TRIBUNAL DE CONTAS DO
ESTADO DE GOIÁS

Diretoria de Tecnologia da Informação (DI-TI)

Serviço de Infraestrutura e Segurança em TI (Serv-Infra TI)

PROCEDIMENTO OPERACIONAL PADRÃO (PO)

Gerir Incidentes de Segurança da Informação

Versão nº: 003

07/10/2024

LISTA DE SIGLAS

CGSI	Comitê Gestor de Segurança da Informação
DPO	Diretor de Proteção de Dados (Data Protection Officer)
LGPD	Lei Geral de Proteção de Dados
SGI	Sistema de Gestão Integrado
SGP	Sistema de Gestão e Planejamento
TCE-GO	Tribunal de Contas do Estado de Goiás
TCP	Protocolo de Controle de Transmissão
TI	Tecnologia da informação
UDP	User Datagram Protocol

SUMÁRIO

1. CADEIA DE VALOR DE PROCESSOS DE TRABALHO

1.1 Núcleo de Valor

Processo de Suporte

1.2 Macroprocesso

Tecnologia da Informação

1.3 Processo de Trabalho

Segurança da Informação

2. RESPONSABILIDADES

2.1 Dono do Processo do Trabalho

Diretoria de Tecnologia da Informação

2.2 Emitente(s) do PO

Serviço de Infraestrutura e Segurança em TI

2.3 Alcance

Este PO contempla atividades em nível institucional, ou seja, relativas a todos os setores do TCE-GO.

3. OBJETIVO

Este Procedimento Operacional Padrão (PO) tem como objetivo determinar padrões para a gestão de incidentes de segurança da informação, visando proteger a integridade, confidencialidade, disponibilidade e autenticidade dos dados organizacionais. Para tanto, visa a detecção e resposta rápida à ameaças e vulnerabilidades, minimizando impactos negativos nos sistemas e informações. Isso envolve uma resposta eficiente para limitar danos e acelerar a recuperação, além do registro detalhado de incidentes para análise e aprendizado futuros.

A gestão de incidentes também exige uma comunicação clara e transparente com as partes interessadas, internas e externas, sobre os incidentes de segurança. Essa prática mantém a transparência e fortalece a confiança.

A conformidade com normas e regulamentos é essencial, assim como a minimização de impactos financeiros e de reputação causados por incidentes de segurança. Esta abordagem ajuda a manter a resiliência e a confiança organizacional.

4. DOCUMENTOS DE REFERÊNCIA

- NBR ISO 9001:2015 - Sistema de Gestão da Qualidade;
- NBR ISO 14001:2015 - Sistema de Gestão Ambiental;
- NBR ISO/IEC 27001:2022 – Sistema de Gestão de Segurança da Informação;
- NBR ISO 37001:2017 – Sistema de Gestão Antissuborno;
- Resolução Administrativa nº 017/2024 - Dispõe sobre a Política de Segurança da Informação do Tribunal de Contas do Estado de Goiás;
- Portaria nº 57/2023 - Institui o Comitê de Segurança da Informação para o biênio 2023-2024;
- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);
- PO Gerir Atendimento de Suporte de TI.

5. DEFINIÇÕES INICIAIS

- **Comitê de Segurança da Informação:** Comitê de Segurança da Informação instituído pelo Tribunal de Contas do Estado de Goiás.

- **Usuários:** servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários, e outras pessoas que se encontrem à serviço do Tribunal de Contas do estado de Goiás, utilizando em caráter temporário os recursos tecnológicos do TCE-GO.

- **Evento de Segurança da Informação:** qualquer situação incomum identificada pelo usuário em um sistema ou serviço ou rede, que possa indicar uma possível violação da política de Segurança da Informação, da rede de computadores ou uma falha de controles de Segurança da Informação.

- **Incidente de segurança da informação:** evento de Segurança da Informação avaliado e confirmado/sob suspeita pela equipe de TI de se tratar de uma ameaça a política de Segurança da Informação, da rede de computadores ou uma falha de controles de Segurança da Informação.

- **Tratamento e Resposta de Incidentes de Segurança da Informação em Redes Computacionais:** é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

- **SOC – Security Operations Center:** é o Centro de Operações de Segurança, que presta serviços relacionados a segurança da informação.

- **Ataque:** evento de exploração de vulnerabilidades, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

- **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em um dano para um sistema ou organização.

- **Vulnerabilidade:** é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

- **Artefato malicioso:** é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores.

