TRIBUNAL DE CONTAS DO
ESTADO DE GOIÁS

Diretoria de Tecnologia da Informação

Serviço de Infraestrutura e Segurança em TI

PROCEDIMENTO OPERACIONAL PADRÃO (PO)

Gerir Vulnerabilidades

Versão nº: 000

30/10/2023

LISTA DE SIGLAS

LGPD	Lei Geral de Proteção de Dados
SGI	Sistema de Gestão Integrado
SGP	Sistema de Gestão e Planejamento
SOC	Centro de Operações de Segurança
TCE-GO	Tribunal de Contas do Estado de Goiás
TI	Tecnologia da Informação

SUMÁRIO

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 de atuação do TCE-GO.

3. Objetivo

Este Procedimento Operacional Padrão (PO) tem como objetivo identificar, avaliar e mitigar potenciais fraquezas em sistemas, redes e softwares. Visa reduzir riscos de ataques cibernéticos ao priorizar correções, melhorando a postura de segurança. Ao manter inventários atualizados, realizar testes regulares e implementar patches, busca-se garantir a integridade, disponibilidade e confidencialidade das informações, fortalecendo a resiliência organizacional contra ameaças digitais.

4. Documentos de Referência

- NBR ISO/IEC 9001:2015 – Sistema de Gestão da Qualidade;
- NBR ISO/IEC 14001:2015 – Sistema de Gestão Ambiental;
- NBR ISO/IEC 27001:2022 – Sistema de Gestão de Segurança da Informação;
- Resolução Administrativa nº 011/2022 – TCE/GO – Dispõe sobre as diretrizes e normas gerais para Gestão da Segurança da Informação do Tribunal de Contas do Estado de Goiás;

- Resolução Administrativa nº 019/2022 – TCE/GO – Atribuições da DI-TI e serviços vinculados;
- Portaria nº 57/2023 – TCE/GO – Institui o Comitê de Gestão da Segurança da Informação para o biênio 2023-2024;
- Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD.

5. Definições Iniciais

- **Comitê Gestor de Segurança da Informação:** Comitê de Gestão da Segurança da Informação instituído pelo Tribunal de Contas do Estado de Goiás;

- **SOC:** do inglês *Security Operations Center*, é o Centro de Operações de Segurança contratado pelo TCE-GO;

- **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;

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

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

- **URL:** *Uniform Resource Locator* é um endereço que identifica a localização única de um recurso na internet, como um site, arquivo ou serviço;

- **Scan de vulnerabilidade:** processo automatizado que examina sistemas de computador, redes ou aplicativos em busca de fraquezas de segurança. Ele identifica potenciais brechas, como falhas de configuração ou software desatualizado, ajudando a prevenir possíveis ataques cibernéticos;

