POLÍTICA DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

Quick Soft Tecnologia da Informação S.A.

1. APRESENTAÇÃO E OBJETIVOS

As definições a seguir foram criadas para guiar a implementação e operação dos principais processos de Gestão de Serviços de TI (ITSM) na Quick Soft Tecnologia da Informação S.A. (“Companhia”). Elas englobam processos fundamentais que asseguram a entrega eficiente e eficaz dos serviços de TI, promovendo excelência operacional e alinhamento com as necessidades do negócio. Essas diretrizes visam garantir que os processos sejam confiáveis, seguros e capazes de se adaptar às mudanças e demandas da empresa.

1.1. Escopo

A política abrange todos os níveis da organização, garantindo que as diretrizes sejam seguidas para a proteção e eficiência das operações de TI.

2. SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

2.1. Gerenciamento De Capacidade e Disponibilidade

A Companhia deve medir e monitorar os níveis de serviço (SLA) relacionados à disponibilidade dos recursos computacionais e à capacidade instalada.

A partir da gestão contínua desses indicadores, a empresa deve implementar ações de melhoria contínua, como a eliminação de incidentes e problemas que afetam a disponibilidade, bem como o ajuste da capacidade computacional para atender as necessidades operacionais da organização. Essas práticas garantem a manutenção de um ambiente de TI eficiente e alinhado com os objetivos do negócio.

2.2. Gerenciamento de Mudanças

A Companhia deve planejar, executar, controlar, registrar e documentar todas as alterações no ambiente de tecnologia da informação, incluindo liberações de novas funcionalidades e manutenções gerais.

Este processo deve garantir que as mudanças sejam implementadas com sucesso, evitando impacto operacional para os usuários, e que os compromissos de níveis de serviço contratados sejam mantidos. O objetivo é assegurar a evolução contínua do ambiente, preservando a integridade e a disponibilidade dos serviços prestados.

2.3. Monitoramento de Infraestrutura e Serviços

A Companhia deve realizar o monitoramento contínuo da infraestrutura e dos serviços, com foco em identificar proativamente indícios de falhas ou comportamentos fora dos padrões estabelecidos.

Este processo deve gerar notificações e alarmes para os responsáveis, além de medir a qualidade dos serviços, garantindo o cumprimento dos níveis de serviço (SLA) dos serviços prestados.

2.4. Gerenciamento de Ativos

A Companhia deve controlar os ativos de hardware utilizados em seus ambientes, garantindo a preservação do tempo de vida útil, monitorando os períodos de garantia dos fabricantes e registrando manutenções planejadas e emergenciais. Esta política tem como objetivo mitigar os riscos de obsolescência e de paradas não programadas, além de otimizar os custos operacionais associados ao ciclo de vida dos ativos.

2.5. Gerenciamento de Licenças de Software

A Companhia deve administrar as licenças de software de terceiros utilizadas em seu ambiente, garantindo a conformidade com a legislação, políticas internas e contratos dos fabricantes de software. Além disso, deve assegurar a atualização técnica contínua dos softwares, aplicando patches e atualizações liberadas pelos fabricantes e a diligência completa na homologação de softwares de terceiros. Esse processo visa manter os ambientes operacionais em condições de alta performance, segurança e alinhados às melhores práticas de mercado, preservando a integridade e eficiência dos serviços oferecidos.

2.6. Gerenciamento de Backup, Recuperação e Continuidade

Para informações complementares, acesse o Manifesto da Administração e o Glossário de Termos.

A Companhia deve garantir a proteção de todos os dados por meio de processos robustos de backup e recuperação, assegurando a restauração em casos de falha de hardware ou contingência. O monitoramento e a melhoria contínua das rotinas devem maximizar a segurança e minimizar os tempos de recuperação (RTO) e ponto de recuperação (RPO), conforme aplicável. Além disso, a Companhia deve manter um Plano de Continuidade de Negócio (PCN) para seus processos críticos, garantindo a continuidade operacional e a resiliência da empresa diante de incidentes.

2.7. Gerenciamento de Banco de Dados

A Companhia deve administrar e manter o serviço de banco de dados operacional e em boas condições na camada de infraestrutura. Esta diretriz também abrange a administração do banco de dados, incluindo a implementação de novos recursos, atualizações de versões, e melhorias funcionais na arquitetura, assegurando a continuidade e a eficiência dos serviços prestados.

2.8. Gerenciamento de Incidentes e Problemas

A Companhia deve manter um processo de gestão de incidentes e problemas com o objetivo de resolver as causas raízes dos incidentes, reduzindo sua recorrência e gravidade. O processo deve investigar a fundo as causas dos problemas, garantindo uma análise completa e implementando soluções permanentes que previnam a repetição de problemas similares.
Além disso, é essencial documentar e compartilhar as lições aprendidas, utilizando uma base de conhecimento para agilizar a resolução de futuros incidentes e melhorar a continuidade dos serviços prestados.

2.9. Gerenciamento de Configurações

A Companhia deve controlar, registrar e administrar os Itens de Configuração (CIs) de seus ambientes, garantindo o gerenciamento eficaz do versionamento. Este processo visa proporcionar suporte e agilidade a outros processos, como Gestão de Mudanças, Incidentes e Problemas, assegurando que os CIs estejam devidamente atualizados e alinhados com as necessidades operacionais e de segurança da empresa.

2.10. Gerenciamento de Redes

A Companhia deve manter de forma controlada a estrutura de rede física e lógica, tanto privada quanto pública, abrangendo todos os recursos de rede utilizados pela empresa. Este processo deve garantir a realização de manutenções seguras, monitorando o ambiente de maneira adequada e assegurando que a segurança seja compatível com os níveis de serviço acordados com seus clientes, preservando a continuidade e a integridade dos serviços prestados.

2.11. Gerenciamento de Identidade e Acesso

A Companhia deve gerenciar as concessões e manutenções dos direitos de acesso aos serviços da empresa e a toda a infraestrutura utilizada. Este processo deve assegurar que os acessos sejam controlados, garantindo a segurança e a integridade dos sistemas e dados, além de assegurar que os direitos de acesso estejam alinhados com as necessidades operacionais e políticas de segurança da empresa.

2.12. Gerenciamento de Segurança de T.I.

A Companhia deve manter a Segurança da Informação em seu ambiente, seguindo as melhores práticas de mercado. O processo deve avaliar e monitorar continuamente o comportamento dos recursos computacionais e das pessoas, adotando práticas que garantam uma segurança cada vez mais efetiva e alinhada ao negócio. A empresa deve assegurar que todas as medidas de segurança estejam compatíveis com as exigências do ambiente e as necessidades operacionais.

3. CONTROLE DOCUMENTAL

Esta Política será revisada periodicamente, e sempre que necessário, para garantir sua eficácia e adequação às mudanças normativas, à evolução das melhores práticas de governança corporativa e às necessidades específicas da Companhia.

Para informações complementares, acesse o Manifesto da Administração e o Glossário de Termos.

Responsável	Controle de Revisões	
CEO	Versão Atual	1.0
	Data da Aprovação	16/10/2024
	Versão Anterior	-
	Ata de Aprovação	Conselho de Administração

Principais Modificações	Legislações e Documentos Relacionados
- Criação da política	- Resolução 304/2023 BCB

Para informações complementares, acesse o Manifesto da Administração e o Glossário de Termos.