POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

Grupo TC
Av. Presidente Jucelino Kubitschek, n°1.830
Torre 2 – 5° Andar
Vila Nova Conceição – São Paulo – SP,
04543-01

tc.com.br
+55 11 4003-6048

Sumário

Grupo TC
Av. Presidente Jucelino Kubitschek, n°1.830 - Torre 2 - 5° Andar
Vila Nova Conceição – São Paulo – SP - 04543-01

tc.com.br
+55 11 4003-6048

1. Abrangência

As diretrizes aqui contidas são aplicáveis a todos os colaboradores do TC, incluindo sócios, administradores e empregados. Nos casos de relações comerciais, contratuais ou de confiança com terceiros, dependendo da natureza das informações trocadas, pode ser necessária a adesão pelo terceiro às políticas aplicáveis ao TC.

A informação contida neste documento é de uso interno e deve estar disponível aos colaboradores através dos canais corporativos. O acesso por clientes ou agentes externos deve ser previamente avaliado e autorizado pela equipe de InfoSec.

Grupo TC
Av. Presidente Jucelino Kubitschek, n°1.830 - Torre 2 - 5° Andar
Vila Nova Conceição – São Paulo – SP - 04543-01

tc.com.br
+55 11 4003-6048

2. Documentos Relacionados

A construção desta política, bem como os procedimentos e normas inerentes a seu cumprimento observam, além das disposições internas das Políticas, procedimentos e disposições contratuais, as disposições regulatórias, autorregulatórias e legais:

- ABNT NBR ISO/IEC 27001:2013 –Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos;
- ABNT NBR ISO/IEC 27002:2013 –Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação;
- ABNT NBR ISO/IEC 27701:2019 – Tecnologia da Informação – Técnicas de segurança – Gestão da privacidade da informação — Requisitos e diretrizes;
- Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei 13.709/2018;
- Lei de Acesso à Informação (LAI) 12.527 de 18/11/2011;
- Resolução CVM nº 35/2021;
- Resolução CMN nº 4893/2021;
- Programa de Qualificação Operacional (versão roteiro 2024);
- Norma de Continuidade de Negócios;
- Norma de Gestão de Acesso;
- Norma de Gestão de Backups;
- Norma de Gestão de Contratos;
- Norma de Gestão de Criptografia;
- Norma de Gestão de Hardware;
- Norma de Gestão de Identidade;
- Norma de Gestão de Incidentes;
- Norma de Gestão da Informação;
- Norma de Gestão de Malwares;
- Norma de Gestão de Monitoração;
- Norma de Gestão de Mudanças;
- Norma de Gestão de Patches;
- Norma de Gestão de Prontidão;
- Norma de Gestão de Redes;
- Norma de Gestão de Serviços;
- Norma de Gestão de Softwares;
- Norma de Gestão de Telefonia;
- Norma de Gestão de Treinamento;
- Norma de Gestão de Vulnerabilidades;
- Norma de Prevenção a Ataques Cibernéticos.

Grupo TC
Av. Presidente Jucelino Kubitschek, n°1.830 - Torre 2 - 5° Andar
Vila Nova Conceição – São Paulo – SP - 04543-01

tc.com.br
+55 11 4003-6048

3. Dicionário de dados

Neste documento, aplicam-se os seguintes termos, definições ou abreviações:

