Política

Segurança da Informação e Cibernética

Versão 4.0 | xx.2025

Classificação: Pública

SUMÁRIO

1. OBJETIVO

Estabelecer os princípios, diretrizes, atribuições e a conduta adotada pela CRDC para proteção e tratamento dos riscos e ameaças relacionadas à Segurança da Informação e Cibernética. Disseminar aos colaboradores, fornecedores, prestadores de serviços, parceiros de negócios e clientes as obrigações a serem adotadas com o objetivo de garantir a confiabilidade, integridade e disponibilidade das informações de seus clientes e do público em geral.

Nortear o processo de construção de normas e procedimentos específicos, bem como a adoção de controles e tecnologias que visam reduzir a vulnerabilidade a incidentes.

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:

- Lei n° 13.709/2018 – Lei Geral de Proteção de Dados Pessoais;
- Resolução BCB n° 304/2023;
- Resolução CMN n° 4.893/2021, como boas práticas;
- Código de Ética e Conduta da CRDC
- ISO/IEC 27.001 – Sistema de gestão de segurança da informação;

- ISO/IEC 27.002 – Código de prática para a gestão da segurança da informação;
- CIS Controls – Center of Internet Security v8; e
- NIST CSF - NIST Cybersecurity Framework v2.

5. PRINCÍPIOS

A segurança é prioridade em todos os processos que manipulam informações na CRDC, sendo os esforços concentrados em garantir a proteção contínua dos dados capturados, tratados e armazenados pelos sistemas.

Os princípios da CRDC são baseados em três pilares:

a. **Confidencialidade:** priorizar as ações que visam garantir que apenas as pessoas autenticadas e autorizadas tomem conhecimento das informações recebidas, manipuladas e enviadas pela CRDC;
b. **Integridade:** adotar tecnologias e processos eficientes, buscando garantir a exatidão, transparência e a completude da informação durante todo o seu ciclo de vida, protegendo-a de modificações indevidas, acidentais ou propositais; e
c. **Disponibilidade:** criar um ambiente tecnológico que garanta a disponibilidade das informações no momento ideal e necessário.

A maior fonte de risco vem do ambiente cibernético, onde a CRDC adota estratégias para prevenir e proteger seus ativos tecnológicos. Ainda assim, caso ocorram incidentes cibernéticos, a equipe está preparada para responder rapidamente, priorizando a recuperação e a disponibilidade da informação, sem impactar sua confidencialidade e a integridade. A inclusão de novas diretrizes ou exceções as atuais serão levantadas e avaliadas pela equipe de Segurança da Informação e Cibernética e submetidas para a aprovação do Comitê Executivo de Segurança da Informação e Cibernética.

6. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações são protegidas e classificadas considerando sua relevância para os negócios da CRDC.

Para cada relevância aplica-se um nível de sigilo, conforme a classificação a seguir:

- **Pública:** seu acesso não é controlado ou registrado, não exige implementação de mecanismos de Segurança da Informação avançados;
- **Interna:** informações relacionadas a assuntos internos da CRDC, sendo que seu acesso é exclusivo para pessoas internas e autorizadas. Embora a CRDC opte por não divulgar as informações classificadas como interna, seu acesso não causa danos sérios a empresa;
- **Confidencial:** tem caráter sigiloso e não pode ser divulgada. Seu acesso é restrito a um determinado número de pessoas com autorização. A divulgação não autorizada destas informações pode causar danos diretos ou indiretos a CRDC; e
- **Restrita:** informação com o mais alto nível de sigilo. Seu acesso é controlado e liberado apenas a um grupo restrito de pessoas previamente designadas. Todos os procedimentos e ferramentas de segurança disponíveis são adotadas para proteger tais informações. Esta categoria compreende as informações de clientes, principalmente os dados pessoais e sensíveis.

A CRDC possui um conjunto de normas e procedimentos específicos que definem as regras, premissas e necessidades, para a atividade de Classificação da Informação.

6.1 Diretrizes para a Classificação da Informação

O processo de Classificação das Informações na CRDC é baseado pelas seguintes diretrizes:

a. **Confidencialidade:** as informações devem ser classificadas com base no impacto que a divulgação não autorizada pode causar;
b. **Somente o necessário:** as informações devem ser classificadas e compartilhadas somente com pessoas ou grupos que realmente precisem ter acesso para a execução de suas funções;
c. **Consciência dos Riscos:** todos os envolvidos devem ter conhecimento dos riscos associados a cada nível de informação e classificá-la de acordo com seu potencial dano a organização ou a indivíduos;

d. **Conformidade regulatória:** é responsabilidade de todos os envolvidos no processo de criação e manipulação garantir que a classificação e o manuseio das informações estejam em conformidade com as leis e regulamentações;

e. **Classificação efetiva:** todos os envolvidos no processo de criação e manipulação de quaisquer informações são responsáveis por sua classificação antes de realizar, ou permitir que realizem, a sua divulgação. Caso receba alguma informação originada na CRDC e não classificada, o participante deve imediatamente classificá-la e notificar o emitente;

f. **Comunicação:** Caso tome conhecimento de alguma informação com tratamento inadequado, deve comunicar imediatamente a área responsável pela informação e a equipe de Segurança da Informação e Cibernética.