- **BOT:** código malicioso o qual permite que o invasor controle remotamente o computador ou dispositivo que hospeda;

- **DPO:** Diretor de Proteção de Dados, encarregado de cuidar das questões referentes à proteção dos dados dentro do Tribunal e da comunicação com as partes interessadas.

- **IP:** Protocolo da Internet (Internet Protocol): número utilizado para identificar um dispositivo de tecnologia da informação em uma rede, ou Internet;

- **LOG:** processo de registro de eventos relevantes num sistema computacional;

- **Porta:** programa de computador específico ou processo específico servindo de ponto final de comunicação em um sistema operacional hospedeiro de um outro dispositivo.

- **Scripts:** conjunto de instruções para que uma função seja executada em determinado aplicativo;

- **SLA:** Acordo de Nível de Serviço (do inglês *Service Level Agreement*);

- **SPAM:** termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;

- **Spyware:** programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;

- **Trojan:** programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário;

- **Redmine-Projetos:** sistema de gerenciamento de tarefas utilizado pela Di-TI.

- **Vírus:** programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;

- **Worm:** programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

- **Risco:** é o efeito da incerteza sobre os objetivos. Uma análise de riscos considera a probabilidade do risco se materializar (alta, média e baixa) e impacto gerado caso o risco venha a se instaurar (grande, médio, pequeno).

- **Sniffing de Rede ou Sniffing de Pacotes:** é uma técnica usada por investigadores para capturar pacotes de dados sendo transferidos através de uma rede. Esses pacotes são então registrados e analisados. As ferramentas utilizadas para esses fins são conhecidas como sniffers de rede ou, simplesmente, sniffers.

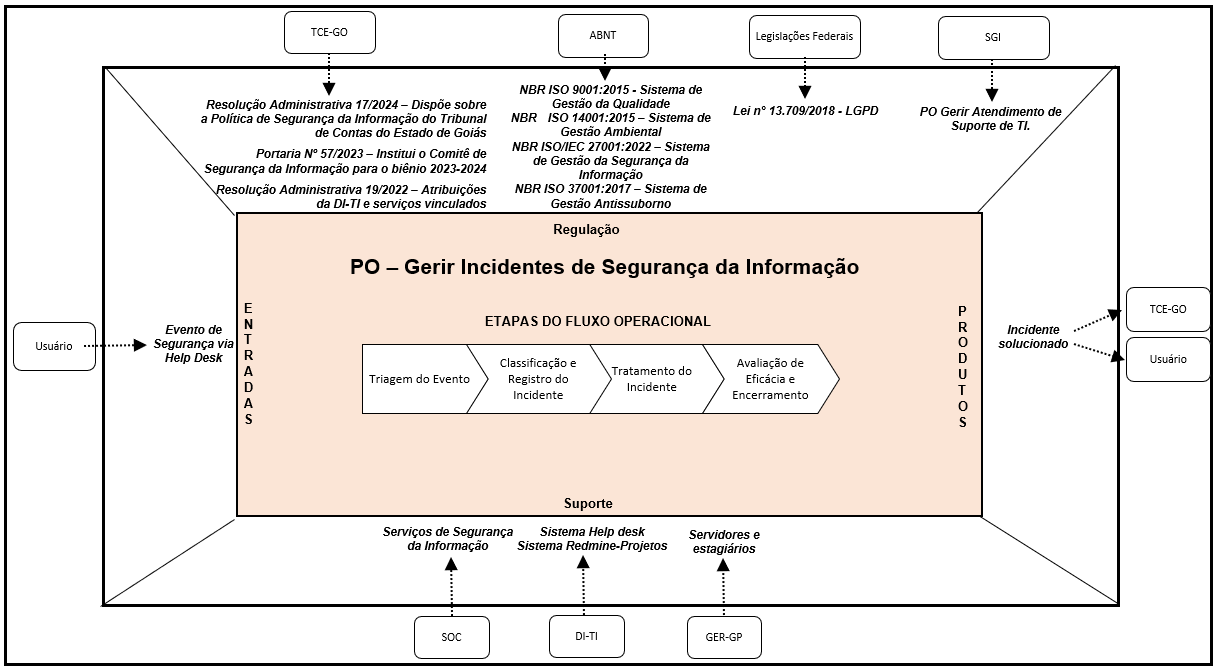
- **Parte Interessada:** qualquer indivíduo, grupo ou organização que mantenha algum tipo de interesse direto ou indireto relacionado à atuação do TCE-GO.

