TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO

COORDENADORIA DE INFRAESTRUTURA TECNOLÓGICA E SEGURANÇA CIBERNÉTICA

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Prática de Gestão de Incidentes

Vitória – 2025

Versão 2.2

Histórico de Versões

Versão	Data	Autor(es) / Revisor(es)	Alterações
1.0	2017	Alessandra Marques e Sandro Merçon	Criação do documento
2.0	2019	Sandro Merçon	Revisão
2.1	2022	Alessandra Marques e Sandro Merçon	Revisão
2.2	2025	Sandro Merçon	Revisão

Conteúdo

1. Objetivo

A Prática de Gestão de Incidentes tem como propósito restaurar a operação normal dos serviços de TIC o mais rapidamente possível, minimizando o impacto das interrupções sobre as atividades do Tribunal Regional Eleitoral do Espírito Santo (TRE-ES) e garantindo a continuidade do negócio.

Essa prática visa não apenas restabelecer serviços, mas também preservar o valor entregue aos usuários e à instituição, promovendo uma experiência de atendimento eficiente e transparente.

2. Escopo

Aplica-se a todos os incidentes que resultem em interrupção, degradação ou falha de qualquer serviço de TIC prestado pela Secretaria de Tecnologia da Informação (STI), constantes no Catálogo de Serviços de TIC do TRE/ES. Alguns exemplos de incidentes são: impossibilidade de enviar um email, 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.

Inclui a identificação, registro, categorização, priorização, diagnóstico, resolução e encerramento dos incidentes, bem como a comunicação contínua com os usuários durante todo o ciclo de vida do chamado.

A prática não abrange requisições de serviço (que devem seguir a Prática de Gestão de Requisições de Serviço), mudanças planejadas (que são tratadas pela Prática de Gestão de Mudanças) nem investigação da causa raiz dos incidentes (que são tratados pela Prática de Gestão de Problemas).

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.
- **Gestão de Incidentes:** prática responsável por gerenciar o ciclo de vida de todos os incidentes. A gestão 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.
- **Prática:** conjunto de recursos organizacionais — incluindo pessoas, competências, processos, tecnologias, informações e parceiros — projetado para realizar um trabalho ou alcançar um objetivo específico de gerenciamento de serviços.
- **Dono da Prática:** papel ao qual são atribuídas responsabilidades de nível estratégico dentro da Prática de Gerenciamento de Incidentes.
- **Gerente da Prática:** papel ao qual são atribuídas responsabilidades de nível tático dentro da Prática de Gerenciamento de Incidentes.
- **Operador do 1º Nível:** técnico responsável por cumprir tarefas de nível básico dentro da Prática de Gerenciamento de Incidentes.
- **Dono do Chamado:** técnico responsável por acompanhar o chamado durante todo o seu ciclo de vida.
- **Operador do 2º Nível:** técnico responsável por cumprir tarefas de nível intermediário e avançado dentro da Prática de Gerenciamento de Incidentes.

4. Diretrizes

A Prática de Gestão de Incidentes deve observar as seguintes diretrizes:

- A Central de Serviços é o ponto único de contato com os usuários e responsável pela correta categorização e priorização dos incidentes.
- Todas as ocorrências que caracterizem falha, interrupção ou degradação de um serviço devem ser registradas no sistema de gerenciamento de serviços.
- A Central de Serviços deve solicitar informações adicionais ao usuário quando o chamado não dispuser de informações suficiente para o atendimento.
- O usuário deve prestar mais informações sobre os incidentes reportados por ele, quando solicitadas.

- As informações coletadas durante o ciclo de vida do incidente devem ser documentadas integralmente, garantindo rastreabilidade e histórico.
- Todas as ações corretivas, preventivas e melhorias devem ser formalmente registradas, garantindo aprendizado organizacional.
- A experiência do usuário deve ser considerada em todas as etapas, priorizando comunicação clara e atendimento satisfatório.
- As ações de diagnóstico e resolução devem ser executadas conforme os Acordos de Nível de Serviço (ANS) estabelecidos.
- As lições aprendidas e oportunidades de melhoria identificadas durante o tratamento de incidentes devem ser registradas e encaminhadas ao Dono da Prática para avaliação no ciclo de Melhoria Contínua.
- A Prática de Gestão de Incidentes deve incorporar análise de resultados e lições aprendidas, promovendo ajustes periódicos em seus procedimentos, indicadores e fluxos, em alinhamento com o ciclo de Melhoria Contínua do ITIL 4.