7. MANUSEIO DA INFORMAÇÃO

A CRDC adota soluções tecnológicas para garantir que o acesso às informações é pessoal e intransferível, sendo responsabilidade do proprietário a administração das permissões seguindo as diretivas referentes ao manuseio, armazenamento e divulgação das informações autorizadas definidas na norma de classificação de dados.

7.1 DIRETRIZES PARA O MANUSEIO DAS INFORMAÇÕES

As diretrizes definidas devem ser adotadas por todos os envolvidos no processo de manuseio de informações

a. **Uso de Impressoras e Copiadoras:** analisar e respeitar a classificação da informação ao decidir sobre seu envio para impressoras ou copiadoras. O uso dos equipamentos de impressão e fotocópias é exclusivo para as suas atividades profissionais, observando ainda que a impressão de documentos com Informações com classificação Restrita deve ser evitada;

b. **Manuseio de informações não públicas**: no manuseio de informações não publicas deve ser considerado todos os riscos presentes e que possibilitam o vazamento destas informações. Estar atento para não deixar anotações ou manipular

documentos que contenham tais informações em locais de circulação comum, tais como: salas de reunião, corredores, mesas compartilhadas ou outros locais públicos;

c. **Armazenamento e Transporte de Informações não Públicas:** informações não públicas podem ser armazenadas em recursos físicos ou digitais, sempre respeitando as regras de ciclo de vida dos dados e os cuidados, de acordo com a sua classificação. Informações classificadas como Confidencial e Restrita só podem ser movimentadas se existir a possibilidade de recuperação ou análise dos registros. Os dados pessoais de clientes, coletados com a finalidade de atender as obrigações legais, regulatórias ou contratuais, não podem ser armazenados ou transportados em mídias sem a devida proteção dos dados;

d. **Descarte de Informações não Públicas:** O descarte dos documentos físicos e/ou a exclusão de arquivos digitais que contenham informações não públicas deve atender aos seguintes requisitos:

   i **Documentos físicos**: não podem ser descartados no lixo comum, devem ser destruídos utilizando um aparelho fragmentador; e

   ii **Documentos digitais:** as mídias flexíveis, tais como DVD ou CD, devem ser destruídas antes de descartadas. Já as mídias rígidas, tais como disco rígido (HD), unidades sólidas (SSD) e pen drive, devem ser apagadas pela equipe de Segurança da Informação e Segurança Cibernética, utilizando ferramentas específicas.

8. GESTÃO DE ATIVOS

Todos os ativos da CRDC, de seus clientes ou do público em geral são tratados com segurança, ética, sigilo e de acordo com as leis vigentes e normas internas. A gestão dos ativos da CRDC é realizada por seus proprietários designados, que são colaboradores capacitados e nomeados com a responsabilidade de avaliar e aprovar qualquer alteração no processo de controle do ativo.

8.1 DIRETRIZES PARA A GESTÃO DE ATIVOS

As diretrizes no definidas para o processo de gestão e uso dos ativos disponibilizados pela CRDC são:

a. **Responsabilidade e propriedade:** cada ativo tem ao menos um responsável designado, sendo este o encarregado de sua gestão, controle e manutenção ao longo do ciclo de vida do ativo;
b. **Ciclo de vida do Ativo:** o processo de gestão do ativo deve considerar todas as etapas de seu ciclo de vida. Cada fase deve ser planejada e controlada para otimizar os usos e minimizar os riscos e custos;
c. **Valor e Risco:** os ativos devem ser geridos com base no valor que trazem para a organização e nos riscos associados a eles. Informações como custo de substituição, impacto na operação, vulnerabilidades e ameaças calculadas com suas respectivas probabilidades e impactos devem ser avaliadas para garantir uma gestão eficaz;
d. **Inventário Completo e Atualizado:** é primordial manter um inventário preciso e atualizado de todos os ativos, sejam eles físicos (Ex. hardware, infraestrutura) ou intangíveis (Ex. dados, software);
e. **Conformidade Legal e Regulatória:** os ativos devem ser geridos em conformidade com as leis e regulamentações aplicáveis, tanto em termos de proteção de dados, como em licenciamento de software e gestão de equipamentos;
f. **Segurança e proteção:** os ativos, especialmente os digitais, devem ser protegidos contra ameaças, perdas ou danos. Envolvendo a implementação de medidas de segurança adequadas.

9. GESTÃO DE CONTROLE DE ACESSO

A CRDC adota processos eficientes e rígidos para a disponibilização, manutenção e revogação de acesso aos seus sistemas. Para os acessos disponibilizados aos colaboradores, o processo exige o preenchimento do formulário de liberação de acesso, que será posteriormente analisado e aprovado pelo gestor do solicitante e o proprietário do ativo solicitado. Para os clientes, fornecedores, prestadores de serviço e parceiros de negócios, quando necessário, o acesso é liberado seguindo as características previstas no contrato e nos serviços utilizados.

Anualmente, capitaneado pela equipe de Segurança da Informação e Segurança Cibernética é realizado o processo de revisão de acessos.

