Política
Tecnologia da Informação

Versão 2.0 | 02.2025

SUMÁRIO

1. OBJETIVO

Estabelecer os princípios, diretrizes, atribuições e a conduta adotada pela CRDC para organizar a aplicar a tecnologia da maneira mais adequada e otimizada para atender seus objetivos. Disseminar aos colaboradores, fornecedores, prestadores de serviços, parceiros de negócios e clientes as regras a serem adotadas visando garantir a confiabilidade, integridade e disponibilidade das informações de seus clientes e do público em geral.

Nortear o processo de construção das normas e procedimentos específicos, bem como a adoção de controles e tecnologias que visam reduzir as falhas e otimizar os recursos de tecnologia.

2. ALCANCE

Essa Política se aplica a todos os envolvidos diretamente e indiretamente nos processos e negócios da CRDC, incluindo, mas não se limitando aos colaboradores, executivos, fornecedores, prestadores de serviços, parceiros de negócios e clientes. Foi desenvolvida considerando o uso de todos os recursos tecnológicos disponibilizados ou mantidos pela CRDC no processo de coleta, tratamento, armazenamento e destruição das informações necessárias para a execução das atividades para a qual foi contratada.

3. DEFINIÇÕES

Ativos: todos os recursos relevantes para os negócios da CRDC, sejam ativos tecnológicos e não tecnológicos.

Ativos tecnológicos: dispositivo físicos ou digitais, equipamentos ou outros componentes que suportem atividades relacionadas à informação.

Informações: é o conjunto de dados e conhecimentos organizados, de forma que possam constituir referências sobre um determinado acontecimento.

Classificação da informação: é a indicação da importância da informação, realizada com o objetivo de garantir o nível adequado de segurança para a informação.

Ciclo de vida da informação: compõe as etapas de vida da informação e as exposições ao risco de cada etapa. As etapas do ciclo de informação da CRDC são manuseio, armazenamento, transporte e descarte.

Confidencialidade: garantir que as informações sejam de conhecimento exclusivo das pessoas autorizadas.

Integridade: garantir que as informações estejam íntegras, sem modificações indevidas, sejam acidentais ou propositais;

Disponibilidade: garantir que as informações estejam disponíveis no momento necessário.

Criptografia: é o processo de codificar uma informação, tornando-a legível apenas para as pessoas autorizadas.

Proprietário da informação: pessoa responsável perante a CRDC pela informação, responsável por classificar a informação e autorizar os acessos.

Risco: qualquer coisa desconhecida ou incerta que pode causar prejuízo para a CRDC.

Segurança da informação/cibernética: são os esforços pautados por ações que objetivam mitigar os riscos e garantir a confidencialidade, disponibilidade e integridade das informações.

Incidentes de segurança cibernética: todo evento adverso que constituía um risco ou violação da Política de Segurança da Informação e Cibernética e dos sistemas da computação.

Espaço cibernético: a internet, os sistemas de informação, os dispositivos e as tecnologias digitais que dão suporte a infraestrutura e aos serviços.

Ataque cibernético: é a exploração das vulnerabilidades por parte de um agente malicioso com intenção de alcançar um impacto negativo no alvo.

4. REFERÊNCIAS

Essa política foi elaborada com base nas recomendações e definições das seguintes normas e referências:

- Resolução BCB nº 304/2023;
- Cobit 5;
- ITIL 4;
- Código de Ética e Conduta CRDC;

- Política de Segurança da Informação e Cibernética da CRDC.

5. PRINCÍPIOS

A tecnologia é essencial para a entrega dos produtos e serviços da CRDC, sendo que é de suma importância adotar soluções que melhorem e favoreçam o uso eficiente da tecnologia. Assegurando a evolução e as inovações requeridas para os produtos e serviços e visando a sustentabilidade e o crescimento planejado. Os princípios que regem o uso da tecnologia da CRDC são:

a. **Governança de TI:** conjunto de princípios, orientações e processos que garantem que as decisões e ações referentes à administração e ao uso de TI estejam em conformidade com as demandas institucionais;
b. **Gestão de TI:** utilizar, de forma racional, os recursos de TI buscando alcançar as metas organizacionais com planejamento, organização, coordenação, monitoramento e controle;
c. **Conformidade Regulatória:** assegurar que a Companhia cumpra com as normas e regulamentos aplicáveis, especialmente aqueles relacionados à proteção de dados e transparência operacional; e
d. **Inovação:** incentivar a inovação e a otimização operacional por meio de políticas e ações que suportem a evolução tecnológica e a adaptação necessárias ao negócio.

6. GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

A CRDC possui um conjunto de normas e procedimentos que definem as regras, premissas e necessidades para a Gestão dos Serviços de Tecnologia da Informação. São considerados serviços de tecnologia:

a. infraestrutura de TI (*hardware* e *software*);
b. aplicativos corporativos utilizados pelos colaboradores da CRDC para desempenhar suas funções;
c. serviços de colaboração e comunicação;
d. suporte técnico aos usuários;
e. gerenciamento de incidentes e problemas relacionados a serviços de TI;

f. implementação de mudanças e liberações de novas versões de *software* e *hardware*;

g. segurança da Informação da CRDC e seus ativos de TI; e

h. gerenciamento de capacidade.

6.1 Diretrizes para a Gestão de Serviços de Tecnologia

A Gestão de Serviços de TI na CRDC é baseada nas seguintes diretrizes:

a. **foco no negócio:** os serviços de TI devem ser alinhados às necessidades e estratégias de negócio da CRDC, contribuindo para o alcance de seus objetivos;

b. **orientação ao cliente:** os serviços de TI devem ser fornecidos com qualidade, atendendo às necessidades e expectativas dos usuários internos da CRDC;

c. **melhoria contínua:** os processos e serviços de TI devem ser constantemente avaliados e aprimorados para aumentar a eficiência, a eficácia e a satisfação do usuário;

d. **abordagem baseada em processos:** os serviços de TI devem ser gerenciados por meio de processos bem definidos, documentados e padronizados;

e. **responsabilidade e propriedade:** as responsabilidades pela entrega e suporte dos serviços de TI devem ser claramente definidas e atribuídas às equipes responsáveis; e

f. **comunicação efetiva:** a comunicação aberta e transparente com os usuários é essencial para o sucesso da Gestão de Serviços de TI.

7. GESTÃO DE MUDANÇA

A CRDC adota um processo de gestão de mudança que prioriza entregas contínuas sem impactos e riscos para os clientes e parceiros. São consideradas mudanças, no âmbito de tecnologia, qualquer alteração que modifique ou transforme o funcionamento de uma plataforma, *software* ou infraestrutura de T.I., incluindo, mas não se limitando a:

a. mudanças em processos, procedimentos e políticas;

b. mudanças em sistemas da informação;

c. mudanças em infraestrutura de tecnologia;

d. mudanças de *hardware*, *software* e *firmware*; e

e. mudanças estruturais na Companhia.

7.1 Diretrizes para a Gestão de Mudanças

a. **foco no cliente:** as mudanças devem ser implementadas para atender às necessidades dos clientes e stakeholders;

b. **planejamento e comunicação eficazes:** as mudanças devem ser cuidadosamente planejadas e comunicadas aos *stakeholders* de forma clara e concisa;

c. **minimização do impacto:** as mudanças devem ser implementadas de forma a minimizar o impacto negativo nas operações da Companhia;

d. **gerenciamento de riscos:** os riscos associados à mudança devem ser identificados, avaliados e mitigados; e

e. **aprendizado contínuo:** as lições aprendidas com as mudanças devem ser documentadas e utilizadas para melhorar o processo de gestão de mudanças no futuro.

8. AQUISIÇÕES, CONTRATAÇÃO E GESTÃO DE SERVIÇOS DE TERCEIROS

A CRDC possuí um conjunto de normas e procedimentos específicos que definem as regras, premissas e necessidades, o monitoramento e os controles necessários para as atividades de aquisições e contratação e gestão de serviços de terceiros. Como aquisições entende-se o processo de compra de qualquer equipamento, plataforma, licença e *software* embarcado. Como serviços de terceiros entende-se: desenvolvimento de sistemas, processamento e armazenamento em nuvem, serviços no modelo IaaS (*Infrastructure as a Service*), PaaS (*Plataform as a Service*) e SaaS (*Software as a Service*), serviços de segurança da informação, serviços de infraestrutura, serviços de auditoria e consultorias, implementação de soluções de *software* prontas (COTS), serviços de tecnologia e comunicação (TIC).

