TRIBUNAL DE CONTAS DO
ESTADO DE GOIÁS

Diretoria de Tecnologia da Informação (DI-TI)

PROCEDIMENTO OPERACIONAL PADRÃO (PO)

Gerir Ativos de Tecnologia da Informação

Versão nº: 004

10/11/2023

LISTA DE SIGLAS

CID	Confidencialidade, Integridade e Disponibilidade
DI-PLAN	Diretoria de Governança, Planejamento e Gestão
DI-TI	Diretoria de Tecnologia da Informação
PO	Procedimento Operacional Padrão
SGI	Sistema de Gestão Integrado
SGP	Sistema de Gestão e Planejamento
TCE-GO	Tribunal de Contas do Estado de Goiás

SUMÁRIO

1. Cadeia de Valor de Processos de Trabalho

1.1 Núcleo de Valor

Processo de Suporte (NPS)

1.2 Macroprocesso

Tecnologia da Informação

1.3 Processo de Trabalho

Gestão da Segurança da Informação

2. Responsabilidades

2.1 Dono do Processo do Trabalho

Diretoria de Tecnologia da Informação

2.2 Emitente do PO

Diretoria de Tecnologia da Informação

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 PO tem como objetivo padronizar a gestão dos ativos de tecnologia da informação no âmbito do TCE-GO, identicando e classificando-os quanto ao tipos de ativo, responsabilidade e grau de classificação da informação, permitindo assim a determinação de controles e diretrizes para alcançar e manter sua adequada proteção e conformidade com os requisitos legais e contratuais. A abordagem adotada contempla a análise de ameaças e vulnerabilidades, desdobradas em consequências, probabilidades e classificação do nível do risco.

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
- NBR ISO/IEC 27002:2022 – Código de Prática para Controles de Segurança da Informação
- NBR ISO/IEC 27005:2019 – Gestão de Riscos de Segurança da Informação

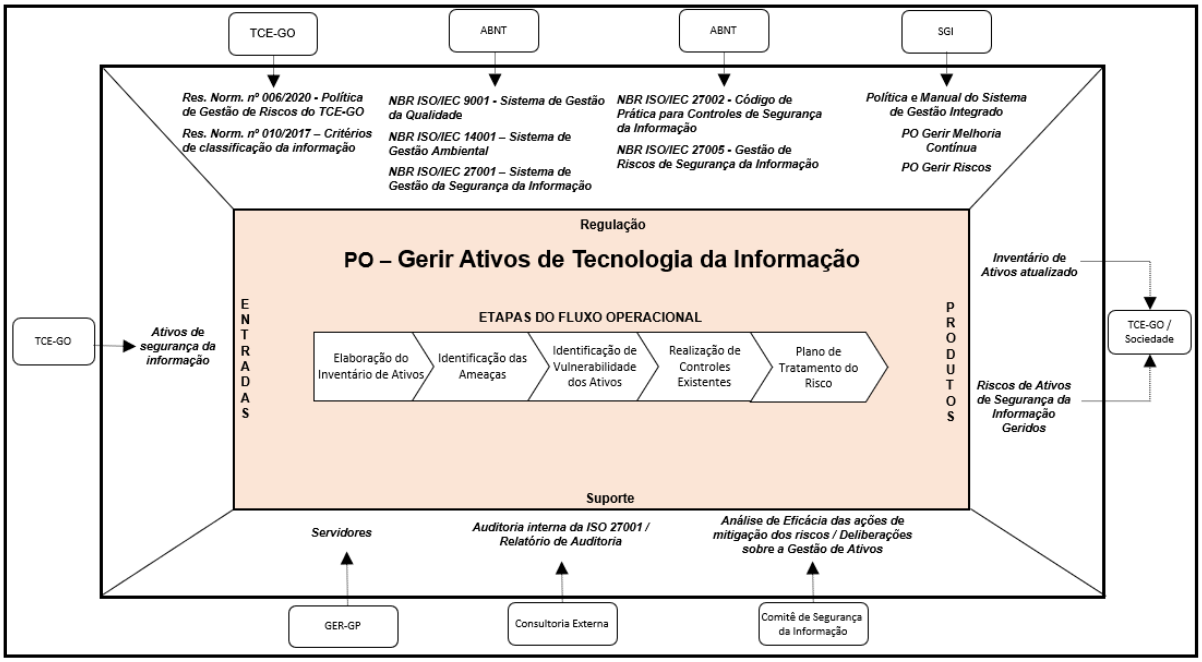
- Res. Norm. nº 006/2020 – Política de Gestão de Riscos do TCE-GO
- Res. Norm. nº 010/2017 – Dispõe sobre os critérios para promover a classificação das informações confidenciais produzidas ou custodiadas pelo Tribunal de Contas doEstado de Goiás
- Política e Manual do Sistema de Gestão Integrado (SGI)
- PO Gerir Riscos do TCE-GO

