, as alterações desse valor em um ticket geram uma entrada no log de atividades.

  Observação: quando se copia um incidente, o valor desse campo é limpo. Além disso, tickets relacionados (incidentes filhos) não incluem o valor do Incidente principal.
- **Item de configuração**
  Especifica o hardware, software ou serviço afetado pelo registro. O administrador do sistema cria um registro que identifica exclusivamente cada item de configuração para a sua organização e indica seu local preciso.
- **Problema**
  Fornece o número e o nome do problema associado a esse registro. Insira o número ou nome do problema diretamente nesse campo ou clique no ícone de pesquisa para procurar o problema.
- **Sintoma**
  Especifica um código que descreve o sintoma primário do incidente. Por exemplo, resposta lenta.
- **Código de resolução**
  Indica a ação que o analista tinha tomado para resolver um incidente ou uma solicitação. Códigos de resolução especificam a resolução geral do ticket. Por exemplo, um código de resolução Patch aplicado indica que o analista usou um patch de software para resolver um incidente.
- **Método de resolução**
  Indica *como* o analista implementou a resolução. Por exemplo, um método de resolução por Sessão de bate-papo indica que o analista usou uma sessão de bate-papo para tratar do incidente.
- **Data/hora do retorno de chamado**
  Especifica a data e a hora do acompanhamento do registro.
- **Mudança**
  Especifica o número e o nome da requisição de mudança associada ao registro.
- **Causado por requisição de mudança**
  Especifica o número da requisição de mudança quando o ticket de Incidente é o resultado de mudanças implementadas a partir de uma requisição de mudança.

4.1.6 Base de Conhecimento

Base de Conhecimento da <Sigla da estatal>

Controle de Versões

<Inserir os dados das versões.>

Versão	Data	Autor	Notas da Revisão

1. Bases de Conhecimento e Lições Aprendidas

<Listar problemas e incidentes e as principais lições aprendidas. >

Projeto	Categoria	Descrição da lição aprendida	Data	Consequência	Ação Tomada

Aprovado em ___ de _____ de _____.

<nome completo da autoridade máxima da Estatal >
<cargo da autoridade máxima da Estatal >

Observações:

É imprescindível manter uma base de conhecimento dos incidentes e problemas ocorridos na estatal, descrevendo as lições aprendidas, ações tomadas e consequências.

Base de Conhecimento define bases de dados ou conhecimento acumulados sobre um determinado assunto. É um tema mítico e que todos desejam ter, mas requer muito empenho e dedicação para conseguir manter. Mas se bem empregada e funcional, melhora e muito a qualidade de atendimento e ajuda aos técnicos na resolução de incidentes.

As informações podem ser utilizadas na solução dos problemas apresentados pelos clientes, por meio de ferramentas e sistemas próprios para isso. É utilizada também em help desk /service desk e suporte técnico como, por exemplo, em uma central de atendimento telefônico. Uma Base de Conhecimento é extremamente útil para ajudar equipes em consultas de informações como por exemplo, resolução de um incidente, descrição de um procedimento, etc. E o mais importante é que muitas vezes a base de conhecimento pode ajudar integrantes novos que conhecem apenas um pouco sobre o sistema.

A Base de conhecimento pode ser usada por equipes:

– Atendimento ao Cliente – Base de conhecimento com scripts de perguntas e respostas esperadas com fluxos de padrão sistêmico.

– Suporte (Help Desk) – Base de conhecimento com conjunto de incidentes e dicas de atendimento ao usuário como problemas de funcionamento de plug-ins de bancos, sistemas ERP, etc., redirecionando inclusive há manuais dos produtos e links de apoio. Por exemplo, qualquer tipo de configuração do ERP, direcionar ao manual do produto.

– Suporte (Service Desk) – Base de conhecimento com conjunto de incidentes, boas práticas, dicas e exemplos de ambientes e configuração, informações de ambientes e ativos de redes, para definição de

como instalar produtos, resolver incidentes graves, buscar informações de determinado ativo ou configuração, entre outros.

– Área de Produtos/Desenvolvimento – Base de conhecimento com informações sobre documentações, boas práticas de arquitetura de software, informações históricas de clientes estratégicos, links para manuais adicionais.

Definir o foco da Base de Conhecimento

Para um bom início de Base de Conhecimento, deve-se definir qual o foco. E para definir esse foco, deve-se entender qual o objetivo que você ou sua equipe pretende atingir, pois o assunto **Base de Conhecimento** é muito amplo e há diversas variações, por isso a necessidade de se definir muito bem antes de iniciar. Por exemplo, você observa:

- Que na sua equipe, alguns técnicos têm dificuldades em resolver determinados incidentes devido à falta de conhecimento em alguns procedimentos que estão hoje apenas "na cabeça" dos técnicos mais antigos;
- Que não se tem um padrão de boas práticas de configuração dos aplicativos da estatal, devido a apenas alguns conhecerem de tais boas práticas;
- Que para procedimentos simples como uma configuração padrão do software, seu técnico tem dificuldades em executar o processo, principalmente quando é um técnico júnior.
- Que não há um padrão de atendimento (primeiro combate) com um roteiro de perguntas para facilitar a identificação de um problema, como por exemplo perguntas: – Quando começou a acontecer? – Foi realizada algum update na aplicação? Entre outras perguntas.
  – Que sua equipe de desenvolvimento/arquitetura não segue padrões de desenvolvimento e boas práticas;
- Que há dificuldades em se achar informações sobre determinados projetos, clientes, alterações ou customizações de produtos;

REFERÊNCIAS BIBLIOGRÁFICAS

5.1. Documentos

- Planejamento Estratégico da Secretaria 2015-2018.
- Guia de Comitê de TIC do SISP (versão 2.0 – 2016).
- Guia do PDTIC do SISP (Versão 2.0 Beta – 2015).
- Guia de Gerenciamento de Projetos do SISP (Versão 1.0 MGP-SISP – 2011).
- Guia de Metodologia de Gerenciamento de Portfólio de Projetos do SISP (Versão 1.0 MGPP-SISP – 2013).
- Guia de Processo de Software do SISP (Versão 1.0 PSW-SISP 2012).
- Guia de Governança de Tecnologia da Informação e Comunicação (GovTIC) do SISP (Versão 2.0 - 2017).