8.1 Diretrizes para Aquisições, Contratação e Gestão de Serviços de Terceiros

a. **alinhamento com os requisitos de negócio:** as aquisições devem atender às necessidades e expectativas da Companhia, contribuindo para a realização de seus objetivos estratégicos;
b. **qualidade e confiabilidade:** as aquisições devem atender aos requisitos de qualidade, confiabilidade e segurança;
c. **eficiência e otimização de recursos:** a eficiência e a otimização de recursos financeiros são a base dos processos de aquisições, as escolhas sempre devem priorizar o melhor custo-benefício;
d. **conformidade com normas e requisitos:** as aquisições devem estar em conformidade com todas as normas e requisitos aplicáveis; e
e. **sustentabilidade e responsabilidade social:** as aquisições devem considerar critérios de sustentabilidade e responsabilidade social, priorizando fornecedores que adotam práticas éticas e ambientalmente responsáveis
f. **governança corporativa e gestão de riscos e compliance:** práticas de governança corporativa, gestão de riscos e compliance robustas e proporcionais à relevância do serviço a ser contratado e aos riscos envolvidos devem ser adotadas;
g. **contratos claros e abrangentes e alinhados a regulamentações:** os contratos com terceiros devem priorizar a clareza em suas clausulas e a segurança dos dados e recursos envolvidos, refletindo os requisitos legais e regulamentares aplicáveis;
h. **gerenciamento e monitoramento de serviços:** devem ser implementados mecanismos, adequados ao tamanho e complexidade, para o gerenciamento e monitoramento contínuo dos serviços prestados por terceiro;
i. **segurança da informação:** a CRDC adota medidas rigorosas de segurança da informação, visando proteger seus dados, sistemas e *softwares*, de acordo com as melhores práticas e as normas do setor financeiro. Estas medidas devem ser consideradas ao contratar e gerir um serviço; e
j. **conformidade regulatória:** devem existir rotinas de acompanhamento e monitoramento, garantindo que estejam em conformidade com as leis e regulamentações aplicáveis;

k. **análise de riscos e necessidades:** toda contratação deve ser precedida de uma análise aprofundada dos riscos e necessidades da CRDC;

l. **seleção rigorosa de provedores:** devem ser definidos processos rigorosos de seleção de provedores de serviços, considerando critérios técnicos, de segurança, de compliance, de custo-benefício e de reputação do mercado. Sendo necessário que os provedores selecionados aceitem os termos de tratamento dos provedores críticos de serviços, quando aplicável;

m. **gerenciamento de contratos:** os processos de governança e gerenciamento de contratos devem ser respeitados, garantindo o cumprimento das obrigações contratuais, por parte do provedor de serviços, incluindo monitoramento de desempenho, controle de custos, avaliação de riscos e auditorias periódicas.

9. *BACKUP* DAS INFORMAÇÕES

A CRDC, considerando a importância da disponibilidade contínua de seus dados e sistemas, estabelece um conjunto de norma e procedimentos para tratar o *backup* de seus dados e infraestrutura. Sendo que todo processo de *backup* é baseado na metodologia 3-2-1, sendo:

- **3 cópias**: cópia primária, cópia secundária e cópia de arquivos;
- **2 formatos**: cópia *online* e cópia *offline*; e
- **1 local**: armazenamento em nuvem.

9.1 DIRETRIZES PARA O SERVIÇO DE *BACKUP*

a. **frequência adequada:** frequência do *backup* é definida considerando a especificidade de cada produto, serviço ou tipo de recurso. Também são considerados fatores como a criticidade dos dados, a taxa de alteração dos dados e os requisitos e exigências regulatórias e legais;

b. **disponibilidade e integridade:** é essencial realizar testes periódicos nos *backup*s para assegurar que as rotinas de execução estejam ocorrendo de maneira adequada e para confirmar a integridade dos dados salvos.

c. **proteção de dados:** é primordial que os padrões de segurança empregados aos dados em ambiente produtivo sejam igualmente implementados nos *backups* armazenados.

