TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO

COORDENADORIA DE INFRAESTRUTURA E SUPORTE - STI

Processo de Gerenciamento de Incidentes

Vitória – março/2022

Versão 2.1

Conteúdo

1. Objetivo

O Gerenciamento de Incidentes 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 ANS (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.

2. Escopo

O Gerenciamento de Incidentes é aplicável a todos os serviços que são prestados pela Secretaria de Tecnologia da Informação (STI) que estão descritos no Catálogo de Serviços de TI do TRE-ES.

Um incidente é qualquer evento que cause ou possa causar interrupção ou redução da qualidade do serviço prestado. Incidentes podem ser reportados à Central de Serviços de TIC (CESTIC) pelos usuários, pelo próprio pessoal da TI ou, automaticamente, pelas ferramentas de monitoramento. Alguns exemplos de incidentes são: impossibilidade de enviar um e-mail, internet indisponível ou um problema na estação de trabalho. É importante diferenciar incidentes de requisições de serviços, já que ambos são reportados à Central de Serviços. Requisição de serviço é uma requisição formal de um usuário por algo a ser fornecido, por exemplo: uma requisição de informação, uma solicitação para redefinir uma senha ou a preparação das estações de trabalho em uma sala de treinamento. As requisições de serviço são gerenciadas pelo processo de cumprimento de requisição.

Por fim, vale ressaltar que não faz parte do escopo do gerenciamento de incidentes investigar a causa raiz dos incidentes (isso faz parte do escopo do gerenciamento de problemas). Como dito acima, o objetivo do gerenciamento de incidentes é restaurar a operação do serviço o mais rápido possível.

3. Definições

Neste documento são adotadas as seguintes definições:

- **Incidente:** interrupção não planejada ou uma redução da qualidade de um serviço de TI.
- **Incidente de Segurança da Informação**: caracterizado por um evento simples ou por uma série de eventos que tenham o potencial de comprometer as operações do negócio, infringir as políticas/normas de segurança vigentes ou ameaçar a Segurança da Informação da instituição.
- **Gerenciamento de Incidentes:** 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 quando possível e que o impacto no negócio seja minimizado.
- **Operação Normal do Serviço:** operação de serviço dentro dos limites estabelecidos no ANS (Acordo de Nível de Serviço).
- **Acordo de Nível de Serviço (ANS):** acordo entre a Secretaria de Tecnologia da Informação (STI) e um cliente (unidade da Justiça Eleitoral do Estado). O acordo de nível de serviço descreve o serviço de TI, documenta metas de nível de serviço e especifica as responsabilidades da STI e do cliente.
- **Central de Serviços de TIC (CESTIC):** ponto único de contato entre a STI e os usuários. Uma central de serviço típica gerencia incidentes, requisições de serviço e também a comunicação com os usuários.
- **Suporte de 1º nível (ou grupo solucionador de 1º nível):** primeiro nível de atendimento, na hierarquia dos grupos de suporte envolvidos na resolução de incidentes.
- **Suporte de 2º nível (ou grupo solucionador de 2º nível):** segundo nível de atendimento, na hierarquia dos grupos de suporte envolvidos na resolução de incidentes. Cada nível contém especialistas com maiores habilidades, mais tempo disponível ou outros recursos necessários à solução do incidente.
- **Base de Conhecimento:** banco de dados que contém todos os registros de erros conhecidos.
- **ETIR**: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

4. Políticas e Diretrizes

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 usuários devem ter acesso a informações sobre o tratamento de incidentes reportados por ele.
- A CESTIC deve solicitar mais informações do usuário quando o chamado não dispuser de informação suficiente para o atendimento.
- O usuário deve prestar mais informações sobre os incidentes reportados por ele, quando solicitado.
- Os chamados devem ser categorizados e priorizados pela CESTIC, dentro do prazo acordado.
- A Base de Conhecimento deve ser atualizada constantemente.
- Ações corretivas, preventivas e oportunidade de melhorias no processo devem ser registradas e encaminhadas ao dono do processo.