5. Definições Iniciais

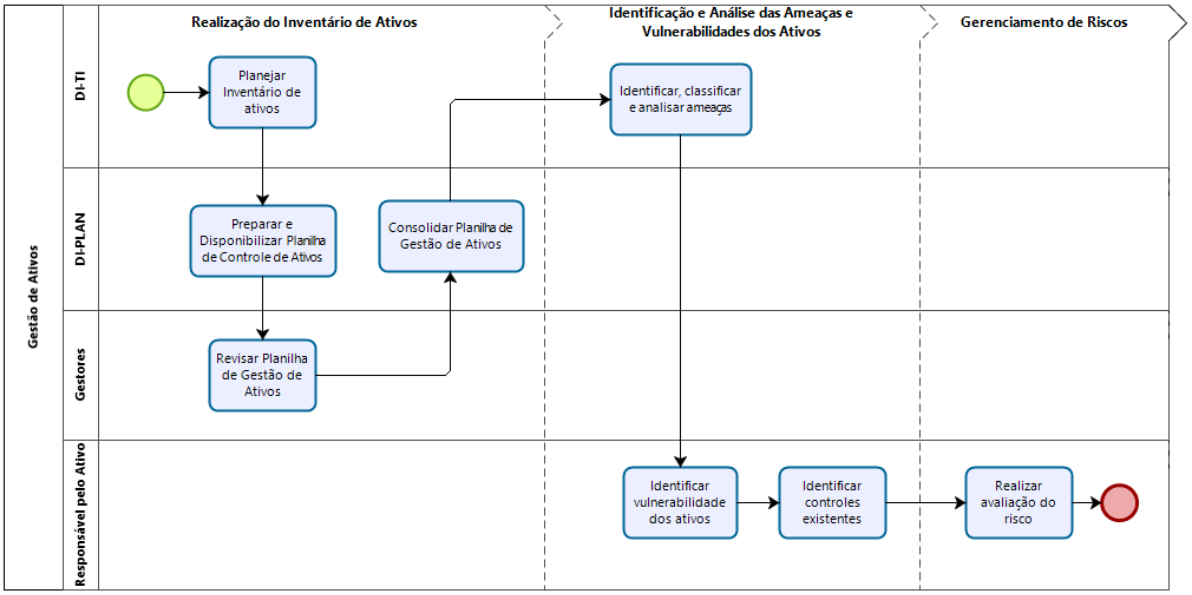
- **Disponibilidade:** propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.
- **Confidencialidade:** propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.
- **Integridade:** propriedade de salvaguarda da exatidão e completeza de ativos.
- **Autenticidade:** garantia que o emissor de determinada informação seja realmente quem alega ser, assegurando que a mensagem é realmente proveniente da fonte declarada. Ou seja, ela garante a identidade, de forma inequívoca, do remetente da informação.
- **Não Repúdio ou Irrefutabilidade:** relacionado à garantia da impossibilidade de o emissor negar a autoria de determinada mensagem ou transação.
- **Ativo:** Informação, produto ou serviço que tenha valor para a organização.
- **Responsável pelo Ativo:** também conhecido como proprietário do ativo e responsável pelo risco de segurança da informação, o qual é responsável pela identificação de ativos sob sua responsabilidade com apoio da Diretoria de Tecnologia da Informação, permitindo assim sua devida classificação quanto ao tipo do ativo, grau de confidencialidade, considerando suas ameaças e vulnerabilidades e avaliando o risco quanto ao grau de significância.
- **Dono do Processo de Trabalho:** é o responsável por realizar a gestão, garantir o padrão de desempenho estabelecido e identificar oportunidades de melhoria que permitam a alavancagem do desempenho para o processo de trabalho. No TCE-GO, são considerados Donos de Processo de Trabalho os responsáveis por Unidades Organizacionais ligadas diretamente à Presidência ou ao Plenário.
- **Proprietário:** uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. Isso não significa que a pessoa tenha qualquer direito de propriedade pelo ativo.
- **Tipos de Ativos:** Ativos de Informação (base de dados de arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, planos de continuidade do negócio, plano de recuperação de desastres, trilhas de auditoria, procedimentos de suporte ou operação e informações armazenadas. Ativos de software: (aplicativos, sistemas, ferramentas de desenvolvimento e utilitários). Ativos físicos: (equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos). Ativos de Serviços: (serviços de computação e comunicações, utilidades gerais, por exemplo aquecimento, iluminação, eletricidade e refrigeração). Ativos de Pessoas (e suas qualificações, habilidades e experiências). Ativos Intangíveis: (reputação e a imagem da organização).
- **Risco:** efeito da incerteza nos objetivos.
- **Ameaça:** causa potencial de um incidente de segurança da informação.

