Política de Gestão de Serviços de Tecnologia da Informação

Versão 1.00

SUMÁRIO

1 INTRODUÇÃO

A Política de Gestão de Serviços de Tecnologia da Informação (ITSM) estabelece os princípios, diretrizes e responsabilidades visando garantir a entrega eficaz e eficiente de serviços de Tecnologia da Informação (TI) na CERC para apoiar as operações do negócio, garantir a satisfação dos clientes e promover a excelência operacional.

2 ABRANGÊNCIA

Abrange todos os colaboradores, contratados e terceiros que estão envolvidos na prestação, suporte e utilização dos serviços de TI na CERC.

3 PRINCÍPIOS GERAIS

A Política de Gestão de Serviços de Tecnologia da Informação (ITSM) possui como direcionadores os seguintes princípios:

- **Integridade:** garantir a consistência, precisão e confiabilidade dos dados, processos e sistemas de TI, garantindo que as pessoas não estejam sujeitas a acessos e alterações não autorizadas.
- **Transparência:** fornecer acesso adequado e claro às informações relacionadas aos serviços de TI, desempenho dos serviços, incidentes, mudanças e outros aspectos relevantes às operações.
- **Equidade:** tratar de forma justa e imparcial todas as partes interessadas envolvidas nos serviços de TI, sem favorecer ou discriminar indivíduos ou grupos.
- **Responsabilização (*Accountability*):** assumir a responsabilidade por ações, decisões e resultados relacionados aos serviços de TI, bem como o cumprimento dos requisitos contratuais, e de todos os acordos e princípios voluntariamente subscritos pela empresa.
- **Sustentabilidade:** fornecer serviços de TI de forma eficiente e eficaz a longo prazo, utilizando de forma responsável os recursos e minimizando o desperdício.

4 DIRETRIZES

As diretrizes a seguir foram desenvolvidas para orientar a implementação e a operação dos processos essenciais da Gestão de Serviços de Tecnologia da Informação (ITSM) na CERC. Estas diretrizes abrangem os processos críticos que garantem a entrega eficaz e eficiente de serviços de TI, resultando na excelência operacional e no atendimento às necessidades do negócio, de forma que as diretrizes sejam confiáveis, seguras e capazes de adaptar-se às mudanças e demandas dos participantes.

4.1 Gestão de Incidente

A gestão de incidentes deve possibilitar a restauração dos serviços de TI o mais rápido possível após interrupções não planejadas, minimizando o impacto nos negócios e mantendo a produtividade dos usuários e participantes. Dessa forma, devendo:

- Identificar e registrar incidentes de forma oportuna;
- Priorizar e resolver os incidentes conforme a criticidade e o impacto nos negócios; e
- Comunicar, de maneira transparente e constante, sobre o *status* dos incidentes aos envolvidos.

4.2 Gestão de Problemas

A gestão de problemas deve possibilitar a identificação e a resolução das causas raízes dos incidentes, reduzindo o número e a gravidade dos incidentes recorrentes. Assim, devendo:

- Investigar e resolver as causas raízes dos problemas identificados; e
- Implementar soluções permanentes para prevenir a recorrência de problemas similares.

4.3 Gestão de Mudanças

A gestão de mudanças deve possibilitar a implementação de mudanças nos sistemas de TI de forma controlada e planejada, mitigando os riscos associados às mudanças, mantendo a estabilidade dos serviços de TI e assegurando que as mudanças estejam alinhadas com os objetivos do negócio. Desse modo, necessitando:

- Avaliar o impacto e o risco de cada mudança proposta antes da implementação;
- Documentar e obter aprovações adequadas para todas as mudanças planejadas; e
- Realizar testes e validações completas antes de implementar as mudanças nos ambientes de produção.

4.3.1 Gestão de Liberações

A gestão de liberações deve garantir que as mudanças autorizadas nos ambientes de produção sejam controladas, minimizando o risco de interrupções nos serviços de TI. Assim, devendo:

- Planejar e coordenar a implementação de mudanças autorizadas de forma controlada; e
- Minimizar os riscos associados às liberações por meio de testes e avaliações rigorosas.

4.4 Gestão de Configuração e Ativos

A gestão de configuração e ativos deve possibilitar, controlar e manter um registro detalhado de todos os ativos de TI e suas relações, facilitando o planejamento e a tomada de decisões, melhoria da precisão e da integridade dos dados de configuração. Dessa forma, devendo:

- Manter um registro preciso e atualizado de todos os ativos de TI e suas relações; e
- Garantir que as configurações dos itens de configuração (CIs) sejam documentadas e controladas adequadamente.

4.5 Gestão de Nível de Serviço

A gestão de nível de serviço deve definir, negociar, monitorar e relatar os níveis de serviço acordados com os participantes, fornecedores, clientes internos, possibilitando que os serviços de TI atendam às expectativas e requisitos dos participantes e clientes internos. Assim, necessitando:

- Definir, negociar e documentar acordos de nível de serviço (SLAs); e
- Monitorar e relatar regularmente o desempenho dos serviços em relação aos SLAs acordados.