10. CONTINUIDADE DE NEGÓCIOS

A CRDC possui um conjunto específico de documentos e procedimentos, desenvolvidos com base nos *frameworks* mais utilizados para o tema e, em total consonância com as normas e regulamentações vigentes. A estrutura de contingência é um requisito importante, sendo considerada vital ao contratar ou disponibilizar qualquer serviço de Tecnologia relevante.

11. DESENVOLVIMENTO DE SOFTWARE

A CRDC possui um conjunto específico de normas e procedimentos, estruturados para garantir que seus sistemas sejam desenvolvidos e mantidos de acordo com as melhores práticas e lógicas de desenvolvimento de sistemas. Atendendo aos requisitos legais e normativos; e assegurando a proteção dos dados, confiabilidade dos sistemas e a qualidade do software.

11.1 Diretrizes para o Desenvolvimento de Software

As seguintes diretrizes são adotadas no processo de desenvolvimento e na manutenção de *softwares* na CRDC:

a. **planejamento:** no momento de planejar o desenvolvimento do software é importante que os objetivos e requisitos sejam definidos com claridade e precisão;
b. **gerenciamento de projetos:** um plano de projeto que inclua as atividades de segurança da informação, análise de riscos, e testes deve ser desenvolvido;
c. **desenvolvimento de software:** práticas que incorporem a revisão de código-fonte, controles que garantam a segurança do software e processos de revisão regular para identificar e corrigir vulnerabilidades devem ser implementadas;

d. **testes:** um roteiro de testes abrangente e exaustivo, que incluía os requisitos de segurança que deve ser aplicado;

e. **implementação:** a implementação de um novo *software* ou de uma funcionalidade para um *software* já existente, deve respeitar os procedimentos do processo de gestão de mudança;

f. **manutenção:** os sistemas devem ser monitorados em busca de ameaças a segurança e falhas que possam afetar seu desempenho ou disponibilidade. Atualizações constantes devem ser realizadas para manter o *software* livre de vulnerabilidades e *bugs*; e

g. **suporte:** o processo de atendimento de suporte e gestão de incidentes devem ser realizados de forma clara e eficaz.

12. ESTRATÉGIAS DE TECNOLOGIA

Para atender aos princípios e cumprir as diretrizes dessa política, bem como contribuir para o alcance dos objetivos e metas da CRDC, serão formulados os seguintes planos:

- **Planejamento Estratégico de Tecnologia (PETI):** o PETI será elaborado em harmonia com o Plano Estratégico da CRDC (PE), normas, leis e regulamentações vigentes e aplicáveis a CRDC.
- **Plano Diretor de Tecnologia da Informação (PDTI):** o PDTI será elaborado em harmonia com o Planejamento Estratégico de Tecnologia (PETI), com o Plano Diretor de Segurança da Informação (PDSI) e alinhado com o orçamento corporativo e com as boas práticas de governança de Tecnologia da Informação.

12.1 DIRETRIZES PARA O DESENVOLVIMENTO DAS ESTRATÉGIAS DE T.I

As seguintes diretrizes são adotadas no processo de desenvolvimento e na manutenção de *softwares* na CRDC:

a. **visão de longo prazo:** o planejamento estratégico de tecnologia deve ser orientado para o futuro, estabelecendo metas e objetivos que reflitam os objetivos da Companhia em um horizonte de tempo mais extenso;

b. **análise abrangente:** uma análise detalhada do ambiente interno e externo é crucial. Isso inclui a análise SWOT (*Strengths, Weaknesses, Opportunities, Threats*), que ajuda a identificar os pontos fortes e fracos da Companhia, bem como as oportunidades e ameaças no ambiente externo.
c. **alinhamento organizacional:** o planejamento estratégico deve estar alinhado com a missão, visão e valores da Companhia;
d. **alinhamento com os objetivos do negócio:** o planejamento estratégico de TI deve estar em consonância com as metas e objetivos gerais da empresa;
e. **inovação e melhoria contínua:** o planejamento estratégico de TI deve promover a inovação e a busca constante por melhorias nos processos e serviços de TI. Isso envolve estar atento às novas tendências tecnológicas e avaliar como elas podem ser incorporadas para melhorar a eficiência operacional e oferecer novas soluções que agreguem valor ao negócio; e
f. **gestão de riscos e segurança:** a segurança da informação e a gestão de riscos devem ser componentes centrais do planejamento estratégico de TI. É essencial identificar, avaliar e mitigar riscos relacionados à tecnologia para proteger os ativos de informação da empresa e garantir a continuidade dos negócios.