- PSI - Política de Segurança da Informação e Cibersegurança;
- InfoSec – equipe de Segurança da Informação;
- SGSI - sigla para Sistema De Gestão De Segurança Da Informação;
- Acesso – capacidade de ingressar/entrar em algum sistema ou ambiente;
- Identidade – característica ou atributo que identifica unicamente o indivíduo;
- Segregação de funções – separação das funções na empresa segundo suas permissões e atribuições;
- Vulnerabilidades – ponto com fragilidade que pode ser explorada;
- Ataques – ações deliberadas visando explorar vulnerabilidades existentes;
- Malwares – software malicioso projetado para prejudicar ou explorar dispositivos, serviço ou rede;
- Antivírus – programa de computador para detecção e eliminação de malwares;
- Hardware – termo para identificar os componentes físicos de uma estrutura de tecnologia;
- Software – termo para identificar programas e instruções voltadas a fazer o hardware funcionar;
- Patches – atualizações voltadas a correção de algum erro ou fragilidade de um software;
- Redes – dispositivos de computação interconectados que podem trocar dados e compartilhar recursos entre si;
- Ambiente produtivo – ambiente voltado a instalação de sistemas para uso de usuários finais;
- Ambiente de desenvolvimento – ambiente voltado para os desenvolvedores para o desenvolvimento de sistemas;
- Ambiente de homologação – ambiente voltado a validar a conformidade dos sistemas desenvolvidos antes de sujeitá-los ao ambiente produtivo;
- Ambiente da matriz – local que hospeda a matriz da empresa;
- Criptografia – mecanismo utilizado para cifrar alguma informação evitando acesso por pessoas desautorizadas;
- Backup – mecanismo de cópia de dados visando redundância em caso de desastre.

Grupo TC
Av. Presidente Jucelino Kubitschek, n°1.830 - Torre 2 - 5° Andar
Vila Nova Conceição – São Paulo – SP - 04543-01

tc.com.br
+55 11 4003-6048

4. Diretrizes

Esta política visa estabelecer normas e procedimentos necessários para proteger as informações e os sistemas de uma organização contra ameaças e ataques cibernéticos.

4.1. Objetivo

O objetivo dessa Política é:

- Proteger os ativos de informação do TC contra acessos não autorizados, divulgações, modificações, destruições indevidas ou interrupções não planejadas;
- Garantir a confidencialidade, integridade e disponibilidade das informações e dos sistemas de informação, bem como assegurar o cumprimento das regulamentações e normas aplicáveis, e
- Minimizar riscos e impactos de incidentes de segurança, promovendo uma cultura de segurança cibernética entre todos os colaboradores e partes interessadas.

4.2. Papéis e Responsabilidades

Todas as áreas, colaboradores, prestadores e prepostos são responsáveis por zelar pela aplicação da Política de Segurança da Informação. Alguns perfis/áreas, entretanto, possuem atribuições destacadas, a citar:

- **Diretoria de Compliance, Risco e Segurança da Informação**
    - Elaborar e revisar a Política de Segurança da Informação anualmente ou sempre que se fizer necessário;
    - Avaliar e apresentar a efetividade e eficácia da segurança sobre todas as tecnologias empregadas e operações;
    - Garantir ações educacionais aumentando o nível médio de conhecimento dos colaboradores sobre segurança da informação;
    - Participar das revisões dos procedimentos nos casos de alterações nos sistemas de informação;

Grupo TC
Av. Presidente Jucelino Kubitschek, n°1.830 - Torre 2 - 5° Andar
Vila Nova Conceição – São Paulo – SP - 04543-01
tc.com.br
+55 11 4003-6048

- Apoiar nas análises de possíveis incidentes envolvendo informações confidenciais ou dados pessoais/sensíveis;
- Garantir a manutenção da matriz de segregação gerenciando as concessões de acesso e permissionamentos;
- Disseminar a cultura de Segurança da Informação e Cibernética;
- Acompanhamento da aderência da empresa quanto a LGPD;
- Analisar e acompanhar auditorias, pentests e plano de ações.

- **Comitê Tecnologia, Segurança da Informação e Dados**

  - Aprovar as normas e procedimentos gerais relacionados à tecnologia, segurança da informação e dados;
  - Designar, definir ou alterar as atribuições das áreas de Tecnologia, Áreas de Segurança da Informação e de Dados;
  - Aprovar as principais iniciativas para a melhoria contínua das medidas de proteção para detectar vulnerabilidades e artefatos maliciosos, monitorar e analisar possíveis ataques;
  - Apoiar a implantação de soluções para eliminação ou minimização dos riscos;
  - Estabelecer uma relação consistente das estratégias de negócios e da Tecnologia da Informação com os aspectos de segurança, dados e continuidade do negócio;
  - Suportar as iniciativas das áreas de Tecnologia, Áreas de Segurança da Informação e de Dados;
  - Garantir a recuperação dos sistemas de informação e dos dados.

