Política de Segurança da Informação

Companhia de Tecnologia e Desenvolvimento S.A.

Versão 1.0

Política de Segurança da Informação
Companhia de Tecnologia e Desenvolvimento S.A.

1. INTRODUÇÃO

Esta Política de Segurança da Informação orienta e estabelece as diretrizes corporativas da Companhia de Tecnologia e Desenvolvimento S.A., para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação e em concordância com a legislação vigente e com o Código de Conduta da companhia.

2. OBJETIVO

Declarar o comprometimento da Companhia de Tecnologia e Desenvolvimento S.A., com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para efetivar a gestão de Segurança da Informação.

Os objetivos das ações a serem implementadas são a salvaguarda dos dados, das informações e materiais sensíveis, críticos e sigilosos de interesse da Companhia de Tecnologia e Desenvolvimento S.A., dos sistemas computacionais, suas instalações e das áreas de trabalho, além da preservação da inviolabilidade e da intimidade da vida privada, da honra e da imagem das pessoas. Integram também a Politica de Segurança da Informação normas e procedimentos complementares destinados à proteção da informação e a disciplina de sua utilização.

Preservar as informações quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- **Confidencialidade:** garantia de que o acesso à informação somente esteja disponível, ou seja, revelada a pessoa, a sistema, a órgão ou a entidade devidamente autorizados.
- **Disponibilidade:** garantia de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado a sistema, a órgão ou a entidade devidamente autorizados.

3. APLICAÇÕES

Esta politica se aplica:

- Aos administradores, aos empregados ativos, aos ocupantes de cargo em comissão, aos cedidos à companhia, aos terceirizados, estagiários e empregados de qualquer natureza jurídica que executem atividades vinculadas à companhia;
- Às informações armazenadas em meios físicos de propriedade ou sob a guarda da companhia;
- A todos os ambientes computacionais e informações neles armazenadas, pertencentes ou sob a guarda da companhia;
- Às contratações, convênios, acordos, termos e outros instrumentos contratuais celebrados pela companhia.

4. CONCEITOS E DEFINIÇÕES

Para efeitos desta Politica de Segurança da Informação, adotam-se as seguintes conceituações:

- **Acesso:** possibilidade de consulta ou reprodução de documentos e arquivos
- **Ativo:** qualquer bem, tangível ou intangível, que tenha valor para a companhia;
- **Ativo de informação:** ativo que guarda informações da companhia;
- **Classificação da informação:** identificação dos níveis de proteção das informações e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;
- **Dado:** informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;
- **Dado pessoal:** informação relacionada à pessoa natural identificada ou identificável;
- **Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- **Incidente de segurança:** indício de fraude, sabotagem, desvio, falha, perda ou evento indesejável ou inesperado que tenha probabilidade de comprometer sistemas de informação ou de redes de computadores;
- **Segurança da informação:** está diretamente relacionada com proteção de um

conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização;

- **Gestor da Informação:** responsável pela administração das informações geridas nos processos de trabalho sob sua responsabilidade;
- **Usuário:** qualquer indivíduo ou instituição que tenha acesso autenticado aos recursos da rede corporativa da Companhia de Tecnologia e Desenvolvimento S.A.

5. PRINCÍPIOS

Para atingir seus objetivos esta política estabelece diretrizes de segurança, que são baseadas nos seguintes princípios:

- Proteção dos dados pessoais para a garantia do direito fundamental à inviolabilidade da privacidade e intimidade;
- Zelo pela proteção das informações, independente do meio em que estão armazenadas ou do ambiente em que estejam sendo processadas ou transitando;
- Adoção de medidas de segurança adaptáveis para atender às necessidades dos serviços e suportar a evolução tecnológica;
- Adequação dos custos das ações de Segurança da Informação ao valor dos ativos e informações, considerando os riscos a que estão expostos, seguindo critérios de proporcionalidade;
- Trabalhar prioritariamente de forma preventiva para obtenção dos objetivos de segurança da informação.

