ÍNDICE

1. OBJETIVO

A organização estabelece os seguintes objetivos fundamentais para o seu Sistema de Gestão de Serviços (SGS):

Alinhamento Estratégico: Garantir que os serviços de TI catalogados estejam alinhados e suportem metas diretas do negócio e requisitos das partes interessadas.

Garantia de Qualidade e SLA: Atingir e manter o índice de conformidade com os Acordos de Nível de Serviço (SLAs) acordados com os clientes.

Continuidade e Disponibilidade: Assegurar a disponibilidade contratada dos serviços críticos e manter o Plano de Continuidade de Serviços testado e atualizado anualmente.

Eficiência e Mitigação de Riscos: Reduzir riscos operacionais identificados mediante avaliações formais periódicas e otimização contínua da alocação de recursos.

Melhoria Contínua: Promover ciclo semestral de avaliação de maturidade do SGS e implementar as ações preventivas/corretivas decorrentes dos planos de melhoria.

Conformidade Legal: Manter conformidade total com requisitos legais, regulamentares e contratuais aplicáveis.

2. APLICAÇÃO E ÁREAS ENVOLVIDAS

Esta política aplica-se a toda a Organização (TIVIT e empresas do Grupo TIVIT), englobando todos os colaboradores, parceiros e fornecedores envolvidos no planejamento, desenho, transição, entrega, suporte e governança dos serviços de TI disponibilizados aos clientes internos e externos.

3. DEFINIÇÕES E PREMISSAS

Sistema de Gestão de Serviços de TI (SGSTI): Conjunto de elementos inter-relacionados para estabelecer políticas, objetivos e processos para o gerenciamento eficaz dos serviços de TI.

ISO/IEC 20000-1: Padrão internacional para Gestão de Serviços de TI que especifica os requisitos para a organização planejar, estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um SGSTI.

Item de Configuração (IC): Ativo ou componente necessário para a entrega de um serviço de TI mantido sob controle no CMDB.

Acordo de Nível de Serviço (SLA): Compromisso formal assinado entre a Organização e o cliente que especifica os níveis de qualidade e prazos do serviço ofertado.

Ambientes Críticos de Negócio (ACN): Infraestruturas e serviços de TI cuja indisponibilidade causa impacto financeiro ou de imagem severo aos clientes.

4. RESPONSABILIDADE

A estrutura de papéis e responsabilidades do SGSTI é regida pela matriz de autoridade da Organização, assegurando a segregação adequada de funções e o envolvimento executivo:

Papel / Área	Responsabilidade Principal no SGSTI
Diretoria de Serviços / Alta Direção	Prover liderança, assegurar o alinhamento do SGSTI à estratégia de negócio, disponibilizar recursos e aprovar diretrizes orçamentárias e de riscos.
Governança de Tecnologia da Informação (GOV)	Manter o arcabouço normativo do SGSTI, conduzir o controle de todo o sistema de Gestão com base no framework ITIL e monitorar indicadores operacionais e auditorias.
Delivery GRC Security & Privacy (DGS) / Segurança (SEG)	Estabelecer políticas de cibersegurança, realizar análises de eficácia e assegurar a conformidade com o Sistema de Gestão de Segurança da Informação (SGSI).
Customer Success (CS)	Gerenciar a interface com os clientes, conduzir comitês operacionais de eficácia, acompanhar o cumprimento de SLAs e registrar oportunidades de melhoria.
Equipes Operacionais e Sustentação	Executar os serviços operacionais conforme Instruções Operacionais (IOPs), tratar eventos e incidentes, e apoiar o processo de aceite de ativos.
PMO & Project Delivery (TDT)	Conduzir a transição de projetos, gerenciar requisições de mudança de projetos (CRQ) e garantir o rigor na criação

Papel / Área	Responsabilidade Principal no SGSTI
	de artefatos.