- **Diretoria de Tecnologia**

  - Garantir o cumprimento desta Política e dos normativos internos e externos, que regulam a atividade de Segurança da Informação e Cibersegurança;
  - Colaborar com a Diretoria de Compliance, Risco e Segurança da Informação na evolução e atualização dessa Política.

- **Colaboradores, terceiros, fornecedores, parceiros e partes Interessadas no TC**

  - Preservar a integridade e guardar sigilo das informações;
  - Zelar e proteger os equipamentos disponibilizados pela empresa;
  - Transitar informações somente nos canais oficiais;

Grupo TC
Av. Presidente Jucelino Kubitschek, n°1.830 - Torre 2 - 5° Andar
Vila Nova Conceição – São Paulo – SP - 04543-01

tc.com.br
+55 11 4003-6048

- Comunicar ao superior imediato qualquer irregularidade;
- Cumprir as determinações desta Política.

4.3. Comitê Executivo

Foi estabelecida a criação de um Comitê Organizacional específico para análise das demandas extraordinárias no âmbito de Tecnologia de Informação, sendo então nomeado como: Comitê de Tecnologia, Segurança da Informação e Dados. Este Comitê é composto por:

- CEO
- Co-CEO;
- CTO;
- Diretora de Compliance;
- Head de Operações;
- Head de Segurança da Informação;
- Head de Infraestrutura;
- Head de Dados;
- Head de Riscos;
- Auditoria Interna (sem direito a voto).

4.3.1. Frequência e Controle

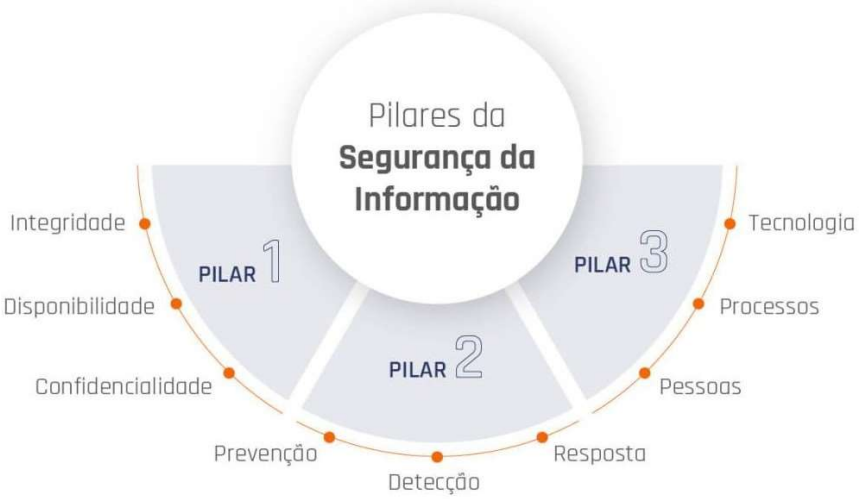
Os membros do Comitê de Tecnologia, Segurança da Informação e Dados se reunirão trimestralmente ou extraordinariamente quando necessário. Todas as reuniões serão registradas em Ata para garantir a confirmação das ações e decisões, por parte de todos.