5. Incidentes de Segurança da Informação

A prática de Gestão de Incidentes aplica-se, em sua totalidade, ao tratamento de Incidentes de Segurança da Informação, observando-se as seguintes especificidades:

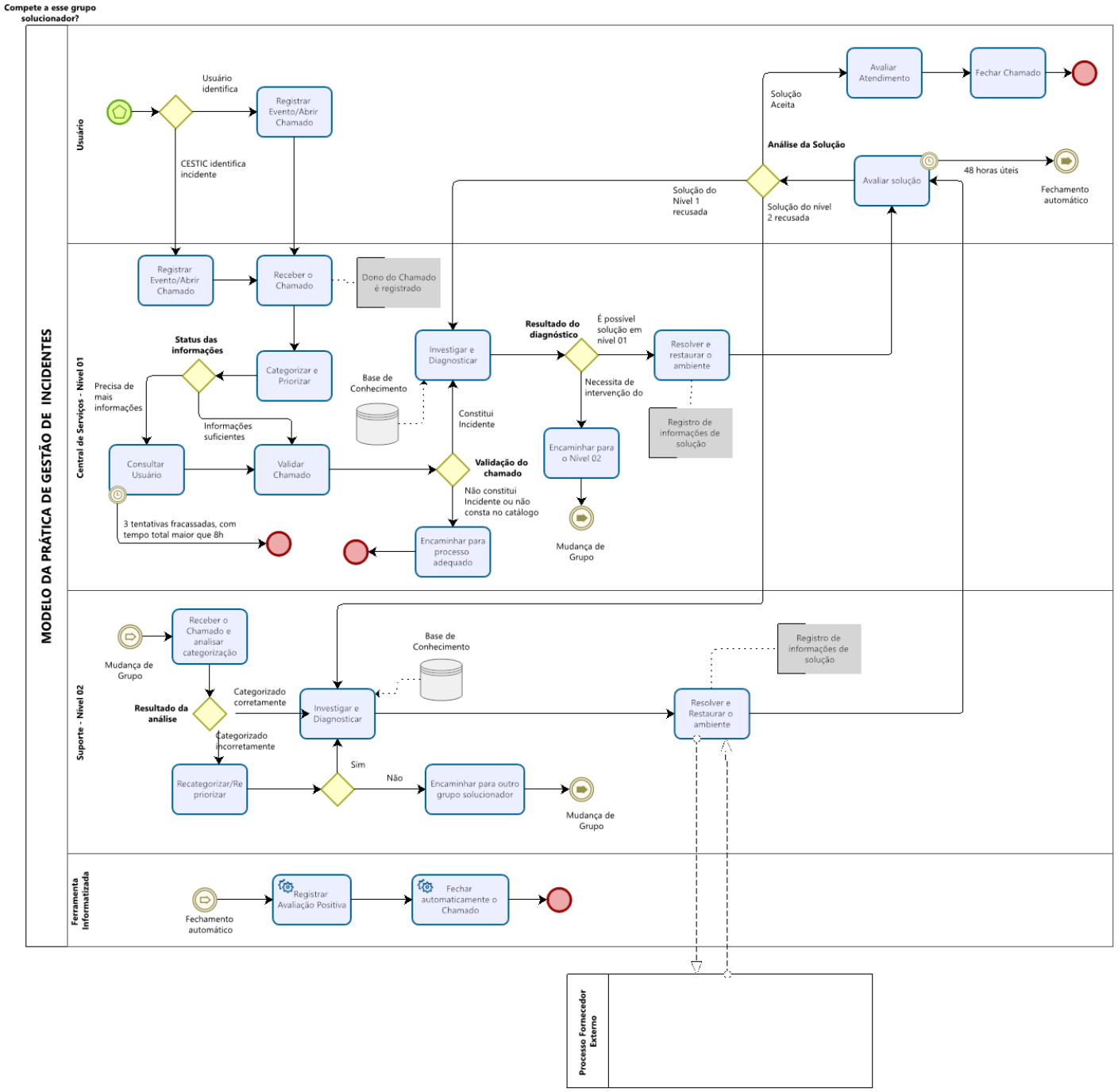
- Eventos suspeitos de serem Incidentes de Segurança da informação, reportados pelos usuários ou identificados pelos operadores de Nível 1 e Nível 2, devem ser direcionados à ETIR, que atuará como área de operação de Nível 2.
- A ETIR (Nível 2) avaliará os chamados encaminhados como suspeita de Incidente 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 da prática.
- 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 da Prática

A figura abaixo mostra o fluxo da Prática de Gestão de Incidentes.