- **Vulnerabilidade:** fraqueza de um ativo ou controle.
- **Probabilidade:** chance de algo acontecer.
- **Consequência:** resultado de um evento que afeta os objetivos/controles.
- **Nível do Risco:** significância de um risco, expressa em termos de combinação das consequências e de suas probabilidades.
- **Risco Residual:** risco remanescente após tratamento aplicado.
- **Avaliação de Riscos:** processo de comparação dos resultados da analise de riscos, determinando se sua significância é aceitável ou tolerável para o sistema de segurança da informação.
- **Aceitação do risco:** decisão consciente de assumir um risco específico.

6. Diagrama de Escopo de Interface (DEIP)



7. Fluxo Operacional



O Fluxograma deste PO encontra-se disponível no seguinte endereço eletrônico: https://portal.tce.go.gov.br/informacao-documentada.

8. Detalhamento do Fluxo Operacional

8.1 Realização do Inventário de Ativos

8.1.1 Planejar Inventário de Ativos

A realização do Inventário de Ativos deve ocorrer, minimamente, a cada dois anos, ou sempre que forem identificados incidentes de segurança da informação e mudanças estratégicas e operacionais no TCE-GO. Nessas ocasiões, a equipe de TI juntamente com a equipe da DI-PLAN planejam a execução do inventário e a orientação das áreas que compõem o TCE-GO, abrindo no SGP o espaço de colaboração das áreas para revisão do Inventário de Ativos.

O inventário é criado a partir dos registros operacionais descritos por meio dos Procedimentos Operacionais das unidades do TCE-GO (seção 10 – Controle de Registros), que preveem informações como o local de acesso, armazenamento a forma de recuperação dos registros, permitindo a identificação e classificação de cada ativo e suas características mínimas a serem monitoradas**.**

8.1.2 Preparar e Disponibilizar Planilha de Controle de Ativos

Cabe a DI-PLAN disponibilizar, via SGP, a Planilha de Gestão de Ativos (Anexo I), para revisão das áreas do TCE-GO, bem como orientar as áreas quanto ao objetivo de realização desta atividade, o cronograma de execução e a forma de revisão e preenchimento da Planilha. Revisar Planilha de Gestão de Ativos

Os gestores de cada área, em conjunto com suas equipes, devem revisar as informações dos ativos inerentes aos seus processos operacionais descritos na Planilha de Gestão de Ativos, na seção “Identificação dos Ativos”, conforme especificado pelo Quadro 1.