9.1 Diretrizes para a Gestão de Acesso

a. **Princípio do menor Privilégio:** os acesso aos sistemas, dados e recursos devem ser os estritamente necessários para realizar suas funções;
b. **Controle de Acesso Baseado em Funções (RBAC):** adotar um controle de acesso baseado em funções, onde as permissões são atribuídas de acordo com os papéis desempenhados na CRDC;
c. **Autenticação Multifator (MFA):** sempre que possível, adotar autenticação de multifator para garantir que os acessos aos sistemas mais sensíveis sejam protegidos por mais de um método de verificação, tais como senha, token, biometria ou autenticação via aplicativo;
d. **Revisão Periódica de Acessos:** realizar auditorias e revisões periódicas das permissões de acesso, visando garantir que os usuários não possuam privilégios desnecessários ou excessivos;
e. **Gerenciamento de Credenciais:** garantir políticas rígidas para a criação e o gerenciamento de senhas, como requisitos de complexidade, expiração e proibições de reutilização;
f. **Registro de Acesso e Monitoramento:** manter *logs* detalhados de acesso para identificar atividades suspeitas ou não autorizadas.

10. IDENTIFICAÇÃO, AUTENTICAÇÃO E SENHAS

Os sistemas utilizados na CRDC ou desenvolvidos pela própria CRDC possuem identificação pessoal e adotam políticas de controle de autenticação e senhas.

Cada pessoa, cliente ou funcionário, recebe seu usuário e é responsável pelo seu bom uso, bem como pelos dados por ele acessados. O compartilhamento de senhas é considerado falta grave, podendo sujeitar ao cliente as sanções previstas no contrato dos serviços. Já os colaboradores, caso compartilhem suas senhas, podem estar sujeitos as sanções previstas no Código de Ética e Conduta CRDC.

10.1 Diretrizes para a Identificação, Autenticação e Senha

As diretrizes para a identificação, autenticação e senha nos processos da CRDC são:

a. **Identificação Única:** cada usuário tem sua identificação única para acessar os sistemas e recursos disponíveis, garantindo a rastreabilidade e responsabilidade das ações;

b. **Política de Senhas Fortes:** adotar políticas que fortaleçam as senhas criadas dificultando sua identificação

   i as senhas devem ter um nível mínimo de complexidade que incluam letras maiúsculas e minúsculas, números e, sempre que possível, caracteres especiais;

   ii as senhas devem possuir tamanho mínimo de 8 a 12 caracteres;

   iii não permitir o uso de senhas comuns, tais como números sequenciais, nomes de usuário, nomes genéricos etc.

c. **Expiração e Renovação de Senhas:** exigir que as senhas sejam renovadas periodicamente, principalmente para os casos em que não ocorre o uso de MFAs ou monitoramento de comportamento. Evitar a reutilização de senhas, evitando minimamente a reutilização das últimas 6 (seis) senhas.

d. **Proteção e Armazenamento das Senhas:** todas as senhas armazenadas devem ser protegidas por *hashing*.

e. **Bloqueio de Contas após Tentativas Falhas:** bloquear o usuário após um limite máximo de 10 (dez) tentativas consecutivas de login com falha;

f. **Processo Seguro de Redefinições:** adotar procedimentos seguros para a recuperação de senhas, garantindo a verificação da identidade do usuário. Dar preferência para métodos como o envio de *links* para a redefinição via e-mail verificado ou perguntas de segurança robustas;

g. **Sessões Automáticas de Desconexão:** definir o tempo máximo de inatividade em sistemas sensíveis, desconectando automaticamente o usuário após um período de inatividade.

11. USO DE SOFTWARES

Todos os *softwares* utilizados na CRDC são devidamente licenciados e homologados pela equipe de tecnologia e Segurança da Informação e Cibernética. Apenas a equipe de tecnologia tem permissão para realizar a instalação de *softwares* nas estações, não sendo permitida a instalação, sob qualquer justificativa, por outros colaboradores. Caso seja identificada a necessidade de instalação de um software ainda não homologado, a solicitação deve ser encaminhada a área de tecnologia, que realizará as devidas análises e a posterior homologação.

11.1 Diretrizes para o uso de Softwares

Visando garantir a segurança e o cumprimento das leis relacionadas ao uso de *softwares* a CRDC estabeleceu as principais diretrizes:

a. **Gestão de Licenças:** todas as licenças de *software*, são monitoradas e gerenciadas pela equipe de governança;
b. **Aprovação de *Software*:** qualquer *software* que não seja oficialmente aprovado pela organização deve passar por um processo prévio de aprovação;
c. **Instalação centralizada:** a instalação de *software* é restrita e realizada apenas por colaboradores da área de Tecnologia devidamente autorizados;
d. **Atualizações e *Patches*:** as atualizações críticas de segurança são realizadas automaticamente e controladas por com console centralizado;
e. **Monitoramento e Auditoria:** são realizadas auditorias periódicas com o objetivo de garantir que os *softwares* estejam sendo utilizados de acordo com as políticas da organização e em conformidade com as licenças.

12. USO DE DISPOSITIVOS DE ARMAZENAMENTO REMOVÍVEL

A CRDC não permite o uso de dispositivos de armazenamento removíveis, independentemente de sua característica ou categoria, para o armazenamento de informações classificadas como não públicas. O armazenamento via porta USB é desativado em todos os computadores disponibilizados pela CRDC e, caso ocorram necessidades excepcionais, devem ser encaminhadas para a análise da equipe de Segurança da Informação e Cibernética.