4.6 Gestão de Capacidade

A gestão de capacidade deve garantir que os recursos de TI sejam dimensionados adequadamente para atender às demandas atuais e futuras do negócio, possibilitando que não haja subutilização nem sobrecarga dos recursos. Desse modo, devendo:

- Avaliar regularmente a capacidade dos recursos de TI para garantir que estejam dimensionados adequadamente para atender às demandas atuais e futuras do negócio;
- Realizar previsões de capacidade com base em tendências de uso, picos sazonais e novas demandas de negócios;

- Identificar e mitigar os gargalos de capacidade antes que afetem a disponibilidade e o desempenho dos serviços de TI; e
- Implementar planos de expansão de capacidade, conforme necessário, para garantir a escalabilidade dos serviços de TI.

4.7 Gestão de Disponibilidade

A gestão de disponibilidade deve assegurar que os serviços de TI estejam disponíveis quando necessário, minimizando o tempo de inatividade e garantindo a continuidade das operações de negócio. Assim, precisando:

- Estabelecer metas de disponibilidade para os serviços de TI com base nas necessidades do negócio e regras regulatórias;
- Monitorar continuamente a disponibilidade dos serviços de TI e identificar áreas de melhoria para minimizar o tempo de inatividade; e
- Implementar medidas preventivas para reduzir a probabilidade de interrupções nos serviços de TI, como redundância de sistemas e *backups* regulares.

4.8 Gestão de Continuidade de Serviço de TI

A gestão de continuidade de serviço de TI deve planejar e preparar a organização para lidar com interrupções significativas nos serviços de TI, garantindo a rápida recuperação e restauração dos serviços após incidentes. Dessa forma, devendo:

- Desenvolver e manter planos de continuidade de negócios e recuperação de desastres; e
- Realizar testes periódicos para garantir a eficácia dos planos de continuidade.

4.9 Gestão de Segurança da Informação

A gestão de segurança da informação deve proteger a confidencialidade, integridade e disponibilidade das informações e sistemas de TI, mitigando os riscos de violações de segurança e ataques cibernéticos. Desse modo, precisando:

- Proteger a confidencialidade, integridade e disponibilidade das informações e sistemas de TI; e
- Implementar controles de segurança adequados para mitigar os riscos de segurança da informação.

5 DISPOSIÇÕES FINAIS

Para garantir a responsabilização efetiva dos terceiros envolvidos na Gestão de Serviços de Tecnologia da Informação (ITSM), deve-se:

- Estabelecer contratos claros e abrangentes que definam as responsabilidades, obrigações e expectativas de desempenho. Isso inclui a definição de acordos de nível de serviço (SLAs) específicos e mensuráveis, bem como a implementação de sistemas de monitoramento contínuo para avaliar o desempenho dos terceiros em relação aos SLAs acordados. Além disso, é essencial manter comunicações transparentes, realizar avaliações regulares, exigir planos de contingência e continuidade de negócios, estabelecer incentivos para o bom desempenho e penalidades para a não conformidade, e conduzir avaliações rigorosas de parceiros potenciais antes da contratação.

6 ATRIBUIÇÕES E RESPONSABILIDADES

Deverão ser observados conforme atribuição de cada membro abaixo listado, as diretrizes contidas nos seguintes documentos: Estatuto Social, Regimentos Internos e demais Normativos Internos da CERC.

6.1 Conselho de Administração

» Aprovar a Política de Gestão de Serviços de Tecnologia da Informação e suas revisões, assegurando que esteja alinhada com os objetivos estratégicos.

6.2 Comitê de Riscos

» Apresentar parecer ao Conselho de Administração sobre a avaliação da gestão de riscos corporativos e eficácia dos controles internos.

6.3 Comitê de Auditoria

» Supervisionar a implementação da política de gestão de terceirização de serviços relevantes, garantindo que os procedimentos sejam integrados às operações diárias da empresa.

6.4 Área de Metodologia (CoEs)

» Zelar pela adoção, realizar acompanhamento e dar visibilidade sobre a Gestão de Serviços de Tecnologia da Informação;

» Gerir o relacionamento com parceiros estratégicos e prestadores de serviços críticos de Tecnologia da Informação; e

» Garantir a conformidade regulatória sobre a Gestão de Serviços de Tecnologia da Informação, instruindo e acompanhando ações das áreas envolvidas no tema.