Quadro 1 – Planilha de Gestão de Ativos (seção “Identificação dos Ativos”)

COLUNA	DESCRIÇÃO
Ativo	Nome do ativo conforme descrito no PO correspondente.
Classificação	Classificação, por tipo de ativo, a seguir: • **Ativos de Informação:** Considerados um conjunto de conhecimento organizado e gerenciado como uma entidade única. De forma geral, tudo o que for uma informação que tenha relação com o funcionamento no dia a dia passa a ser um ativo com importância a ser protegido. • **Ativos de Software:** Compreende todos os programas que contribuem para a operação do sistema de processamento de dados em rede do TCE Goiás. • **Ativos Físicos:** Esta definição engloba ativos físicos, como equipamentos móveis, ferramentas, máquinas (hardware), estoques e infraestruturas, ou seja, Bens Patrimoniados, mas também ativos imateriais, como direitos de autor ou propriedade intelectual.

	• **Ativos de Serviços:** Considerado qualquer componente necessário para a entrega de um serviço, e contribui para agregar valor na execução dos serviços do TCE Goiás. **Ativos de Pessoas:** São as pessoas, com suas habilidades e experiências que agregam serviço e informações para o TCE Goiás. **Ativos de Intangíveis/Organização:** Os ativos intangíveis descrevem a estrutura da organização, compreendendo as hierarquias de pessoas voltadas para a execução de uma tarefa e os procedimentos que controlam essas hierarquias e seus devidos papeisde trabalho.
Responsável pelo ativo	Área / sub-área responsável pelo ativo (emitente do procedimento operacional vinculado ao ativo).
Localidade	Aponta a localidade (sistema eletrônico ou localização física) onde se encontra o ativo operado pela área (conforme descrição do PO corresponente).
Grau de Confidencialidade	A classificação da informação quanto ao grau de confidencialidade é dada de acordo com o art. 3º da Res. Normativa 010/2017, a qual classifica os ativos como: • **Informação Reservada:** a informação imprescindível à segurança da sociedade ou do Estado e cuja divulgação ou acesso irrestrito possam: I - Pôr em risco a vida, a segurança ou a saúde da população; II - Prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico estadual; III - Pôr em risco a segurança de instituições ou de autoridades estaduais, nacionais ou estrangeiras e seus familiares; ou IV - Comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações. • **Informação pessoal:** a informação referente à intimidade, vida privada, honra e imagem da pessoa, bem como às liberdades e garantias individuais. • **Informação sigilosa:** a informação enquadrada nas hipóteses, previstas na legislação, de sigilo fiscal, bancário, de operações e serviços no mercado de capitais,comercial, profissional, industrial, segredo de justiça e relativo a denúncias. • **Informação pública:** a informação consiste num patrimônio cultural de uso comum da sociedade e de propriedade das entidades/instituições públicas da administração centralizada, das autarquias e das fundações públicas.
Procedimento Operacional	Procedimento Operacional ao qual o ativo está vinculado.
Processo de Trabalho	Processo de Trabalho ao qual o Procedimento Operacional está vinculado, conforme matriz da Cadeia de Valor do TCE-GO.

Versão	Número e data da versão do Procedimento Operacional vinculado ao ativo.
Dono do Processo de Trabalho	Área do TCE-GO responsável pelo Processo de Trabalho relacionado ao ativo.
Núcleo	Núcleo de Processo (Finalístico, de Suporte ou de Gestão) relacionado ao Processo de Trabalho.

Após a finalização da revisão, cada área responsável deve inserir a Planilha de Gestão de Ativos no módulo correspondente do SGP, conforme prazo definido no cronograma.

Nota 1: Cada área do TCE-GO possui a responsabilidade sobre os ativos que estão sob sua gestão, no que tange a sua produção, desenvolvimento, manutenção, utilização e segurança, conforme apropriado, tendo como principais responsabilidades:

- Assegurar que os ativos sejam inventariados;
- Assegurar que os ativos sejam adequadamente classificados e protegidos;
- Definir e analisar periodicamente as classificações e restrições de acesso aos ativos, levando em conta as políticas de controles de acesso aplicadas;
- Assegurar o adequado tratamento quando um ativo é excluído ou destruído.

Nota 2: Em sistemas de informação complexos, pode ser útil definir grupos de ativos que atuem juntos para fornecer um serviço particular. Neste caso, o proprietário deste serviço é responsável por sua entrega, incluindo sua operação.

8.1.4 Consolidar Planilha de Gestão de Ativos

A Di-Plan é responsável por consolidar as informações de cada área, e atualizar a versão vigente da Planilha no módulo correspondente do SGP.