- **Confidencialidade:** Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

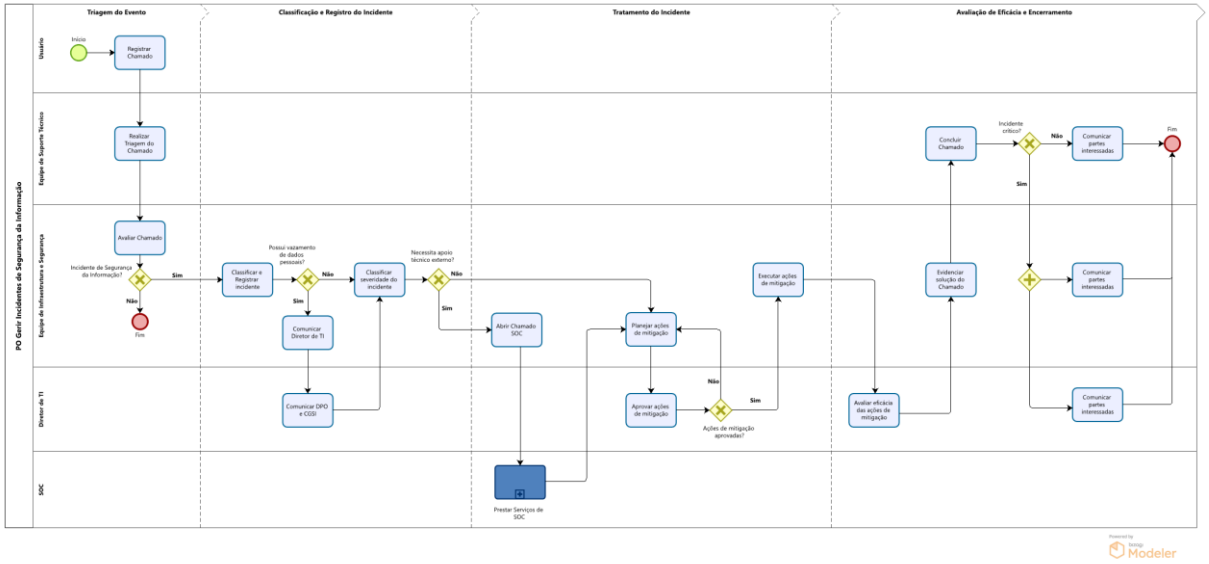
- **Integridade:** Propriedade de que a informação somente será alterada por indivíduos, entidades ou processos autorizados.

- **Disponibilidade:** Propriedade de que a informação esteja sempre disponível para indivíduos, entidades ou processos autorizados.

6. Diagrama de Escopo de Interface (DEIP)



7. Fluxo Operacional



8. Detalhamento do Fluxo Operacional

8.1 Triagem do Evento

8.1.1 Registrar Chamado

Os eventos de segurança são registrados via sistema Help Desk, conforme padrão determinado em PO Gerir Atendimento de Suporte de TI. Ao identificar um evento, o usuário abre um chamado e informa o problema ocorrido com o máximo de detalhes possível (usuário, nome da máquina, mensagem de erro), mencionando no início da descrição o termo “Evento de Segurança”.

8.1.2 Realizar Triagem do Chamado

Após registro do Evento de Segurança pelo usuário, a equipe de Suporte Técnico realiza a triagem e gera um registro de chamado no Redmine-Projetos.

8.1.3 Avaliar Chamado

A partir da geração do chamado no Redmine-Projetos, a equipe de Infraestrutura e Segurança analisa e avalia as informações para melhor entendimento do evento ocorrido e determinar se trata realmente de um incidente de segurança.

8.2 Classificação e Registro do Incidente

8.2.1 Classificar e Registrar Incidente

Confirmado o incidente de segurança pela equipe de Infraestrutura e Segurança, esta verifica previamente se houve registros de incidentes anteriores com o mesmo contexto. Caso positivo, registra a situação no descritivo da tarefa do Redmine-Projetos.