12.1 DIRETRIZES PARA O USO DE DISPOSITIVOS DE ARMAZENAMENTO REMOVÍVEL

As principais diretrizes para o uso de dispositivos de armazenamento removível são:

a. **Exceções restritas:** em situações excepcionais em que o uso de dispositivos removíveis seja necessário, uma autorização formal deve ser concedida pela equipe de Segurança da Informação. A justificativa deve ser registrada, incluindo o propósito, o período de uso e as medidas de segurança aplicadas;

b. **Monitoramento contínuo:** todos os equipamentos devem ser monitorados constantemente permitindo a identificação de tentativas de uso de dispositivos de armazenamento não autorizados;

c. **Alternativas seguras para o compartilhamento:** a CRDC escabece métodos seguros para o compartilhamento de dados, tais como o uso de drives controlados, plataformas de compartilhamento de arquivos autorizados e soluções de nuvem corporativa com criptografia.

13. USO DE E-MAIL CORPORATIVO E FERRAMENTAS DE COMUNICAÇÃO INSTANTÂNEA

A CRDC disponibiliza aos seus colaboradores o serviço de e-mail corporativo e ferramenta de comunicação instantânea, cujo uso é exclusivamente para a execução das atividades relacionadas aos negócios da CRDC. Para o uso destes serviços o colaborador deve respeitar a norma especifica e ter ciência de que os serviços são monitorados e possuem regras de análise de conteúdo com o objetivo de evitar o vazamento de informações não públicas.

13.1 DIRETRIZES PARA O USO DO E-MAIL CORPORATIVO E FERRAMENTAS DE COMUNICAÇÃO INSTANTÂNEA

Para garantir a segurança durante o processo de uso do e-mail corporativo e das ferramentas de comunicação instantânea foram definidas as seguintes diretrizes:

a. **Use exclusivamente profissional:** e-mails e ferramentas de comunicação instantânea devem ser utilizados apara para assuntos relacionados ao trabalho. Evite o uso pessoal e não autorizado destes canais para manter a integridade e a confidencialidade das comunicações da empresa;

b. **Proteção da imagem:** prezando por sua imagem e pela imagem de seus clientes, a CRDC proíbe o envio de mensagens com comentários abusivos, obscenos,

difamatórios ou qualquer outro material que possa trazer má publicidade ou constrangimento a CRDC, seus clientes ou prestadores de serviços;

c. **Proteção de senhas de acesso:** não compartilhar ou permitir compartilhar senhas ou informações de acesso através do e-mail ou ferramentas de comunicação instantânea, com os proprietários ou com terceiros;

d. **Cuidado com *links* e anexos:** evitar abrir *links*, anexos de e-mails ou mensagens de remetentes desconhecidos ou suspeitos;

e. **Confidencialidade das informações compartilhadas:** não compartilhar ou permitir compartilhar informações confidenciais, como dados de clientes, contratos, ou detalhes financeiros, por e-mail ou mensagens. Caso seja inevitável, adotar medidas de proteção como criptografia;

f. **Verificação de destinatários:** revisar cuidadosamente os destinatários antes de enviar um e-mail ou mensagem instantânea, especialmente quando utilizar o "responder a todos" para evitar o compartilhamento acidental de informações confidenciais para destinatários errados ou desnecessários;

g. **Monitoramento e compliance com políticas normas vigentes:** seguir as políticas e normas internas da CRDC sobre o uso de e-mails e ferramentas de comunicação instantâneas. A CRDC pode monitorar e-mails e ferramentas de comunicação instantânea para assegurar as normas de segurança;

h. **Cuidado com respostas automáticas e assinaturas:** ao configurar respostas automáticas, evitar compartilhar informações detalhadas, como datas de ausência e contatos de terceiros. Sempre manter a assinatura profissional e incluir apenas as informações necessárias.

14. PREVENÇÃO CONTRA SOFTWARES MALICIOSOS

A CRDC possui controles para prevenir que quaisquer tipos de softwares maliciosos contaminem e espalhem-se nos sistemas e estações de trabalho de sua rede. Todos os computadores possuem EDRs (*Endpoint Detection and Response*) instalados e monitorados por um sistema de gerenciamento centralizado, garantindo a análise comportamental de todos os

processos em execução nas máquinas de colaboradores, incluindo terceiros prestadores de serviço.

14.1 DIRETRIZES PARA A PREVENÇÃO CONTRA *SOFTWARES* MALICIOSOS

Tendo em vista que a solução de EDR automatiza a instalação e aplicação das políticas para softwares como; Antivírus, *Antimalware*, Redução de Superfície de Ataque, Gerenciamento de Privilégios de Execução, Proteção de Aplicações e Navegadores, Proteção contra *Exploits*, *Firewall*, Filtro de Conteúdo Web e *Criptografia* de Disco, deve-se:

a. ***Baseline* de Configuração*:*** manter uma *baseline* de configuração de segurança capaz de fornecer a proteção necessária para todos os ativos;
b. **Políticas:** manter as políticas de cada módulo atualizadas e seguindo o princípio do menor privilégio;
c. **Abrangência a todos os ativos:** garantir que as políticas de cada módulo estejam aplicadas em todos os ativos da CRDC;
d. **Revisão periódica das políticas:** revisar as políticas de cada módulo periodicamente; e
e. **Reporte de conformidades:** reportar ao Comitê de Tecnologia e Segurança da Informação o status de conformidade das políticas aplicadas nos ativos da CRDC.