5. Incidentes de Segurança da Informação

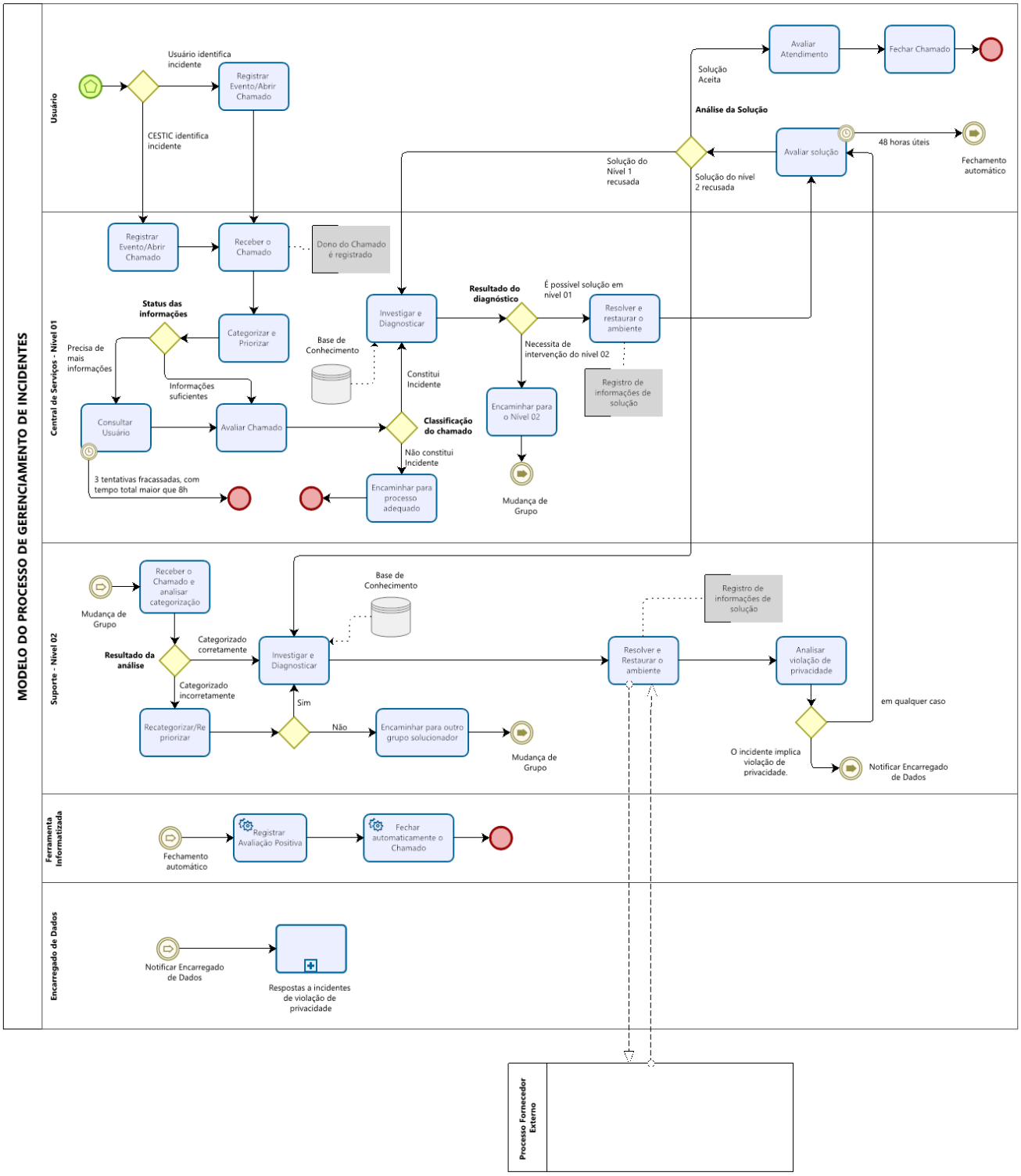
O processo de Gerenciamento de Incidentes adotado pela CESTIC no tratamento de chamados aplica-se, em sua totalidade, ao tratamento de Incidentes de Segurança da Informação, observando-se as seguintes especificidades:

- Eventos suspeitos de serem Incidentes de Segurança da informação, reportados pelos usuários ou identificados pelos operadores de Nível 1 e Nível 2, devem ser direcionados à ETIR, que atuará no processo como área de operação de Nível 2.
- A ETIR (Nível 2) avaliará os chamados encaminhados como suspeita de Incidente de Segurança da Informação. Caso se confirme a suspeita, os qualificará na CESTIC como Incidente de Segurança da Informação e adotará as providências a seu cargo, acionando, se necessário, a Comissão de Segurança da Informação do Tribunal. As informações e a solução dos chamados qualificados como Incidente de Segurança da Informação estarão restritas à ETIR.
- A ETIR (Nível 2) encerrará o chamado, informando no sistema as ações adotadas para tratamento do Incidente de Segurança da Informação.