Em seguida, segue-se com a classificação do incidente no sistema Redmine-Projetos, preenchendo os campos seguintes:

Campo	Informação
Contato de origem	Descrição da origem do incidente: unidade, setor ou organização à qual dispositivo ou o processo que originou o incidente.
Registro do tempo	Registro do tempo da ocorrência do incidente considerando a data e hora na qual o incidente foi identificado.
Descrição	Breve descrição do incidente, tais como tipo do ataque, motivação aparente, ou outras características relevantes.
Classificação Tipo de incidente	Cabe ao analista de infraestrutura e segurança realizar a investigação do tipo de incidente promovendo assim sua classificação: • Ativo com vulnerabilidade conhecida; • Ativo com software desatualizado; • Conteúdo abusivo: spam, assédio, etc.; • Código malicioso: bot, worm, vírus, trojan, spyware, scripts; • Erro de sistema; • Prospecção por informações: varredura, sniffing, engenharia social; • Tentativa de intrusão: tentativa de exploração de vulnerabilidades, tentativa de acesso lógico; • Intrusão: acesso lógico indesejável, comprometimento de conta de usuário, comprometimento de aplicação; • Indisponibilidade de serviço ou informação: negação de Serviço, sabotagem; • Segurança da informação: acesso não-autorizado à informação, modificação não autorizada da informação;

	• Fraude: violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não-autorizada; • Outros: incidente não categorizado.

8.2.2 Comunicar Diretor de TI

Caso o incidente envolva vazamento de dados pessoais, a Equipe de Infraestrutura e Segurança deve informar imediatamente o Diretor de TI.

8.2.3 Comunicar DPO e CSI

Após informado sobre incidente com vazamento de dados pessoais, o Diretor de TI deve comunicar o DPO e o Comitê de Segurança da Informação.

8.2.4 Classificar Severidade do incidente

A severidade do incidente define uma ordem de atendimento dos incidentes de acordo com a urgência de tratamento e o impacto nas áreas de negócio do TCE-GO.

A equipe de Infraestrutura e Segurança classifica a criticidade do incidente sempre observando o art. 48 da LGPD:

- **Alto (Impacto Grave):** incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre a organização. Incidentes de alta criticidade devem ser imediatamente comunicados a alta direção, para acionamento das partes interessadas;
- **Médio (Impacto Significativo):** incidente que afeta sistemas ou informações não críticas, sem impacto negativo à organização;
- **Baixo (Impacto Mínimo):** possível incidente, sistemas não críticos; investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

Nota: o nível das ações de investigação dos incidentes depende da existência de prejuízo evidente e da capacidade operacional da equipe. Incidentes que resultem em prejuízos significativos ou que comprometam a operação dos sistemas tem prioridade máxima. A capacidade operacional da equipe é considerada para determinar a profundidade e a extensão das investigações, garantindo que os recursos sejam utilizados de forma eficiente e eficaz.

8.3 Tratamento do Incidente

8.3.1 Abrir Chamado SOC (Centro de Operações de Segurança)

Havendo necessidade de apoio técnico externo, a equipe de Infraestrutura e Segurança abre um chamado em sistema específico da empresa fornecedora de serviços de SOC (Centro de Operações de Segurança).

8.3.2 Prestar Serviços de SOC

A empresa prestadora de serviços de SOC atua como executora ou consultora, dependendo do tipo de incidente, sendo que os serviços atualmente contratados pelo TCE-GO são:

- Serviço Gerenciado de Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança;
- Serviço de Operações e Resposta as Requisições (Firewall e Antivírus);
- Serviço de Gestão de Vulnerabilidades.

8.3.3 Planejar ações de mitigação

A equipe de Infraestrutura e Segurança realiza a propositura de ações para tratamento do incidente, de forma a evitar que os danos e impactos aumentem com o passar do tempo, buscando a erradicação da causa raiz do incidente e recuperação dos danos avariados. Além disso, as ações propostas devem permitir o reestabelecimento do sistema ou serviço, ainda que parcialmente, via solução de contorno ou resolução da causa do incidente.

As propostas de solução são encaminhadas para aprovação do Diretor de TI, o qual analisa as propostas, aprova ou solicita melhorias.

As ações são registradas no Redmine-Projetos.

8.3.4 Aprovar ações de mitigação

O Diretor de TI avalia as ações de mitigação propostas, e caso aprovado, encaminha para execução das ações. Caso reprovado, retorna para a Equipe de Infraestrutura e Segurança para realizar adequações, sendo ambas as ações registradas no Redmine-Projetos.