15. USO DA INTERNET

O uso da internet nos equipamentos da CRDC tem a finalidade única e exclusiva de atender as necessidades para o desenvolvimento das atividades relacionadas ao negócio da CRDC. Para o uso deste recurso o colaborador deve respeitar a norma específica e saber que todo acesso é registrado e monitorado, sendo vedado o acesso a sites com conteúdo classificados como impróprios e o uso dos recursos da internet para práticas de atividades ilícitas ou que venham a prejudicar a CRDC, seus fornecedores, prestadores de serviço, parceiros de negócio e clientes.

15.1 DIRETRIZES PARA O USO DA INTERNET

As diretrizes para o uso seguro dos recursos da Internet são definidas a seguir e devem ser respeitados por todos os utilizados ou administradores dos recursos de Internet.

a. **Utilizar conexões seguras:** sempre que possível acessar sites utilizando conexões que adotam o protocolo HTTPS, indicado por um cadeado ao lado do endereço do site. Isso garante que a comunicação entre o computador e o site seja criptografada, reduzindo o risco de interceptação de dados.
b. **Verificar a autenticidade de sites:** todos os utilizadores devem validar e chegar a confiabilidade de um site antes de acessá-lo ou digitar dados pessoais ou corporativos.
c. **Limitar o compartilhamento de informações pessoais:** deve ser evitado o fornecimento de informações desnecessárias em sites e redes sociais;
d. **Manter o navegador e extensões atualizados:** o navegador e suas extensões devem estar sempre atualizados. As extensões não utilizadas ou desconhecidas devem ser desativas.

16. CONTROLES CRIPTOGRÁFICOS

A CRDC adota controles criptográficos sempre que identifica a necessidade de proteções adicionais durante o tráfego e armazenamento das informações não públicas. Para a garantia do processo e dos controles criptográficos, seu funcionamento e suas aplicações são descritos em normativo específico.

16.1 DIRETRIZES AO ADOTAR CONTROLES CRIPTOGRÁFICOS

a. **Adotar algoritmos de criptografia seguros e atualizados:** sempre adotar algoritmos de criptografia confiáveis e atualizados. Evitar o uso de algoritmos obsoletos e vulneráveis a ataques;
b. **Implementar criptografia para dados em trânsito e repouso:** sempre que necessário aplicar criptografia para os dados em repouso (armazenados em discos, banco de dados e *backups*) quanto para os dados em trânsito (dados transmitidos em redes internas ou externas).

c. **Gerenciar chaves de criptografias:** adotar o uso de um sistema seguro de gerenciamento de chaves criptográficas, que inclua geração, armazenamento, rotação e destruição das chaves. As chaves devem ser protegidas com políticas rígidas e accessíveis somente a pessoas autorizadas;

d. **Definir políticas de acesso a dados criptografados:** a equipe de segurança deve estabelecer políticas de controle de acesso para dados criptografados. Apenas usuários autorizados devem ter acesso às chaves de descriptografias, e todos os acessos devem ser monitorados e registrados;

e. **Automatizar a rotação periódica de chaves:** a equipe de segurança deve estabelecer políticas para a rotação periódica de chaves criptográficas, minimizando o risco de comprometimento a longo prazo;

f. **Realizar auditorias e monitoramento contínuo:** a equipe de segurança da informação deve realizar regularmente auditorias nos controles criptográficos assegurando a conformidade das políticas e detectando possíveis invasões;

g. **Capacitar equipes sobre práticas de criptografia segura:** a equipe de segurança da informação deve promover treinamentos para a equipe de tecnologia e colaboradores que gerenciam ou acessam dados criptografados;

h. **Planejar a recuperação de dados e *backup* criptografados:** a equipe de segurança da informação deve certificar-se de que o *backup* também seja criptografado e exista um plano de recuperação de dados em caso de falhas;

17. CÓPIAS DE SEGURANÇA

A CRDC possui normativo específico para o tratamento de cópias de segurança, onde estão definidas as tecnologias utilizadas, as regras de periodicidade e de retenção, sempre considerando a criticidade e a disponibilidade exigida pelo ativo envolvido. A equipe de tecnologia é responsável por garantir a execução das rotinas definidas, seu correto armazenamento e proteção.

17.1 DIRETRIZES AO REALIZAR CÓPIAS DE SEGURANÇA

As diretrizes a serem adotadas ao definir e executar o processo de criação de cópias de segurança (*backups*) são:

a. **Definir uma norma de *backup* formal:** a equipe de tecnologia da informação deve estruturar uma norma que defina com clareza o que será copiado, com que frequência, quem é o responsável pelo processo e quais são os procedimentos de recuperação;
b. **Classificar e priorizar dados:** a equipe de tecnologia da informação deve identificar e classificar os dados com base em sua importância e sensibilidade;
c. **Estabelecer uma frequência adequada:** a equipe de tecnologia da informação deve estabelecer uma frequência adequada, que minimiza a perda de dados em caso de incidentes;
d. **Implementar o princípio do *Backup* 3-2-1:** a equipe de tecnologia da informação deve seguir o princípio 3-2-1. Mantendo três cópias dos dados (dados originais e dois *backups*), armazenado em dois locais diferentes;
e. **Automatizar o processo de *Backup*:** o processo de *backup* deve ser automatizado, evitando a possibilidade de falhas humanas e garantindo sua execução conforme a política;
f. **Realizar testes de restauração periódicos:** devem ser realizados testes periódicos de restauração, buscando garantir que os *backups* são recuperáveis e que o processo funciona corretamente;
g. **Monitorar e auditar o processo de *Backup*:** a equipe de tecnologia deve implementar um sistema de monitoramento e auditoria para o processo de *backup*, registrando falhas de acessos.