8.2 Identificação e análise das Ameaças e Vulnerabilidades dos Ativos

8.2.1 Identificar, classificar e analisar Ameaças

Ao finalizar o levantamento e identificação dos ativos, inicia-se a etapa de Identificação, classificação e análise das ameaças por ativo, realizadas pela DI-TI em conjunto com a área responsável pelo ativo, por meio da Planilha de Gestão de Ativos consolidada.

Uma ameaça tem o potencial de comprometer ativos como informações, processos e sistemas e, por isso, também ações estratégicas e operacionais do TCE Goiás.

Algumas ameaças podem afetar mais de um ativo. Nesses casos, elas podem provocar impactos diferentes, dependendo de quais ativos são afetados. Sendo assim, cabe a DI-TI em conjunto com o responsável pelo ativo analisar cada ameaça disponível na Planilha de Gestão de Ativos e promover a devida classificação.

Nota 3: A metodologia de análise e classificação de ameaças por ativo fundamenta-se da Gestão de Riscos da Segurança da Informação padronizada na NBR ISO/IEC 27005.

Os tipos possíveis de ameaças estão listadas na “Planilha de Gestão de Ativos” na aba “Ameaças”, podendo ser Ameaças Físicas, Ameaças Naturais, Falhas na Infraestrutura, Falhas Técnicas, Ações Humanas, comprometimento de funções ou serviços, Ameaças Organizacionais, dentre outros.

Cada tipo de ameaça possui um mapeamento prévio das possíveis ameaças associadas.

Exemplo:

- Tipo de Ameaça: Dano Físico
- Descrição da Ameaça para Dano Físico: fogo, água, poluição, acidente grave, etc.

Ao se definir o tipo de ameaça, e consequentemente, as ameaças associadas, deve-se identificar a origem da ameaça, a seguir:

- **Ameaças de origem Intencionais:** são provocadas por invasões, fraudes e roubo de informações.

- **Ameaças de origem Acidentais:** são causadas por erros de desconhecimento no uso do ativo, onde aparecem erros inconscientes de funcionários que não foram devidamente treinados, infecções por vírus ou até mesmo os acessos indevidos.

- **Ameaças de origem Natural** são causadas por eventos de ordem natural sem qualquer intervenção física humana.

Em seguida, deve-se estabelecer quais são as consequências e o impacto que pode ser provocado pelas ameaças identificadas, caso venham a se materializar, ocasionando perda de confidencialidade, de integridade e de disponibilidade da informação. As consequências/impactos estão diretamente relacionadas à descrição das ameaças, conforme previsto na aba “Ameças” da Planilha de Gestão de Ativos, e devem ser validadas pelas áreas responsáveis em conjunto com a equipe de TI.

8.2.2 Identificar vulnerabilidade dos ativos

Cabe ao responsável pelo ativo, em conjunto com a equipe de TI, a identificação de sua vulnerabilidade com base na caracterização das ameaças, considerando dentre os possíveis tipos de vulnerabilidades de segurança da informação: (i) vulnerabilidade de Hardware; (ii) de Software; (iii) de Rede; (iv) de Pessoal; de Locais ou Instalações; (v) do tipo Organizacional. Para cada tipologia estão definidas suas respectivas vulnerabilidades, a serem destacadas e trabalhadas pelo TCE-GO, conforme descrição da Planilha de Gestão de Ativos, na aba de “Vulnerabilidades” (pré-determinadas conforme NBR ISO/IEC 27005:2023 – Anexo A).

Para avaliação das vulnerabilidades técnicas o TCE-GO adota métodos proativos os quais incluem:

- ferramenta automatizada de varredura de vulnerabilidades;

- testes de segurança e avaliação;

- dentre outros inseridos em contrato terceirizado.

8.2.3 Identificar Controles Existentes

Para concluir a identificação e a análise das ameças e vulnerabilidades dos ativos inventariados, o responsável pelo ativo, em conjunto com a equipe de TI, realizam a identificação dos Controles internos existentes, ou seja, ferramentas, documentos, conjunto de atividades administrativas, planos, rotinas, métodos e procedimentos interligados, realizados pelo TCE-GO, para assegurar que os ativos da organização possuam controle confiável, concreto, eficiente e eficaz, evidenciando eventuais desvios ao longo do uso do ativo. Cada área do TCE-GO possui controles contra possíveis ameaças, implementados em conjunto com a área de TI, e em sua maioria, constituem-se em locais físicos e remotos com segurança de acesso, principalmente quando se tratam de ativos do tipo “Sigiloso”.