- A ETIR (Nível 2) deverá manter em tratamento somente Incidentes de Segurança da Informação. Caso identifique incidente que não se enquadre nessa categoria, deve adotar os procedimentos de redirecionamento de chamados já previstos no fluxo do processo.
- Para efeitos de estatísticas, todos os chamados técnicos tratados/solucionados pela ETIR serão contabilizados como Incidentes de Segurança da Informação.
- Os Incidentes de Segurança da Informação deverão ser registrados em uma base de conhecimento, permitindo que as ações executadas possam ser usadas para reduzir a probabilidade ou o impacto de incidentes futuros.
- A ETIR (Nível 2) deverá definir e aplicar procedimentos para a identificação, coleta, aquisição e preservação das informações referentes aos Incidentes de Segurança da Informação, a fim de que elas possam servir como evidências.
- Em casos de Incidentes de Segurança que impliquem violação de privacidade, a ETIR deverá notificar o Encarregado de Dados e o Comitê Gestor de Proteção de Dados Pessoais do TRE/ES, que adotarão as providências a seu cargo.

6. Fluxo do Processo

A figura abaixo mostra o fluxo do processo Gerenciamento de Incidentes.



7. Descrição das principais atividades do processo

7.1. Registrar Evento/Abrir Chamado

O chamado deve ser registrado pelo usuário por meio de ferramenta informatizada, ou pela CESTIC, quando aberto por telefone ou quando o próprio operador identificar algum incidente. Incidentes podem também ser registrados automaticamente por ferramentas de monitoramento de eventos. Todos os incidentes 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.

7.2. Receber o chamado

Ação pela qual um operador de nível 1 recebe e se torna “dono do Chamado”, sendo responsável por acompanhar todas as ações desenvolvidas para solucionar a falha durante o ciclo de vida do chamado, zelar pelo cumprimento do ANS e prestar informações solicitadas pelos usuários.

7.3. Categorizar e Priorizar

Os chamados devem ser categorizados e priorizados pela CESTIC, dentro do prazo acordado. Categorizar um chamado consiste em associá-lo a um dos serviços constantes do Catálogo de Serviços.

Nesta atividade, os incidentes devem também ser priorizados, levando em consideração a urgência (quão rápido o usuário necessita que o problema seja resolvido) e o impacto causado às operações do Tribunal (p. ex., as atividades do Tribunal ou a quantidade de usuários afetados). Incidentes de maior prioridade terão precedência no atendimento.

7.4. Investigar e Diagnosticar

Durante esta atividade, o técnico (operador de 1º ou 2º nível) deverá analisar todas as informações registradas no chamado, a fim reproduzir ou diagnosticar o incidente de forma precisa. O operador poderá utilizar-se de vários meios que auxiliem na solução do incidente, dentre os quais, destacam-se:

- Base de conhecimento e chamados semelhantes;
- Procedimentos e outros documentos técnicos da organização;
- Consulta a especialistas;
- Fornecedores externos.

7.5. Encaminhar para o 2º nível

Caso não exista na Base de Conhecimento um registro com a solução para o incidente, ou o operador de 1º nível não consiga resolver o incidente de forma rápida, deverá encaminhar imediatamente o chamado para o 2º nível de suporte, zelando pelo cumprimento do ANS estabelecido para aquele tipo de serviço.

É importante que o operador da CESTIC se certifique de que o chamado possui informações suficientes para o atendimento. Caso o chamado não possua informações suficientes para o atendimento, a CESTIC deverá solicitar mais informações ao usuário.

7.6. Resolver e restaurar o ambiente

Esta atividade pode ser realizada tanto pelo operador de 1º nível, quanto pelo suporte de 2º nível, conforme mostra o fluxo do processo. Em ambos os casos, o operador (suporte de 1º ou 2º nível) deverá atuar na resolução do incidente visando restaurar o ambiente. Ao constatar a restauração, deverá registrar a solução aplicada ao incidente e informar ao usuário.

7.7. Avaliar a Solução

Tratado o incidente pela CESTIC, o usuário de TIC que demandou o suporte terá um prazo de 48 horas úteis para avaliar se a solução aplicada foi suficiente para corrigir a falha. Caso a solução seja

recusada, o chamado retornará diretamente à área técnica responsável. Caso o prazo termine sem que haja manifestação, o chamado será fechado automaticamente pela ferramenta informatizada.