18. MONITORAMENTO E AUDITORIA DO AMBIENTE

Visando garantir a disponibilidade e a segurança de seus ambientes tecnológicos, a CRDC adota mecanismos de monitoramento e controle automatizados. Especificamente para a segurança dos ambientes a CRDC adota soluções de IDS e IPS para identificação e prevenção de intrusões. Os recursos, os processos de monitoramento, armazenamento de *logs*, auditoria e testes são descritos em normativo específico.

18.1 Diretrizes para o monitoramento e auditoria do ambiente

a. **Definir uma norma de auditoria e monitoramento:** a equipe de segurança da informação deve definir uma norma clara que inclua os objetivos, o escopo, as responsabilidades e o método de análise de dados;
b. **Estabelecer padrões e frequência de auditoria:** a equipe de segurança da informação deve definir os padrões e a frequência dos processos de auditoria;
c. **Implementar *logs* e armazenamento seguro dos dados de auditoria:** deve-se garantir que todos os *logs* de atividades e dados de auditoria sejam armazenados de forma segura e em conformidade com as normas de retenção de dados;
d. **Estabelecer limites e alertas para atividades anômalas:** a equipe de segurança e tecnologia da informação devem configurar limites de comportamento normal para o ambiente e definir alertas para atividades anômalas, tais como tentativas de acesso suspeitas, transferências de doados incomuns ou acessos fora do padrão;
e. **Implementar ações corretivas de não-conformidades:** a equipe de segurança e tecnologia da informação devem definir processos para tratar não-conformidades identificadas nas auditorias, incluindo prazos e responsáveis por implementar as correções.

19. REGISTRO, RESPOSTA E TRATAMENTO A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

A CRDC adota procedimentos para a identificação, resposta e tratamento dos incidentes de Segurança da Informação. As atividades suspeitas identificadas devem ser reportadas através da caixa postal seguranca@crdc.com.br ou ainda pelo formulário disponível no sítio eletrônico da CRDC. Os eventos alertados pelos sistemas de monitoramento de segurança (SOC) da CRDC ou de seus fornecedores seguem as definições do normativo específico.

19.1 Diretrizes para Registro, Resposta e Tratamento de incidentes de Segurança da Informação e Cibernética

A CRDC possuí um conjunto de normas e procedimentos específicos para tratar o tema de registro, resposta e tratamento de incidentes de segurança da informação e cibernética, construídos com base nas seguintes diretrizes:

a. **Estabelecer mecanismos para a detecção precoce e o registro de incidentes:** garantindo que cada evento seja documentado com data, hora, descrição e informações sobre os sistemas afetados;
b. **Classificar os incidentes em diferentes níveis de severidade:** tendo como base o impacto potencial sobre os dados, sistemas, ou operações e no grau de exposição ao risco regulatório e reputacional;
c. **Ter uma equipe multidisciplinar e treinada de resposta a incidente:** pronta para atuar imediatamente após a detecção de um incidente, para mitigar danos e restaurar a operação normal de sistemas e dados afetados;
d. **Implementar um plano de contenção**: isolando a origem do incidente, evitando que ele afete outros sistemas ou dados sensíveis;
e. **Realizar uma análise forense de cada incidente:** identificando as causas principais, os sistemas afetados e o impacto no ambiente de segurança da informação. A análise deve ser documentada e servir de base para ações corretivas;
f. **Adotar medidas corretivas eficazes:** para restaurar os sistemas afetados e eliminar as causas do incidente, além de implementar ações preventivas que evitem a recorrência de incidentes semelhantes;
g. **Ter um plano de comunicação interna e externa**: garantindo que todos os *stakeholders* relevantes sejam informados adequadamente sobre o incidente, respeitando os requisitos regulatórios, as obrigações legais e a proteção da reputação;
h. **Notificações ao regulador:** incidentes graves que possam afetar a operação, incluindo os que envolvem falhas críticas em sistemas ou dados sensíveis, devem ser imediatamente notificados ao Banco Central, conforme as exigências da Resolução nº 304, seguindo os protocolos de reporte estabelecidos;
i. **Manter registros detalhados de todos os incidentes de segurança:** incluindo a descrição do evento, as ações tomadas para a contenção e remediação, os impactos

identificados e quaisquer ações corretivas implementadas. Esses registros deverão ser mantidos por um período mínimo de 5 anos, ou conforme exigido pela legislação;

j. **Manutenção e melhoria constante:** realizar revisões pós-incidente buscando avaliar a eficácia das respostas, identificar as falhas ou melhorias necessárias nos processos e atualizar os planos de resposta a incidentes com base nas lições aprendidas;

k. **Registro, Resposta e Tratamento de Incidentes Envolvendo Terceiros:** assegura que todos os incidentes de segurança, incluindo aqueles envolvendo informações recebidas de empresas prestadoras de serviços, sejam registrados, analisados e controlados. As análises devem incluir a identificação da causa primaria, a avaliação detalhada do impacto nas operações da CRDC, nos dados dos clientes e na continuidade dos negócios e a implementação de controles para mitigar os efeitos imediatos e prevenir recorrências;

l. **Comunicação de incidentes de terceiros:** todos os incidentes relacionados a provedores e fornecedores devem ser comunicados à CRDC pelo canal oficial e tratados em conformidade com os SLAs estabelecidos nos contratos.