8.3.5 Executar ações de mitigação

A equipe de Infraestrutura e Segurança deve realizar as configurações e/ou modificações necessárias para conter o incidente, executando as ações aprovadas. Com foco na contenção do incidente de maneira a atenuar os danos e evitar que outros recursos sejam comprometidos, deve:

I. Desconectar o sistema comprometido ou isolar a rede afetada;

II. Desativar o sistema para evitar maiores perdas quando há perda ou roubo de informações durante o ataque;

III. Alterar políticas de roteamento dos equipamentos de rede ou bloquear padrões de tráfego, interrompendo o fluxo malicioso;

IV. Desabilitar serviços vulneráveis, inibindo comprometimento de outros sistemas e demais ações aprovadas pelo Diretor de TI.

No tocante à erradicação das causas do incidente, removendo todos os eventos relacionados:

V. Garantir que as causas do incidente foram removidas, assim como todas as atividades e arquivos associados ao incidente;

VI. Assegurar a remoção de todos os métodos de acesso utilizados pelo atacante: novas contas de acesso; backdoors e, se aplicável, acesso físico ao sistema comprometido, etc.

Quanto à recuperação do sistema ao seu estado normal ou parcial:

VII. Restaurar a integridade do sistema;

VIII. Garantir que o sistema foi recuperado corretamente e que as funcionalidades estejam ativas;

IX. Implementar medidas de segurança para evitar novos comprometimentos;

X. Restaurar o último e íntegro backup completo armazenado.

8.4 Avaliação de Eficácia e Encerramento

8.4.1 Avaliar eficácia das ações de mitigação

O Diretor de TI deve verificar se as medidas aplicadas foram efetivas em prol da mitigação da causa raiz do incidente e de seu efetivo controle para novos eventos, considerando o mesmo cenário.

8.4.2 Evidenciar solução do chamado

Cabe a equipe de Infraestrutura e Segurança evidenciar a solução do chamado no Redmine-Projetos, indicando sua conclusão. Deve-se incluir as evidências tanto do incidente quanto das ações implementadas para sua solução, garantindo a rastreabilidade do evento (exemplo: print das ações executadas durante o atendimento do chamado).

8.4.3 Concluir Chamado

Cabe a equipe de Suporte Técnico concluir o chamado no Help Desk.

8.4.4 Comunicar Partes Interessadas

A comunicação das partes interessadas é realizada ao usuário com a conclusão do chamado no Help Desk pela equipe de Suporte Técnico, e dependendo da situação (tipo de incidente e sua criticidade), outros interessados também podem ser comunicados pela equipe de Infraestrutura e Segurança e o Diretor de TI.

9. Indicadores

9.1 Indicadores de Verificação

Não mapeado

9.2 Indicadores de Controle

Nome	Descrição	Forma de cálculo
Percentual de incidentes de informação tratados	Mostrar o percentual de incidentes de informação tratados dentre os identificados (aplicado a incidentes com criticidade alta e média)	$\frac{\sum \ Incidentes\ de\ Informação\ Tratados}{\sum \ Incidentes\ de\ Informação\ Identificados}$

10. Controle de Registros

Nome do Registro / Código	Armazenamento e Preservação	Distribuição e Acesso*	Recuperação**	Retenção e Disposição
Chamado	Sistema de Help-Desk	Distribuição por meio de sistema eletrônico disponível no portal do TCE-GO com acesso controlado por senha da rede corporativa.	Backup	Tempo indeterminado
Registro de Ocorrência	Sistema Informatizado Redmine-Projetos)	Distribuição por meio de sistema eletrônico disponível no portal do TCE-GO com acesso controlado por senha da rede corporativa.	Backup	Tempo indeterminado

*A distribuição e o acesso a sistemas eletrônicos do TCE-GO são regidos pelas diretrizes e normas concernentes ao Sistema de Gestão da Segurança da Informação.

** A recuperação de informações eletrônicas custodiadas pelo TCE-GO é regida pelas diretrizes e normas concernentes ao Sistema de Gestão da Segurança da Informação.

11. Anexos

Não se aplica.

12. Elaboração, Revisão e Aprovação

PO - Gestão de Incidentes de Segurança da Informação		
Responsável por	***Nome***	***Função***
Elaboração	Leandro dos Santos	Chefe do Serviço de Infraestrutura e Segurança em TI
Revisão/Aprovação	Licardino Siqueira Pires	Diretor de Tecnologia da Informação

Controle de Qualidade	Fabrício Borges dos Santos	Chefe do Serviço de Gestão da Melhoria Contínua
Controle de Versionamento		
Versão anterior: nº 002 de 05/08/2024	Versão atual: nº 003 de 07/10/2024	Próxima revisão programada: 07/10/2027