Neste momento são considerados controles operacionais instituídos conforme detalhamento da declaração de aplicabilidade, a qual descreve o controle conforme o Anexo A da NBR ISO/IEC 27001:2022 aplicado às atividades do TCE-GO, e os documentos comprobatórios de atendimento.

8.3 Gerenciamento de Riscos

8.3.1 Realizar avaliação do risco

Finalizada a identificação das ameaças, vulnerabilidades e os atuais controles existentes, inicia-se a etapa de Plano de Tratamento dos Riscos, onde o Responsável pelo ativo, juntamente com a Equipe de TI, realiza a Avaliação do Risco, distribuída em 3 etapas: 1ª etapa - Avaliação de Risco; 2ª etapa - Avaliação de Risco Residual; 3ª etapa – Avaliação de Eficácia.

a) 1ª Etapa – Avaliação de Risco

Na 1ª Etapa de Avaliação de Risco, por meio da Planilha de Gestão de Riscos é realizada a avaliação referente a Probabilidade/Frequência de ocorrência das ameaças e vulnerabilidades vinculadas ao ativo, bem como sua Consequência/Severidade de Impacto para as atividades operacionais e estratégicas do TCE-GO caso os cenários previstos se materializem. Para tanto, é utilizada como metodologia a Matriz de Análise de Riscos, conforme Quadros 2 e 3.

Quadro 2 – Critérios de avaliação

NUMERAÇÃO (3, 5, 7 e 9)	PROBABILIDADE/FREQUÊNCIA	CONSEQUÊNCIA / SEVERIDADE DO IMPACTO
3	Nunca aconteceu.	A consequência possui resultados pouco significativo para o TCE/GO.
5	Ocorreu menos de uma vez no semestre.	A consequência possui resultados com custos baixos ou nenhuma ação positiva.
7	Ocorreu mais de uma vez no semestre.	A consequência possui resultados com custos altos ou oportunidades de melhoria para o TCE/GO.
9	Ocorre mensalmente.	A consequência possui resultados

		ameaças ou oportunidades irreversíveis.

Ao atribuir o valor de numeração para os campos “Probabilidade/Frequência” e “Consequência/Severidade do Impacto” , obtem-se o Nível do Risco/Grau de Atenção ao risco avaliado, conforme Matriz de Análise de Riscos (Quadro 3).

Quadro 3 – Matriz de Análise de Riscos

Matriz de Análise de Riscos de Segurança da Informação			**Probabilidade/Frequência**			
			Raro	Provável	Muito provável	Praticamente certo
			3	5	7	9
Consequência Severidade do Impacto	Baixo	3	9	15	21	27
	Médio	5	15	25	35	45
	Alto	7	21	35	49	63
	Muito alto	9	27	45	63	81

Considerando a maior prioridade o número 81 e a menor prioridade o número 9, o responsável pelo ativo, em conjunto com a Equipe de TI, deve determinar ações específicas a fim de mitigar, prevenir, aceitar, transferir, monitorar ou eliminar a ocorrência de ameaças e vulnerabilidades associadas ao ativo, conforme resultados abaixo:

- **Faixa Vermelha:** Risco com alta probabilidade de ocorrência, impactando diretamente a segurança da informação no TCE Goiás. Deve-se realizar a proposta de tratamento do risco. Considerado neste caso como um risco significativo ao SGSI.

- **Faixa Amarela:** Risco com média probabilidade de ocorrência possuindo uma tendência a impactar a segurança da informação. Deve-se realizar a proposta de tratamento do risco, considerando seu monitoramento contínuo.

- **Faixa Verde:** Riscos com baixa probabilidade de ocorrência não gerando impacto a segurança da informação. Não há necessidade de adoção de medidas para tratamento do risco.

Cabe destacar que neste momento é avaliada a aplicação dos controles existentes, considerando sua efetividade para com a gestão do risco analisado.