6.5 Área de Infraestrutura (CoEs)

» Identificar e implementar estratégias para otimizar os gastos com serviços de nuvem;

» Estabelecer ferramentas e processos para monitorar e reportar o uso e custos da nuvem;

» Implementar práticas de governança para gerenciar o uso da nuvem, incluindo a gestão de custos e a conformidade com os padrões estabelecidos;

» Definir estratégia de uso de *cloud;*

» Difundir conhecimento sobre melhores práticas do uso de *cloud; e*

» Criar e gerenciar as plataformas tecnológicas sob o ponto de vista de infraestrutura.

6.6 Área de Arquitetura (CoEs)

» Desenvolver e manter uma estratégia tecnológica alinhada com os objetivos de negócio, incluindo a seleção de tecnologias-chave e padrões a serem seguidos;

» Estabelecer e fazer cumprir diretrizes, políticas e melhores práticas para garantir a conformidade com os padrões de arquitetura definidos (arquitetura de referência, tecnologias e ferramentas);

» Colaborar com equipes de tecnologia para garantir que as soluções propostas estejam alinhadas com a arquitetura tecnológica da empresa;

» Manter uma comunicação eficaz e proporcionar treinamentos a fim de garantir alinhamento com os princípios e diretrizes arquiteturais; e

» Promover e garantir a inovação contínua, explorando novas oportunidades tecnológicas que possam trazer vantagens competitivas para a organização.

6.7 Área de Infosec (CoEs)

» Estabelecer Políticas, Normas e procedimentos de Segurança da Informação adotando as melhores práticas para assegurar a integridade, confidencialidade e disponibilidade do ambiente tecnológico;

» Desenvolver controles de segurança robustos com o objetivo de prevenir, detectar e responder de forma eficaz a incidentes de segurança que possam afetar os serviços de tecnologia da informação;

» Promover a disseminação da cultura de segurança da informação de forma colaborativa com toda a empresa, garantindo que estejam familiarizados com o tema e alinhados com os princípios e diretrizes de segurança da informação; e

» Colaborar estreitamente com as equipes de tecnologia para que possam tomar decisões incorporando a perspectiva de segurança da informação em suas deliberações.

6.8 Área de *Command Center* (Operações)

» Estabelecer e fazer cumprir diretrizes, políticas e melhores práticas para garantir a conformidade na Gestão de Incidentes, Gestão de Problemas e Gestão de Mudanças com os padrões de governança definidos;

» Implementar e gerenciar soluções que proporcionam visibilidade em tempo real sobre o desempenho, a saúde e a eficiência dos sistemas e aplicações, incluindo a coleta, análise e interpretação de dados provenientes de métricas, *logs* e *tracking* de aplicações para detectar, investigar e resolver proativamente problemas, além de otimizar a performance;

» Desenvolver *dashboards* e alertas para monitorar indicadores chave de desempenho, possibilitando e facilitando a tomada de decisões baseada em dados e a rápida resposta a incidentes, garantindo assim a alta disponibilidade e a confiabilidade dos serviços prestados pela CERC;

» Garantir o suporte contínuo das aplicações nos ambientes existentes, visando reduzir o tempo de atendimento, aprimorar a qualidade dos futuros atendimentos e propor melhorias nos módulos;

» Implementar diretrizes para manter uma base de conhecimento atualizada e concisa, a fim de fornecer suporte eficaz aos usuários internos e externos, otimizando o uso das aplicações nos ambientes atuais e de Inteligência Artificial; e

» Reduzir custos e erros operacionais através de automação de processos de negócio. Aumentar a qualidade dos serviços prestados apoiando áreas de negócio com ferramentas de Inteligência Artificial.

6.9 Diretoria de Tecnologia

» Garantir que a estratégia de tecnologia esteja alinhada aos objetivos de negócio da organização e que os serviços de TI sejam entregues de forma eficaz e eficiente.

7 CONTROLE DOCUMENTAL

CRIAÇÃO | REVISÃO | REVOGAÇÃO			
Versão Anterior	**Versão Atual**	**Data da Aprovação**	**Ref. De ATA/Aprovação**
N/A	**1.0**	**22/03/2024**	**Conselho de Administração**
Diretoria Responsável		**Área Responsável**	
CoEs		**Metodologia**	
PRINCIPAIS MODIFICAÇÕES			
Alterações: » N/A **Inclusões:** » N/A **Revogações:** » N/A			

LEGISLAÇÕES OU DOCUMENTOS RELACIONADOS
» Resolução 304/2023 BCB.

8 ANEXOS

8.1 Anexo 1 - Termos e Definições

» **ITSM:** Gestão de Serviços de Tecnologia da Informação.

» **SLA:** Acordo de Nível de Serviço, estabelece os parâmetros e metas de desempenho acordados entre o provedor de serviços de TI e o cliente.

» **CI:** Item de Configuração, representa um componente ou recurso de TI que precisa ser gerenciado em relação à sua configuração e relacionamentos.

» **Continuidade de Serviço de TI:** Capacidade de uma organização em continuar a prestação de serviços de TI após um incidente ou interrupção significativa.