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

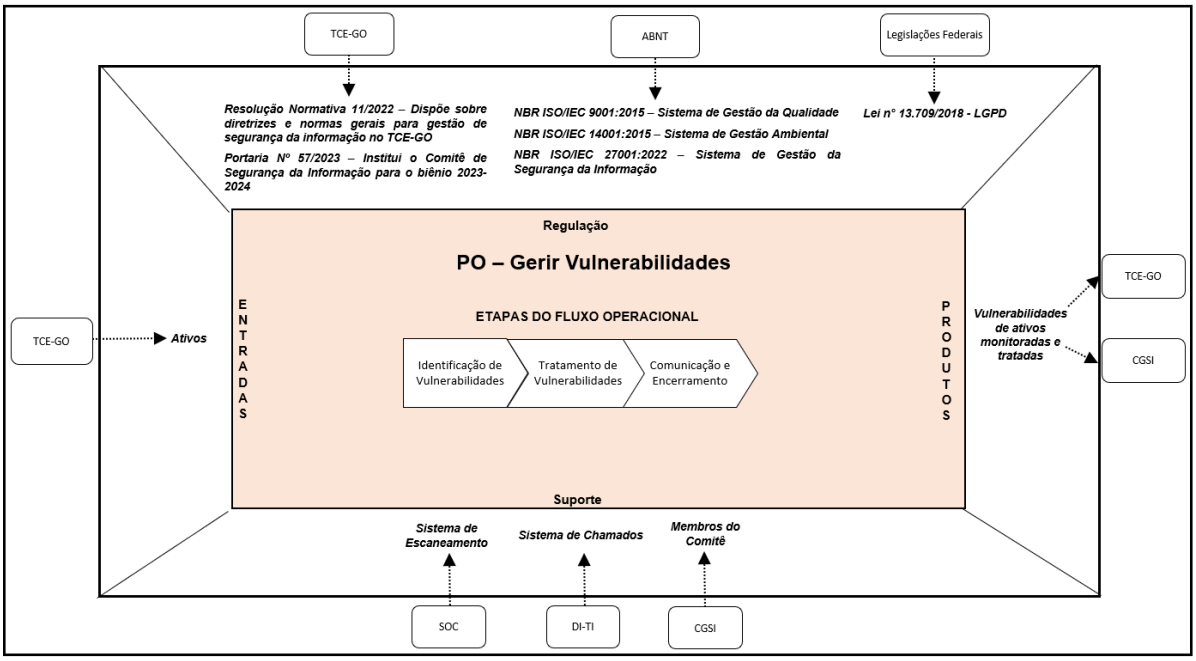
- **Risco:** combinação entre probabilidade de um evento (chance de ocorrer) e suas consequências (impacto que causaria se ele acontecesse). Como exemplo: a chance de uma ameaça explorar uma vulnerabilidade e causar um dano a um ativo de informação, às informações ou à Organização;

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

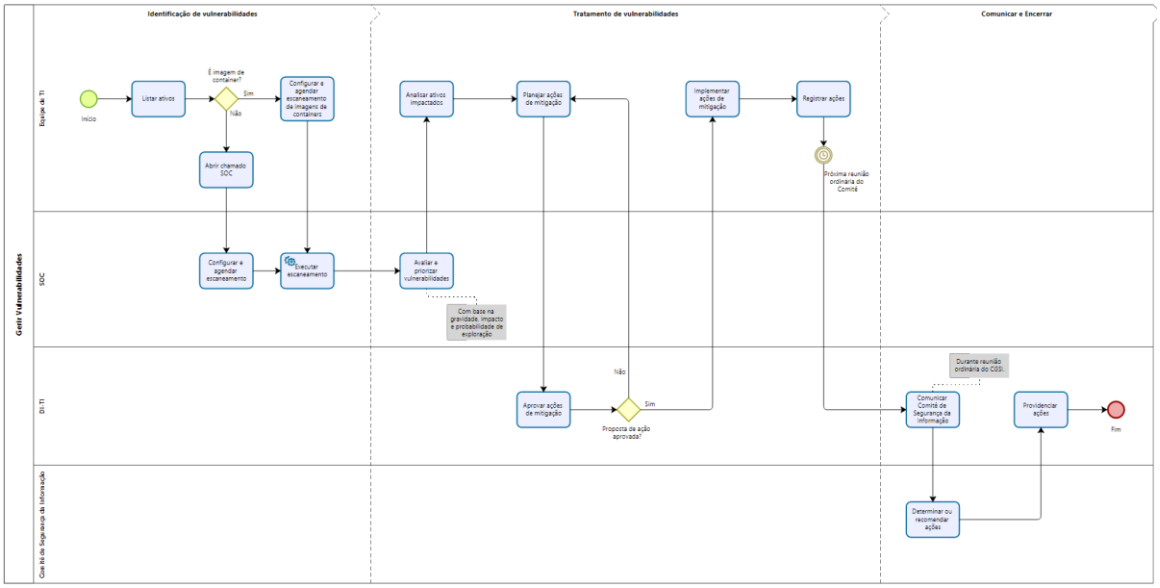
- **Integridade:** Propriedade de que a informação somente será alterada por indivíduos, entidades ou processos autorizados;

- **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. 

9. Detalhamento do Fluxo Operacional

9.1 Identificação de Vulnerabilidades

9.1.1 Listar Ativos

A equipe de TI deve listar os ativos que serão escaneados pela ferramenta Tenable em busca de vulnerabilidades. Os ativos poderão ser listados individualmente (Exemplos: URL do sistema, imagem de container, IP do servidor) ou via faixas de endereços IP, indicando o tipo de scan (webapps, desktops, servidores, imagens de containers) e a periodicidade.