7. Descrição das principais atividades da prática

7.1. Registrar Evento/Abrir Chamado

Os chamados para resolução de incidentes podem ser registrados:

a) Pelos usuários, através da ferramenta informatizada ou pelo telefone.
b) Pela Central de Serviços, quando um operador identificar algum incidente.

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, as requisições devem também ser priorizadas, levando em consideração:

a) **a urgência:** quão rápido o usuário necessita que a requisição seja cumprida
b) **o impacto causado às operações do Tribunal:** por exemplo, a quantidade de usuários ou atividades do Tribunal que dependem daquele cumprimento.

c) **o valor para o Negócio** – relevância estratégica ou institucional do serviço solicitado.

A prioridade final deve ser definida pela combinação desses fatores, de forma a assegurar que os recursos da TI sejam aplicados primeiro onde há maior risco ou geração de valor.

7.4. Consultar Usuário

Caso não haja informações suficientes no chamado para que ele seja atendido, o operador deve consultar o usuário a fim de obtê-las.

Devem ser realizadas no mínimo três tentativas de contato com o usuário, utilizando os canais disponíveis. As tentativas não devem ocorrer de forma consecutiva, devendo ser distribuídas ao longo de um intervalo entre 6 e 8 horas, contado a partir do primeiro contato. Todas as tentativas devem ser registradas no histórico do chamado, indicando data, horário e meio de comunicação utilizado.

7.5. Validar Chamado

O técnico irá validar se o chamado registrado corresponde efetivamente a um incidente e se está contemplado no Catálogo de Serviços de TIC.

- **Se não for um incidente:** a solicitação deverá ser imediatamente redirecionada para a Prática adequada, garantindo o tratamento adequado.
- **Se não constar no Catálogo de Serviços:** o chamado deve ser encaminhado para a Prática de Gestão do Catálogo de Serviços, a fim de avaliar sua inclusão como novo serviço ou tratá-lo conforme procedimentos internos.

Essa validação é essencial para assegurar que cada chamado seja tratado de acordo com sua natureza, evitando atrasos, inconsistências e retrabalho no atendimento.

7.6. 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.

7.7. 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.

7.8. 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.

7.9. 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, deverá indicar o motivo, podendo retornar o chamado para a Central de Serviços ou fechá-lo definitivamente. Caso o prazo termine sem que haja manifestação, o chamado será fechado automaticamente pela ferramenta informatizada, com registro de uma avaliação positiva para a solução aplicada e para o atendente.

7.10. Avaliar o atendimento/Fechar o chamado

Ao final de cada atendimento, o usuário do serviço irá indicar o seu grau de satisfação com a solução aplicada e com o atendimento prestado pela Central de Serviços. Após esse procedimento o chamado será fechado definitivamente.

8. Papéis e responsabilidades

Os papéis e responsabilidades dos envolvidos na Prática de Gestão de Incidentes são os seguintes:

8.1. Dono da Prática

- Garantir que a Prática esteja adequada aos propósitos do TRE-ES e realizar as melhorias necessárias;
- Garantir que a documentação da Prática esteja atualizada e acessível a todos os envolvidos;
- Garantir que os envolvidos sejam informados das mudanças efetuadas na Prática;
- Definir e revisar periodicamente os indicadores de desempenho utilizados para aferir a eficácia e eficiência da Prática;

- Garantir que relatórios com os indicadores de desempenho estejam disponíveis aos interessados;
- Zelar para que a Prática esteja sendo seguido conforme o especificado;
- Garantir que os envolvidos recebam os treinamentos adequados para a fiel execução da Prática;
- Garantir a autoridade necessária a todos os papéis da Prática.

No âmbito do TRE/ES, este papel será exercido pelo Coordenador de Infraestrutura Tecnológica e Segurança Cibernética**.**

8.2. Gerente da Prática

- Indicar as pessoas adequadas aos papéis definidos na Prática;
- Promover e garantir que a Prática seja seguido conforme o especificado;
- Gerenciar os recursos alocados à Prática de forma otimizada;
- Garantir que os indicadores de desempenho da Prática sejam atingidos;
- Registrar e informar ao Dono da Prática as sugestões de melhorias na Prática 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 de Gestão de Serviços de TIC e Microinformática.

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 da Prática as 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

A Prática de Gestão de Incidentes será monitorada e constantemente medida por meio de indicador(es) de desempenho inserido(s) no PETIC 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 da Prática, identificando tendências, falhas e oportunidades de correções, promovendo sempre a

melhoria contínua. Os seguintes índices foram definidos para a Prática de Gestão de Incidentes, sem prejuízo da apresentação de outros resultados que o Dono da Prática 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