4.4. Governança Corporativa – SGSI

O sistema de gestão da Segurança da informação é composto por 3 Pilares, sendo:

Grupo TC
Av. Presidente Jucelino Kubitschek, n°1.830 - Torre 2 - 5° Andar
Vila Nova Conceição – São Paulo – SP - 04543-01

tc.com.br
+55 11 4003-6048



A importância de cada um dos pilares na eficiência e eficácia da Governança de Segurança da Informação e Cibersegurança:

Pilar 1:
Integridade – assegurar que as informações não sejam alteradas durante seu tráfego, armazenamento ou processamento; **Disponibilidade** – garantir que a informação esteja disponível sempre que necessário; **Confidencialidade** – proteger as informações, garantido que elas trafeguem de forma segura e sigilosa, garantindo acesso somente por devidamente pessoas autorizadas.

Pilar 2:
Prevenção – aplicar medidas de controles preventivos para a proteção dos ativos; **Detecção** – estabelecer controles de monitoramento e diagnósticos tempestivos do ambiente de controle de SI; **Resposta** – assegurar a criação tempestiva de soluções e controles que garantam a minimização ou mitigação dos riscos de incidentes.

Pilar 3:
Pessoas – treinar e orientar todos os colaboradores, clientes, parceiros e acionistas sobre o cenário e as questões de segurança da informação na Companhia; **Processos** – estabelecer políticas, normativos, procedimentos e controles que assegurem as atividades de Segurança da Informação;

Grupo TC
Av. Presidente Jucelino Kubitschek, n°1.830 - Torre 2 - 5° Andar
Vila Nova Conceição – São Paulo – SP - 04543-01

tc.com.br
+55 11 4003-6048

Tecnologia – assegurar que as ferramentas e aplicações utilizadas para prevenção, detecção e resposta estão em conformidade e atendam as necessidades da Companhia.

4.5. Processos – SGSI:

Todos os normativos que regulam a conformidade dos processos sob responsabilidade da área de Segurança da Informação e Cibersegurança, encontram-se disponíveis na "Intranet – Governança Corporativa - SGSI". Sendo:

Gestão de acesso: o acesso às informações e aos ambientes do TC deve ser permitido apenas às pessoas autorizadas, levando-se em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

Gestão de identidade: a gestão de credenciais no ambiente do TC deve implementar critérios rígidos de complexidade de senha e segundo fator de autenticação (quando aplicável).

Gestão de Vulnerabilidades: processo contínuo de identificação, avaliação e mitigação de vulnerabilidade em sistemas, redes e aplicativos, através da realização regular de testes de penetração (pentests), análise de resultados e priorização de correções com base em critérios associados a matriz de risco.

Gestão de Treinamentos: promover uma cultura de segurança, incentivando comportamentos proativos e responsáveis entre os funcionários. Validações regulares e feedbacks são integrados ao processo para garantir a eficácia contínua dos treinamentos e a adaptação às ameaças emergentes, fortalecendo assim a postura de segurança da informação da organização em um ambiente digital em contante evolução.

Prevenção a Ataques Cibernéticos: diversos sistemas de reconhecimento de padrões que analisam a comunicação entrante no ambiente produtivo identificando comportamento suspeitos, alertando-os ou mesmo bloqueando-os preventivamente.

Gestão de Malwares: é a instalação de agentes de antivírus em todo o parque de máquinas da empresa e a configuração adequada dos firewalls para o correto isolamento de ambientes evitando a propagação de uma possível infecção.

Grupo TC
Av. Presidente Jucelino Kubitschek, n°1.830 - Torre 2 - 5° Andar
Vila Nova Conceição – São Paulo – SP - 04543-01

tc.com.br
+55 11 4003-6048

Gestão de Hardware: é aplicada na preservação da confidencialidade, integridade e disponibilidade das informações contidas nos equipamentos da Companhia.

Gestão de Software: é o controle dos softwares externos instalados em seu ambiente, definindo uma lista de softwares homologados pelo time de Infraestrutura e InfoSec em quesitos de segurança e uso de recursos.

Gestão de Patches: estabelece procedimentos claros para a identificação, avaliação, implementação e monitoramento de patches em todos os dispositivos e sistemas críticos. Com um foco na minimização de vulnerabilidades e na manutenção da integridade operacional, a política assegura que todos os patches sejam aplicados de maneira oportuna e segura, com a realização de testes controlados antes da implementação geral.