13. RESPONSABILIDADES

São descritas as responsabilidades dos envolvidos, direta e indiretamente, no processo de gestão e governança de Tecnologia da Informação.

13.1 Diretoria e Gestores de equipe

Responsáveis por cumprir e fazer cumprir as determinações presentes nesta política, informando à área responsável pela tecnologia, toda e qualquer ação não condizente às práticas aqui estabelecidas. Deve ainda:

a. viabilizar treinamentos à sua equipe, assim como o acesso a todos os materiais fornecidos pela área de tecnologia;
b. fiscalizar regularmente o cumprimento desta política e demais normas nos locais de trabalho sob sua responsabilidade;

c. participar, junto à Diretoria responsável, da elaboração de matrizes de risco dos sistemas de informação sob sua gestão;
d. atribuir aos colaboradores, na fase de contração e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento desta política.

13.2 Gestão e Governança de Tecnologia da Informação

Responsáveis por estabelecer as políticas, padrões, procedimentos e controles, otimizar e adequar o uso das tecnologias as necessidades da CRDC. Devem ainda:

a. garantir que a TI ofereça serviços rápidos, constantes e de qualidade aos usuários, atuais ou potenciais;
b. definir, priorizar e implementar os projetos que resultem no máximo valor para o negócio, com o mínimo de prazo, custo e risco;
c. liderar, motivar e envolver pessoas, de forma contínua e alinhada, para aprimorar os resultados da TI;
d. incentivar a criatividade, o teste e a aplicação de novas ideias que levem a inovações na área de TI;
e. garantir que a infraestrutura e os serviços de TI sejam resilientes a falhas causadas por erros, desastres e ataques, ou que possam se restaurar com dano mínimo para o negócio;
f. proteger os ativos de informação da organização segundo o grau de criticidade para o negócio e seus respectivos níveis de confidencialidade;
g. garantir que os colaboradores tenham apenas os acessos necessários para o desempenho de suas atividades;
h. gerenciar sistema de controle gerencial que promova a satisfação dos clientes, o aperfeiçoamento de processos, a otimização de recursos e o crescimento de pessoas; e
i. estimular a independência dos grupos de trabalho e a procura pelo desenvolvimento de habilidades técnicas e administrativas;
j. assegurar a conformidade as normas, contratos e padrões aplicáveis;

k. garantir a transparência e o entendimento sobre os benefícios, as estratégias, os custos, os níveis de serviço e outros aspectos relevantes da atuação da TI;
l. organizar o trabalho para aumentar os benefícios da TI, com níveis adequados de riscos e recursos;
m. auxiliar, orientar e incentivar gestores e equipes a atingir os propósitos e resultados da TI;
n. monitorar os resultados e os riscos da TI com vistas a mobilizar pessoas, aprimorar processos, adequar ferramentas e estruturas de TI; e
o. reportar, periódica e consistentemente, os progressos alcançados pela TI.

13.3 Equipes de Tecnologia da Informação

As equipes de tecnologia precisam conhecer detalhadamente e adotar os princípios e diretrizes desta política em todas as ações realizadas em seu dia a dia. Devem ainda:

a. compreender os processos de negócio envolvidos nas soluções de T.I, melhorando a comunicação entre as pessoas e aumentando a habilidade de implementar soluções mais eficientes;
b. realizar as atividades, provenientes de projetos ou operações, de acordo com os princípios, diretrizes, processos e critérios estabelecidos;
c. desenvolver continuamente as competências técnicas e gerenciais dos processos essenciais à governança e à gestão da TI; e
d. engajar partes interessadas em ações de TI que colaborem na execução de processos de TI.