7.8. Avaliar o atendimento/Fechar o chamado

Ao final de cada atendimento, o usuário do serviço avaliará o atendimento prestado e fechará o chamado. Caso não haja manifestação do usuário no prazo de 48 horas úteis, o sistema registrará uma avaliação positiva para o atendimento e o chamado será fechado.

8. Papéis e responsabilidades

Os papéis e responsabilidades dos envolvidos no processo de Gerenciamento de Incidentes são os seguintes:

8.1. Dono do Processo

- Garantir que o processo esteja adequado aos propósitos do TRE-ES 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 estejam disponíveis aos interessados;
- Garantir que o processo seja automatizado na ferramenta de Gerenciamento de Serviços do TRE-ES;
- Zelar para que o processo esteja sendo seguido conforme o especificado;
- Garantir que os envolvidos recebam os treinamentos adequados para a fiel execução do processo;
- Garantir a autoridade necessária a todos os papéis do processo.

No âmbito do TRE/ES, este papel será exercido pelo Coordenador da área responsável pela infraestrutura tecnológica e segurança cibernética.

8.2. 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 de forma otimizada;
- Garantir que os indicadores de desempenho do processo sejam atingidos;
- Registrar e informar ao Dono do Processo as sugestões de melhorias no processo e na Ferramenta Informatizada;
- Garantir que os usuários sejam mantidos informados sobre seus incidentes;
- Decidir sobre as escalações hierárquicas de incidentes;
- Garantir a inclusão e atualização dos erros conhecidos na Base de Conhecimento;
- Conduzir reuniões periódicas com a equipe de atendimento do 1º nível;
- Auxiliar os operadores na solução de incidentes.

No âmbito do TRE/ES, este papel será exercido pelo chefe da seção responsável pelo suporte em microinformática da STI.

8.3. Operador do 1º nível

- Registrar todos os incidentes reportados através de ligações telefônicas;
- Receber e realizar a categorização dos incidentes no prazo acordado no ANS;
- Buscar mais informações do usuário quando o chamado não estiver suficientemente descrito;
- Realizar o atendimento dos incidentes, utilizando pesquisa na Base de Conhecimento e documentações técnicas disponíveis;
- Apoiar na atualização dos erros conhecidos na Base de Conhecimento.

8.4. Dono do Chamado

- Acompanhar todas as ações desenvolvidas para solucionar a falha durante o ciclo de vida do chamado, cobrando as áreas responsáveis;
- Zelar pelo cumprimento do ANS;
- Prestar informações solicitadas pelos usuários;
- Comunicar ao gerente do processo situações recorrentes de descumprimento do ANS.

8.5. Operador do 2º nível

- Recategorizar os chamados categorizados de forma equivocada e comunicar os operadores de 1º nível sobre o equívoco;
- Solucionar os incidentes que não foram solucionados pelos operadores de 1º nível;
- Atualizar ou adicionar novos registros de erros conhecidos na Base de Conhecimento.

9. Indicadores de Desempenho

O Processo de Gerenciamento de Incidentes será monitorado e constantemente medido por meio de indicador(es) de desempenho inserido(s) no PDTIC do TRE/ES. Os resultados da Central serão consolidados periodicamente em relatórios publicados na página da CESTIC na Intranet. Esses relatórios têm como objetivo acompanhar a eficácia do processo, identificando tendências, falhas e oportunidades de correções, promovendo sempre a melhoria contínua. Os seguintes índices foram definidos para o Processo de Gerenciamento de Incidentes, sem prejuízo da apresentação de outros resultados que o Dono do Processo considerar pertinentes de publicação.

9.1. Percentual de incidentes fechados dentro do ANS

Descrição: percentual de incidentes que foram fechados dentro do tempo acordado.

Periodicidade: mensal

9.2. Percentual de incidentes resolvidos pelo 1º nível

Descrição: percentual de incidentes que foram resolvidos pela Central de Serviços sem a necessidade de escalação para os grupos solucionadores de 2º nível.

Periodicidade: mensal

9.3. Percentual de incidentes reabertos

Descrição: percentual de incidentes que foram solucionados pela área técnica, cuja solução não foi aceita pelo usuário final.

Periodicidade: mensal

9.4. Percentual de usuários satisfeitos com o serviço

Descrição: percentual de usuários que usaram o serviço e avaliaram positivamente o atendimento.

Periodicidade: mensal