Gestão de Telefonia: estabelece procedimentos e diretrizes para a gravação de chamadas telefônicas, é onde se define os critérios de longevidade do armazenamento, restrição ao acesso e recuperação, assim como mecanismos de monitoramento e auditoria.

Gestão de Serviços: estabelece controles de filtragem, monitoração e moderação da comunicação, independentemente do canal utilizado (internet, e-mail e mensageria instantânea).

Gestão de Redes: estabelece diversos mecanismos voltados a segregação e segurança da rede corporativa. Os ambientes produtivos, dos ambientes de homologação/desenvolvimento e o ambiente da matriz são segregados

Gestão de Prontidão: visa medir a prontidão dos serviços oferecidos a seus clientes antes do horário do expediente comercial. Tais verificações visam antecipar o diagnóstico e as tratativas de não conformidades não alertadas espontaneamente pelos mecanismos de monitoração.

Gestão de Criptografia – estabelece um conjunto de requisitos para o uso adequado de controles criptográficos para proteger as informações sensíveis ou confidenciais contra acesso não autorizado e para manter a integridade dos dados.

Gestão de Contratos: estabelece um fluxo detalhado na gestão de contratos, assegurando que estejam alinhados com a política de segurança da informação da organização e que protejam adequadamente os ativos de informação.

Grupo TC
Av. Presidente Jucelino Kubitschek, n°1.830 - Torre 2 - 5° Andar
Vila Nova Conceição – São Paulo – SP - 04543-01

tc.com.br
+55 11 4003-6048

Gestão da Informação: estabelece parâmetros claros para a correta classificação da informação durante todo o seu clico de vida. Essa classificação permite regular a rigidez dos processos de controle no trânsito, armazenamento, tratamento, monitoramento e descarte da informação, preservando a segurança de informações confidenciais da empresa e/ou dos clientes.

Gestão da Monitoração: define critérios mínimos de configuração dos sistemas e dispositivos para gerar e armazenar logs com os níveis de detalhamento necessários para o rastreio dos eventos e atendimento dos requisitos regulatórios.

Gestão de Backups: Assegura que os dados da organização possam ser recuperados em casos de falhas, desastres ou incidentes de segurança.

Gestão de Incidentes: estabelece diretrizes e responsabilidades para o tratamento de incidentes, visando garantir uma resposta rápida e eficaz a incidentes que possam comprometer a confidencialidade, integridade e disponibilidade das informações da organização.

Gestão de Mudanças: estabelece diretrizes para a gestão de mudanças, visando controlar e coordenar as alterações no ambiente de TI.

5. Revisões e Atualizações

Essa política deverá ser revisada anualmente ou sempre que algum elemento relevante justifique sua atualização, seja de negócio, ambiente, sistema, regulatório ou jurídico. Após revisada a política deve ser aprovada pelo Comite de Tecnologia, Segurança da Informação e Dados, substituindo a versão anterior.

Grupo TC
Av. Presidente Jucelino Kubitschek, n°1.830 - Torre 2 - 5° Andar
Vila Nova Conceição – São Paulo – SP - 04543-01

tc.com.br
+55 11 4003-6048

6. Controle de Versão

Informações Básicas

Título	Política de Segurança da Informação e Cibersegurança
Versão	1.00
Aprovador	Conselho de Administração
Data da elaboração	12/11/2024
Data da aprovação	28/03/2025
Data da próxima revisão	28/03/2026
Area proprietária	Segurança da Informação

Histórico de Revisão

Versão:	Motivo de Alteração	Autor	Aprovado em:
1.00	Versão Inicial	Luis Serrano	28/03/2025

Grupo TC
Av. Presidente Jucelino Kubitschek, n°1.830 - Torre 2 - 5° Andar
Vila Nova Conceição – São Paulo – SP - 04543-01

tc.com.br
+55 11 4003-6048