6. DIRETRIZES

São diretrizes de Segurança da Informação da Companhia de Tecnologia e Desenvolvimento S.A.:

- **Responsabilidade e comprometimento:** Compreender que a Segurança da Informação é responsabilidade de todas as pessoas abrangidas pela Política de Segurança da Informação;
- **Treinamento e conscientização:** Estabelecer iniciativas e programas que fomentem a cultura de Segurança da Informação na Companhia de Tecnologia e Desenvolvimento S.A.;

- **Gestão de riscos:** Avaliar riscos de Segurança da Informação por meio de processos contínuos, com abrangência das fases de análise, avaliação e tratamento dos riscos;

- **Classificação de segurança e tratamento da informação:** Classificar as informações para permitir o tratamento adequado, considerando o grau de importância, a criticidade, a sensibilidade e as normas legais;
- **Controle de acesso:** Controlar acessos de qualquer natureza aos ambientes físicos, computacionais ou aplicações, a fim de definir as ações permitidas, e garantir rastreabilidade, identificação do usuário e as ações executadas;
- **Contratações e aquisições:** Incluir nos contratos, acordos, convênios, ajustes e instrumentos congêneres, quando aplicável, especificações de Segurança da Informação que definam, no mínimo, regras de transferência das informações, acordos de confidencialidade e não divulgação, limites de eventuais tratamentos de dados pessoais e obrigação de atendimento às normas da Companhia de Tecnologia e Desenvolvimento S.A., quando pertinentes;
- **Privacidade e proteção de dados pessoais:** Garantir os direitos e a privacidade dos titulares de dados pessoais, e o tratamento destes dados apenas para as finalidades para as quais foram coletados;
- **Desenvolvimento seguro:** Seguir princípios de Segurança da Informação e proteção de dados desde o planejamento e concepção até a execução e acompanhamento em qualquer projeto desenvolvido, internalizado ou mantido pela Companhia de Tecnologia e Desenvolvimento S.A.;
- **Ambiente computacional seguro:** Manter o ambiente de software e hardware atualizado, em particular no que diz respeito a atualizações de segurança, respeitando critérios de proporcionalidade.
- **Identificação segura:** Conceder aos usuários contas pessoais intransferíveis e que não devem ser compartilhadas com outros usuários.

7. NORMAS

Para o cumprimento das diretrizes desta política devem ser derivadas normas de Segurança da Informação, dentro do contexto de cada atividade ou objetivo específico. Se for necessário um detalhamento operacional destas normas, devem ser elaboradas instruções de trabalho

correspondentes.

8. RESPONSABILIDADES

Cabe a todos os abrangidos por esta política:

- Proteger as informações contra uso, acesso, divulgação, modificação ou destruição não autorizados conforme as diretrizes desta política;
- Proteger suas contas pessoais contra o uso indevido.

Cabe aos gestores de pessoas ou de processos:

- Cumprir e fazer cumprir no âmbito de sua atuação esta política, as normas e os procedimentos de segurança da Informação;

9. COMPETÊNCIAS E RESPONSABILIDADES

É de responsabilidade de todos que têm acesso aos ativos da companhia manter níveis de Segurança da Informação adequados, segundo preceitos desta política.

9.1 ALTA DIREÇÃO

É de responsabilidade da alta administração desta companhia prover orientação e o apoio necessário às ações de Segurança da Informação, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes.

9.2 ADMINISTRAÇÃO DO ATIVO DA INFORMAÇÃO

A área detentora do ativo ou conjunto de ativos é responsável por proteger, administrar, manter e controlar o acesso às informações, conforme requisitos definidos neste instrumento e em conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD).

9.3 ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

Compete ao Encarregado pelo Tratamento de Dados Pessoais:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os empregados e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

9.4 EQUIPE DE SEGURANÇA

Compete à Equipe de Segurança:

I - desenvolver, implementar e monitorar estratégias de segurança que atendam aos objetivos estratégicos da Companhia de Tecnologia e Desenvolvimento S.A.;

II - avaliar, selecionar, utilizar, administrar e monitorar controles apropriados de proteção dos ativos de informação;

III - conscientizar os usuários a respeito da implementação desses controles;

IV - verificar se todos os usuários colaboram com as medidas de segurança implantadas.

9.5 GESTOR DO ATIVO DE INFORMAÇÃO

Cabe ao Gestor do Ativo de Informação:

I - tratar e classificar a informação;

II - definir os requisitos de segurança para os ativos sob sua responsabilidade;

III - conceder e revogar acessos;

IV - autorizar a divulgação de informações;

9.6 GESTORES ADMINISTRATIVOS

Cabe aos Gestores Administrativos:

I - multiplicar e catalisar os princípios de segurança;

II - autorizar concessão, transferência e revogação de acessos;

III - responder conjuntamente pelas ações realizadas por seus subordinados;

IV - conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de Segurança da Informação;

V - incorporar aos processos de trabalho de sua área, práticas inerentes à Segurança da informação;

VI - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas

nos casos de comprometimento da Segurança da Informação por parte dos usuários sob sua supervisão;