5. DESCRIÇÃO DA POLÍTICA

5.1. Liderança e Comprometimento da Alta Direção

A Alta Direção demonstra seu comprometimento com o SGSTI garantindo a integração dos requisitos do sistema de gestão aos processos de negócio, promovendo a cultura de foco no cliente e assegurando que os objetivos de serviço sejam estabelecidos e mensurados.

5.2. Planejamento e Gestão de Riscos

A Organização realiza a identificação sistemática de riscos e oportunidades que impactam a prestação de serviços. Toda mudança estrutural, transição de tecnologia ou novo serviço deve passar por avaliação de impacto financeiro e operacional antes de sua execução.

5.3. Desenho, Transição e Aceite de Novos Serviços (Framework de Aceite)

A transição de novos Itens de Configuração (Servidores, Redes/Segurança e Storage) para os times de sustentação deve seguir o **Framework de Aceite**. O aceite formal exige a validação prévia de pré-requisitos essenciais, tais como:

1. Instalação e validação do Agente de Automação e Agentes de Monitoração.
2. Instalação e validação de conectividade do Agente de Backup.
3. Cadastro e atualização completa de atributos obrigatórios na CMDB
4. Aprovação de mudanças de aceite mínimo no ITSM.

5.4. Entrega e Operação dos Serviços

5.4.1. Gerenciamento de Nível de Serviço e Eficácia

Os serviços prestados são continuamente avaliados quanto à sua eficácia operacional e alinhamento às metas contratuais, garantindo transparência e rastreabilidade através de relatórios periódicos e comitês conjuntos entre CS e Clientes.

5.4.2. Gerenciamento de Incidentes e Eventos

A monitoração do ambiente é realizada de forma contínua através de ferramentas integradas e correlacionadas. Eventos críticos em Ambientes Críticos de Negócio (ICs ACN - Prioridade 1) geram abertura automática de incidentes para pronta atuação das equipes operacionais 24x7.

5.4.3. Gerenciamento de Mudanças (GOV-PRO-001)

Todas as alterações na infraestrutura ou nos serviços são controladas para mitigar riscos de indisponibilidade. Mudanças recorrentes e de baixo risco devem utilizar templates pré-configurados e auditados (TBR, TPA, TAM), dispensando aprovação em comitê (CAB) quando elegíveis.

5.4.4. Gerenciamento de Configuração e CMDB (GOV-PRO-011)

A integridade e acuracidade da base de dados do CMDB são garantidas por meio do controle estrito do ciclo de vida dos ativos (Pending Install, Installed, Retired) e por auditorias mensais amostrais em carteiras de clientes.

5.4.5. Governança de Projetos e Change Requests (CRQ em Projetos)

Projetos gerenciados pela área de PMO utilizam um fluxo formal de homologação de Change Requests (CRQ Normal de Custo ou Informativa) para controlar desvios de escopo, prazo e custo, garantindo visibilidade para FP&A, PMO e Diretorias envolvidas.

5.4.6. Avaliação de Desempenho e Indicadores

A eficácia do SGSTI é monitorada continuamente através dos indicadores-chave de processo acompanhados pelo TIVIT Docs.

5.4.7. Melhoria Contínua e Análise Crítica

A Organização mantém a prática da melhoria contínua como pilar central, estimulada pela análise de causa raiz em investigações de Problemas (PRB), lições aprendidas de CRQs e auditorias de qualidade. O ciclo PDCA é aplicado para revisar periodicamente os processos operacionais e adequá-los às evoluções do negócio e avanços tecnológicos.

6. REFERÊNCIA A OUTROS DOCUMENTOS

ISO/IEC 20000-1: Information technology — Service management — Part 1: Service management system requirements.
GOV-PRO-001: Gerenciamento de Mudanças
GOV-PRO-011: Gerenciamento de Configuração
GOV-PRO-005: Gerenciamento de Incidentes e Requisição
GOV-PRO-043: Gestão de Performance Metric Book (PMB)
DGS-PRO-001: Governança de Cibersegurança
QP-PRO-003: Auditorias