9.1.2 Configurar e agendar escaneamento de imagens de containers

No caso de imagens de containers, a equipe de TI deve configurar o script e o agendamento de execução do scan de vulnerabilidades.

9.1.3 Abrir chamado SOC

Caso não seja scan de imagens de containers, um chamado é aberto para o Centro de Operações de Segurança (SOC) informando a lista de ativos e os dados para agendamento.

9.1.4 Configurar e agendar escaneamento

O SOC deverá configurar e agendar na ferramenta de scan de vulnerabilidades conforme dados repassados via chamado.

9.1.5 Executar escaneamento

Os scans de vulnerabilidades são executados automática e periodicamente e os resultados ficam disponíveis no console do sistema.

9.2 Tratamento de vulnerabilidades

9.2.1 Avaliar e priorizar vulnerabilidades

O SOC avalia mensalmente as vulnerabilidades encontradas e informa através de relatório uma sugestão de priorização com base na gravidade, impacto e probabilidade de exploração de cada vulnerabilidade encontrada.

9.2.2 Analisar ativos impactados

A equipe de TI analisa os ativos impactados subsidiada pelo relatório do SOC e pelos dados disponíveis na ferramenta Tenable. A análise é focada em determinar a priorização final para as ações de mitigação.

9.2.3 Planejar ações de mitigação

A equipe de TI faz o planejamento das ações de mitigação que passarão por aprovação da Diretoria de TI.

9.2.4 Aprovar ações de mitigação

A Diretoria de TI aprova o planejamento das ações de mitigação que serão implementadas pela equipe de TI. Caso o planejamento não seja aprovado, este será retornado para ajustes.

9.2.5 Implementar ações de mitigação

A equipe de TI implementa as ações de mitigação conforme o planejamento aprovado.

Nota1: Qualquer intercorrência deve ser devidamente registrada.

9.2.6 Registrar ações

Todas as ações de mitigação, resultados e observações devem ser devidamente registradas em ferramenta específica.

9.3 Comunicar e encerrar

9.3.1 Comunicar Comitê de Segurança da Informação

Nas reuniões ordinárias do Comitê de Segurança da Informação, a Diretoria de TI relata as ações executadas e os resultados obtidos, bem como possíveis intercorrências que não tenham sido tratadas.

9.3.2 Determinar ou recomendar ações

O Comitê de Segurança da Informação determina ou recomenda ações relacionadas à gestão e tratamento de vulnerabilidades.

9.3.3 Providenciar ações

A DI-TI providencia as ações que porventura sejam indicadas pelo Comitê de Segurança da Informação.

10. Indicadores

10.1 Indicadores de Verificação

Não mapeados.

10.2 Indicadores de Controle

Nome	Descrição	Forma de cálculo
Percentual de vulnerabilidades tratadas no período.	Mostra o percentual de vulnerabilidades tratadas dentre as identificadas no período.	$\frac{\sum \ Vulnerabilidades\ Tratadas}{\sum \ Vulnerabilidades\ Identificadas}$

11. Controle de Registros

Nome do Registro / Código	Armazenamento e Preservação	Distribuição e Acesso*	Recuperação**	Retenção e Disposição
Planilha PIQ	Drive	Distribuição por compartilhamento controlado por senha corporativa	Backup	Tempo indeterminado
Chamado SOC	Portal de Atendimento	Distribuição por meio de sistema eletrônico disponível via portal com acesso controlado por senha.	Backup	Tempo indeterminado
Registro de Ações	Sistema Informatizado Redmine	Distribuição por meio de sistema eletrônico disponível via portal 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.

12. Anexos

Não se aplica.

13. Elaboração, Revisão e Aprovação

PO – Gerir Vulnerabilidades		
Diretoria de Tecnologia da Informação - DI-TI		
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

Datas das Versões do PO		
Versão anterior: não se aplica.	Versão atual: n. 000 de 30/10/2023.	Próxima Revisão Programada: 30/10/2025