20. GESTÃO DE PROVEDORES CRÍTICOS DE SERVIÇOS

A CRDC estruturou um conjunto de norma e procedimentos específicos com o objetivo de garantir que os provedores de serviços essenciais para a operação da CRDC estejam em conformidade com a política de segurança da informação e normas vigentes. Especificando procedimentos e controles que garantam que sua atuação não comprometa a segurança dos dados, dos sistemas e operações da empresa.

Para a CRDC os Provedores Críticos de Serviços (PSC) são aqueles que fornecem serviços essenciais para o funcionamento da organização, e que, caso comprometidos, podem impactar significativamente a segurança, a operação ou a continuidade dos serviços prestados. Os PSC incluem, mas não se limitam a:

- Provedores de infraestrutura de TI (ex.: *cloud computing*, servidores, redes);
- Provedores de soluções de segurança cibernética (ex.: *firewall*, antivírus, sistemas de monitoramento);
- Provedores de processamento de pagamentos e sistemas de transações financeiras;

- Consultorias de TI ou empresas terceirizadas que prestam serviços de suporte e manutenção de sistemas críticos.

O processo de avaliação de risco será realizado periodicamente para identificar quais provedores são críticos para as operações da CRDC.

20.1 Diretrizes para a Gestão de Provedores Críticos de Serviço

O processo de gestão de provedores críticos de serviços deve atender as exigências regulatórias para Instituições Operadoras do Sistema do Mercado Financeiro (IOSMF), adotando as seguintes diretrizes:

a. **Contratos e Acordos de Nível de Serviço (SLAs):** devem incluir cláusulas específicas sobre segurança cibernética, detalhando as obrigações que o provedor deve seguir, como:
    i Proteção de dados confidenciais e sensíveis.
    ii Adoção de controles de segurança física e lógica.
    iii Notificação imediata à Instituição em caso de incidentes de segurança.
b. **Avaliação de riscos e auditorias regulares:** garantindo que os provedores críticos atendam aos padrões de segurança exigidos;
c. **Plano de Continuidade de Negócios e Recuperação de Desastres:** o provedor deve possuir um PCN que garanta a continuidade dos serviços essenciais, mesmo em caso de incidentes cibernéticos ou falhas operacionais. O plano deve estabelecer procedimentos de recuperação de desastres claros e compatíveis com as necessidades da CRDC;
d. **Monitoramento contínuo:** o provedor deve implementar o monitoramento contínuo de seus serviços, permitindo detectar e responder a incidentes de segurança de forma eficaz. A CRDC deve ter acesso ao relatório de monitoramento de segurança e, quando aplicável, realizar auditorias periódicas;
e. **Notificação de incidentes:** estabelecer canais e procedimentos de comunicação para que o PSC comunique imediatamente a CRDC sobre a ocorrência de incidentes de segurança da informação e cibernética;

f. **Notificações ao Banco Central do Brasil:** incidentes graves, que possam afetar a operação da CRDC, como vazamentos de dados sensíveis ou ataques cibernéticos de grande escala, o provedor deve cooperar com a Instituição na notificação ao Banco Central, conforme exigido pela Resolução nº 304;

g. **Treinamento e Conscientização:** os PSC devem realizar treinamentos regulares sobre cibersegurança, abordando temas como *phishing*, segurança de dados, proteção contra *malware*, e gestão de incidentes de segurança;

h. **Revisão e melhoria contínua:** após cada incidente de segurança ou auditoria, a CRDC deve realizar uma análise detalhada, avaliando a eficácia das medidas corretivas e aprimorar continuamente os procedimentos; e

i. **Reavaliar os riscos continuamente:** ajustando conforme as mudanças tecnológicas, a evolução das ameaças e as necessidades da organização.

21. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

Cientes da criticidade e relevância dos serviços prestados, a CRDC adota estratégias adequadas de Gestão de Continuidade de Negócios (GCN) garantindo, que mesmo diante de eventos inesperados ou desastres, a empresa possa manter suas operações essenciais e reduzir os impactos aos seus clientes e parceiros. Um Comitê de Crises foi instituído com o objetivo de aprovar as estratégias e ações em momentos de crise, garantindo as devidas orientações e direcionamentos dos demais colaboradores em situações que ameaçam ou impactam a continuidade dos negócios.