13.4 Risco, Controles INTERNOS E *compliance*

Apoiar as áreas da CRDC na gestão de riscos, avaliação do ambiente de controle, normativas e regulamentações vigentes, sugerindo ações de controle. Deve ainda:

a. manter as áreas informadas sobre alterações legais e/ou regulatórias que reflitam na governança e processos de tecnologia; e
b. supervisionar a gestão de riscos, apoiando a área de Tecnologia da Informação no monitoramento de seus riscos;

13.5 Auditoria Interna

Realizar periodicamente auditorias internas, visando garantir que os sistemas de informação e os processos relacionadas a área de Tecnologia da Informação estejam alinhados aos objetivos estratégicos da Companhia e em conformidade com os normativos internos e externos. A área de Auditoria ainda deve realizar o acompanhamentos dos planos de ação ofertados pela área em decorrência dos eventuais apontamentos e recomendações.

13.6 Segurança da Informação

Atua em conjunto com as equipes de Tecnologia da Informação, sendo suas principais responsabilidades:

a. participar das decisões sempre apontando as melhores soluções no aspecto de Segurança;
b. sugerir as práticas e, acompanhar sua aplicação, nos padrões de desenvolvimento de sistemas e infraestruturas;
c. recomendar práticas e técnicas de segurança, visando garantir a segurança das tecnologias aplicadas aos produtos e serviços da CRDC; e
d. comunicar imediatamente a equipe de Tecnologia da Informação sobre qualquer comportamento suspeito do parque tecnológico.

13.7 Produtos

Responsável por garantir que as boas práticas determinadas pela equipe de Tecnologia da Informação são aplicadas corretamente no decorrer do ciclo de vida dos produtos desenvolvidos pela CRDC. Deve ainda:

a. aceitar e respeitar as especificações técnicas e requisitos técnicos definidos pela área de Tecnologia;
b. garantir que o processo de desenvolvimento é executado conforme as normas específicas;
c. reportar deficiência técnicas que possam prejudicar a evolução dos produtos;
d. garantir que os envolvidos na concepção do produto receberam o treinamento sobre os processos e procedimentos de tecnologia;

e. auditar periodicamente os prestadores de serviço envolvidos no desenvolvimento do produto;
f. garantir o envolvimento da equipe de Tecnologia da Informação nas definições do produto; e
g. garantir a priorização das atividades de adequação técnica nos produtos, atendendo ao acordo de nível de serviço (SLA) de correção por nível de criticidade.

13.8 Comitê de Tecnologia e Segurança da Informação e Cibernética

Responsável por aprovar as estratégias, os objetivos e ações propostas para a mitigar os riscos e aplicar as tecnologias sugeridas pela equipe de Tecnologia Informação. Anualmente receberá o relatório de evoluções das metas de Tecnologia e avaliará o tratamento adotado e as ações de melhoria proposta.

a. alinhar as estratégias, as políticas, os processos, as decisões, os produtos e serviços da TI às necessidades do negócio;
b. estabelecer formatos organizacionais que direcionem o trabalho para a satisfação de demandas, gerando valor dentro de prazos e custos compatíveis;
c. estabelecer processos de gestão que apoiem a definição, a execução e o monitoramento da estratégia de TI; e
d. promover o engajamento dos dirigentes, gestores, usuários, técnicos e demais envolvidos na implementação e manutenção dos processos de TI.

13.9 Colaboradores, fornecedores, prestadores de serviços e parceiros de negócios

Todos precisam conhecer, incorporar e fazer cumprir os termos desta política e as normas que dão suporte, além de observar as seguintes responsabilidades. Restando ainda:

a. compreender o papel e a necessidade da tecnologia e seu impacto em suas atividades diárias;
b. notificar seu superior hierárquico ou as equipes de Tecnologia, caso perceba qualquer anormalidade em seu ambiente de trabalho ou sistemas utilizados em suas atividades diárias;

c. contribuir e disseminar a cultura de proteção e otimização dos recursos tecnológicos;

d. participar e incentivar a participação de seus pares, nos treinamentos de tecnologia da Informação.

14. CONTROLE DE VERSIONAMENTO

Versão	Data	Área responsável	Descrição
1.0	02/05/2024	Tecnologia da informação	Elaboração
2.0	03/02/2025	Tecnologia da informação	Adaptações no texto para aderência a nova política de Segurança da Informação

15. APROVAÇÃO

Declaramos que a presente é cópia fiel da Política de Tecnologia da Informação aprovada na Reunião Ordinária do Conselho de Administração de 03/02/2025.