9.7 TERCEIROS E FORNECEDORES

É responsabilidade dos terceiros e fornecedores:

I - proteger os ativos de informação desta companhia, incluindo informação, evitando perda ou modificação de dados, software e hardware;
II - assegurar o retorno ou a destruição da informação e dos ativos no final do contrato, ou em um dado momento definido no acordo;
III - observar restrições em relação a cópias e divulgação de informações, e uso dos acordos de confidencialidade;
IV - observar restrições em relação à manutenção e instalação de software e hardware;
V - atender à política de controle de acesso desta companhia;
VI - relatar incidentes de Segurança da Informação e violação da segurança ao Encarregado pelo Tratamento de Dados Pessoais; e
VII - atender aos princípios e diretrizes contidos nesta Política de Segurança da Informação, incluindo normas e procedimentos complementares destinados à Segurança da Informação.

9.8 USUÁRIOS

É responsabilidade dos usuários:
I - difundir e exigir o cumprimento da Politica de Segurança da Informação, das normas de segurança e da legislação vigente acerca do tema;
II - proteger os ativos de informação desta companhia, incluindo informação, evitando perda ou modificação de dados, software e hardware;
III - observar restrições em relação a cópias e divulgação de informações, e uso dos acordos de confidencialidade;
IV - observar restrições em relação à manutenção e instalação de software e hardware;
V - atender à política de controle de acesso desta companhia;
VI - relatar incidentes de Segurança da Informação e violação da segurança; e
VII - atender aos princípios e diretrizes contidos nesta Politica de Segurança da Informação, incluindo normas e procedimentos complementares destinados à Segurança da Informação; e

VIII - ser responsável por todos os atos praticados com suas identificações (login, crachá, carimbo, e-mail, assinatura digital, etc).

10. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

A Gestão de Continuidade de Negócios compreenderá um conjunto de normas e

procedimentos que visem assegurar o funcionamento continuo ou recuperação antecipada da Companhia de Tecnologia e Desenvolvimento S.A., quando da ocorrência de indisponibilidade de recursos de infraestrutura, de tecnologia ou de recursos humanos, isolada ou simultaneamente.

O Plano de Continuidade de Negócios da companhia, baseado em metodologias e boas práticas e aprovado pela diretoria, deverá ser desenvolvido, implementado e testado periodicamente para garantir a continuidade dos serviços críticos.

11. AUDITORIA E CONFORMIDADE

A Companhia de Tecnologia e Desenvolvimento S.A., manterá registros e procedimentos, como trilhas de auditoria e outros, que assegurem o rastreamento, acompanhamento, controle e verificação de acessos aos seus ativos de informação, considerando sua criticidade.

A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pelo auditor e aprovado pelo Encarregado pelo Tratamento de Dados Pessoais.

Parágrafo único. Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo auditor ao Encarregado pelo Tratamento de Dados Pessoais, e será montado um plano de ação para a tomada das ações cabíveis.

12. SANÇÕES E PENALIDADES

Ações que violem esta politica, diretrizes, normas e procedimentos, ou que quebrem os controles de Segurança da Informação, serão passíveis de investigação, podendo implicar em penas e sanções legais impostas por meio de medidas administrativas, sem prejuízo das demais medidas cíveis e penais cabíveis.

Processo disciplinar específico poderá ser elaborado para apurar as ações que constituem em

quebra das diretrizes impostas por esta política.

13. DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Esta Politica será complementada por normas, procedimentos e outros documentos pertinentes, os quais serão considerados partes integrantes desta política.

As propostas de alteração ou criação de normas internas sobre Segurança da Informação deverão ser encaminhadas ao Coordenador da área de Tecnologia e Informação.

Após sua publicação, o Encarregado pelo Tratamento de Dados Pessoais deverá dar ampla divulgação da Política a todos os empregados.

A Politica de Segurança da Informação bem como os documentos gerados a partir dela, deverão ser revisada e atualizada sempre que eventos ou mudanças significativas relativas ao tema assim o exigirem.

14. VIGÊNCIA

Esta Politica de Segurança da Informação foi aprovada na 204ª Reunião do Conselho de Administração da Companhia de Tecnologia e Desenvolvimento S.A., sendo que qualquer alteração ou revisão posterior deverá ser submetida a este órgão da administração, passando a vigorar a partir de 01/08/2021.

Rua Deputado Nilson Ribas, 120 | +55 43 3379-3300 | Jd. Bancários | CEP 86062-090 | Londrina | PR
www.ctdlondrina.com.br