Após a classificação do grau de significância, cabe ao responsável pelo ativo avaliado em conjunto com a DI-TI adotar a estratégia necessária a cada risco classificado como significativo, sendo considerados os seguintes cenários:

– **Prevenir o Risco:** Aplica-se ao risco considerado inaceitável para a organização. Tendo como ação a eliminação das causas raiz vinculadas ao risco, considerando as

ameaças e vulnerabilidades associadas.

- **Transferir o Risco/Compartilhar o Risco:** Transferir/Compartilhar o risco para um terceiro, transferindo os impactos e a responsabilidade de gestão de suas ameaças e vulnerabilidades associadas.

- **Mitigar o Risco:** Reduzir a probabilidade ou impacto de um risco até um nível aceitável.

- **Monitorar o Risco:** Riscos não priorizados, porém considerados como faixa amarela estão aptos a monitoramento contínuo conforme gestão de incidentes de segurança da informação considerando avaliações de consequência a confidencialidade, integridade, disponibilidade e autenticidade. Sendo este assunto pauta oficial das reuniões do comitê de segurança da informação.

- **Aceitar o Risco:** Quando não é possível aplicar nenhuma das outras estratégias, e a equipe do projeto decide correr o risco, porém com medidas de controles aplicadas e identificadas na planilha de gestão de ativos, apoiado nas ações previstas e sistema SGP, assim como o monitoramento contínuo junto a avaliação de incidentes de segurança da informação.

Nota 4: O plano de tratamento do risco deve compor ações vinculadas a itens de controle específicos do Anexo A da NBR ISO/IEC 27001:2022, considerando em específico a avaliação de conformidade com requisitos legais e contratuais de cada ativo identificado, e assim, a associação com as evidências documentais atribuídas a cada controle.

Nota 5: Os meios de tratamentos dos riscos serão tomados considerando as medidas de controle propostas pelo Anexo A da NBR ISO/IEC 27001:2022.

Nota 6: Os controles existentes podem ser identificados na “Planilha de Ativos” na coluna de “Controles Existentes”.

Após obter a classificação do nível do risco, determinando o Grau de Significância e a estratégia de atuação, neste momento o responsável pelo ativo em parceria com a DI-TI deve justificar a estratégia adotada considerando critérios de confidencialidade, disponibilidade e integridade de cada ativo analisado.

Em seguida, deve-se partir para a elaboração do plano de tratamento de riscos, que consiste na definição de iniciativas de melhoria (vide PO Gerir Melhoria Contínua) conforme estratégias definidas para tratamento do risco. O embasamento para construção das iniciativas parte do entendimento de que há a possibilidade do controle existente não funcionar como esperado (risco classificado entre as faixas amarela e vermelha) permitindo a análise precisa da causa raiz do fato ocorrido, e contemplando ainda a existência das vulnerabilidades vinculadas as ameaças deste ativo.

b) 2ª Etapa – Avaliação de Risco Residual

A segunda etapa consiste na Avaliação do Risco Residual. O Risco Residual representa o nível de risco que permanece ou que aparece após a inclusão dos controles adicionais e/ou

ajustes dos controles existentes, em que, após a aplicação do 1º Tratamento do Risco (desenvolvimento do plano de ação sugerido por meio das iniciativas de melhoria), o risco permanece sendo significativo ao SGI do TCE-GO.

A realização desta etapa ocorre por meio de auditoria interna (conforme PO Gerir Auditorias do SGI), onde será avaliada a completa implementação das medidas de controle descritas no plano de tratamento proposto na 1º Etapa de Tratamento do Risco, verificando assim a conformidade das evidências apresentadas. Realiza-se uma nova avaliação de risco para identificação de riscos residuais, e posteriormente atribui-se um novo nível ao risco (Grau de Significância), conforme metodologia anteriormente descrita. A partir dos resultados obtidos, aplica-se os seguintes critérios:

- **Faixa Vermelha:** Risco com alta probabilidade de ocorrência, impactando diretamente a segurança da informação no TCE-GO, sendo neste caso avaliada a não eficiênciado 1º Plano de Tratamento Proposto e atribuição direta do Grau de Significância. Deve-se determinar a estratégia de atuação e proposição do 2º Plano de Tratamento para o risco.

- **Faixa Amarela:** Risco com média probabilidade de ocorrência possuindo uma tendência a impactar a segurança da informação. Deve-se realizar o contínuo monitoramento deste risco verificando seu grau de incidência, esse monitoramento deve estar vinculado a indicadores estratégicos e/ou operacionais. A estratégia adotada neste caso é de monitoramento, não sendo considerado um risco significativo para o SGI.

- **Faixa Verde:** Riscos com baixa probabilidade de ocorrência não gerando impacto a segurança da informação. Não é considerado um risco significativo para o SGI.

Após esta análise, o resultado da avaliação do Risco Residual pode ser:

- “SIM”, considera-se o risco secundário ou residual como significativo ao SGI do TCE-GO, devendo-se prever novas ações de tratamento do risco.

- “NÃO”, deverá se manter em observação e monitoramento pelo Emitente responsável pelo ativo para um novo ciclo anual de auditoria interna.

Nota 7: A DI-TI deve realizar o monitoramento das ações de controle propostas para os riscos residuais, considerando sua eficácia, assim como sua reavaliação de classificação quanto ao Grau de Significância, sendo este assunto atribuido em pauta fixa tratada em reunião do Comitê de Segurança da Informação, ocorrendo preferencialmente a cada três meses.

Para as situações em que houveram riscos residuais identificados por meio de apontamentos da auditoria interna, novas propostas de ação (iniciativas de melhoria registradas no SGP) serão definidas pela área responsável, com suporte da DI-PLAN, sendo apresentadas em Reunião de Análise Crítica (RAC) e/ou Ata de Reunião do Comitê de Segurança da Informação.

Nota 8: Os planos de ação propostos devem fazer menção a qual controle do Anexo A da

NBR ISO/IEC 27001 está sendo contemplado e trabalhado, considerando em específico a contínua proposta de plano de ações para avaliação de conformidade com requisitos legais e contratuais de cada ativo identificado.

c) 3ª Etapa – Avaliação de Eficácia

A análise de eficácia é realizada por meio da avaliação dos resultados dos indicadores relacionados ao CID – Confidencialidade, Integridade e Disponibilidade, gerenciados pela DI-TI, a cada reunião do Comitê Gestor de Segurança da Informação, baseado na ocorrência / incidência de eventos relacionados aos ativos monitorados, com registro da análise realizada na Planilha de Gestão de Ativos.

9. Indicadores

9.1 Indicadores de Verificação

Não aplicável até o presente momento.

9.2 Indicadores de Controle

Não aplicável até o presente momento.

10. Controle de Registros

Nome do Registro / Código	Armazenamentoe Preservação	Distribuição e Acesso*	Recuperação**	Retenção e Disposição
Planilha de Gestão de Ativos	SGP	Acesso controlado por senha e site institucional.	Backup	Retenção por tempo Indeterminado
Processos Operacionais	SGP	Acesso controlado por senha e site institucional.	Backup	Retenção por tempo Indeterminado
Gestão de Riscos	SGP	Acesso controlado por senha e site institucional.	Backup	Retenção por tempo Indeterminado
Gestão da Melhoria Contínua	SGP	Acesso controlado por senha e site institucional.	Backup	Retenção por tempo Indeterminado
Ata de Análise Crítica	SGP	Acesso controlado por senha e site institucional.	Backup	Retenção por tempo Indeterminado
Ata de Reunião CSI	SGP	Acesso controlado por senha e site institucional.	Backup	Retenção por tempo Indeterminado

Cadeia de Valor	SGP	Acesso controlado por senha e site institucional.	Backup	Retenção por 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

Anexo I – Planilha de Gestão de Ativos

12. Elaboração, Revisão e Aprovação

PO – Gerir Ativos de Tecnologia da Informação		
Diretoria de Tecnologia da Informação		
Responsável por	***Nome***	***Função***
Elaboração	Licardino Siqueira Pires	Diretor de Tecnologia da Informação
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: n. 003 de 24/11/2022	Versão atual: n. 004 de 10/11/2023	Próxima revisão programada: 10/11/2025