21.1 Diretrizes para a Gestões de Continuidade dos Negócios

A GCN é detalhada em um conjunto de normativos e procedimentos específicos baseados nos seguintes princípios

a. **Garantir que a Instituição seja capaz de manter suas operações críticas:** mesmo diante de situações adversas ou emergenciais, garantindo o mínimo impacto nas suas atividades e cumprindo as obrigações regulatórias;

b. **Criar e manter um Plano de Continuidade de Negócios**: que abranja todos os processos críticos, processamento de operações, comunicação com os clientes e com o Banco Central. O plano será revisto anualmente e testado regularmente;
c. **Realizar periodicamente a avaliação de impacto nos negócios (BIA)**: identificando as funções críticas, sistemas essenciais, riscos associados e o impacto potencial de sua interrupção;
d. **Estabelecer uma estrutura de governança para a continuidade de negócios:** responsável pela coordenação de ações, análise de riscos e garantia de que todos os colaboradores, fornecedores e parceiros estejam alinhados com os objetivos de continuidade;
e. **Adotar estratégias de recuperação de desastres:** incluindo *backups* regulares, planos de recuperação para sistemas e serviços críticos, locais alternativos de operação (sites de recuperação) para garantir que a operação seja retomada rapidamente após um incidente;
f. **Realizar testes anuais de continuidade de negócios:** simulando minimamente os cenários de falha tecnológica generalizada, ataques cibernéticos e desastre natural. Deve ser avaliada a eficácia do plano de recuperação e a prontidão das equipes envolvidas;
g. **Manter um plano de comunicação de crise:** que contemple a comunicação interna e externa, incluindo o Banco Central do Brasil. Em caso de um incidente, todas as partes interessadas devem ser informadas sobre o impacto e as ações corretivas em tempo hábil;
h. **Realizar avaliações de continuidade de negócios para os fornecedores e prestadores de serviços críticos:** assegurando que tenham seus próprios planos de continuidade e que possam retomar suas atividades rapidamente, caso um incidente afete a cadeia de fornecedores;
i. **Garantir que o Plano de Continuidade de Negócios esteja em conformidade com as regulamentações:** incluindo a Resolução nº 304, bem como com outras leis e normas aplicáveis relacionadas à proteção de dados e à segurança cibernética;

j. **Promover um processo de melhoria contínua:** atualizando periodicamente os planos e procedimentos com base nas lições aprendidas de testes, incidentes reais e mudanças no ambiente de negócios.

22. DISSEMINAÇÃO DA CULTURA DE SEGURANÇA DA INFORMAÇÃO

A CRDC, entendendo que uma cultura baseada em segurança da informação é fundamental para garantir a construção e manutenção de um ambiente seguro, promove a disseminação dos princípios e diretrizes de Segurança da Informação e Cibernética usando programas de conscientização e capacitação que fortalecem a cultura do pensamento e atuação segura.

Existe um comprometimento genuíno em educar e engajar a equipe em práticas de segurança, garantindo que a segurança da informação será incorporada como um valor compartilhado e essencial para o sucesso e a continuidade do negócio.

22.1 Diretrizes para a Disseminação da Cultura de Segurança da Informação

As diretrizes adotadas pela CRDC para divulgar a disseminação da cultura de Segurança da Informação são:

a. **Patrocínio da alta gestão:** demonstrando compromisso com a proteção dos dados e sistemas, e incentivando a adoção de práticas de segurança em todos os níveis organizacionais;
b. **Realizar treinamentos regulares de conscientização**: para todos os colaboradores, incluindo sessões de integração para novos colaboradores, e reciclagens periódicas para reforçar a importância das boas práticas de segurança;
c. **Promover a segurança da informação como uma responsabilidade compartilhada**: com todos os colaboradores, independentemente de sua área ou cargo, sendo responsáveis pela proteção das informações e pela adoção de práticas seguras em suas atividades diárias;
d. **Garantir que todas as políticas de segurança da informação sejam comunicadas:** de maneira clara a todos os colaboradores e com acesso fácil a essas políticas, assegurando que todos compreendam e sigam as normas estabelecidas;

e. **Realizar simulações de incidentes de segurança**: como ataques de *phishing*, engenharia social ou tentativas de fraude, treinando os colaboradores em como identificar e reagir rapidamente a essas ameaças;
f. **Criar canais seguros e confidenciais**: permitindo que os colaboradores possam relatar incidentes, falhas de segurança ou sugestões de melhorias;
g. **Implementar programas de reconhecimento:** incentivando o compromisso e ações exemplares em segurança da informação, seja em boas práticas, como a proteção de dados ou pela contribuição em iniciativas de melhoria do ambiente de segurança;
h. **Incorporar a segurança da informação a todos os processos de negócios da Instituição**: com a inclusão de critérios de segurança em todas as fases dos projetos e produtos, desde a concepção até a execução;
i. **A liderança deve adotar práticas exemplares em segurança da informação:** cumprindo e promovendo as políticas de segurança de forma consistente, influenciando positivamente os colaboradores a seguir as boas práticas e reforçando a importância da segurança como prioridade organizacional.

22.2 Informações aos Participantes

A CRDC compromete-se a fornecer informações claras, acessíveis e regulares aos seus participantes, incluindo colaboradores, fornecedores, parceiros de negócios e clientes, sobre as precauções necessárias na utilização de produtos e serviços oferecidos. Este compromisso inclui as seguintes iniciativas:

a. **Guia de uso Seguro:** disponibilização de um guia digital ou físico com instruções sobre o uso seguro de produtos e serviços, destacando práticas recomendadas e precauções;
b. **Treinamentos e conscientização:** realização de treinamentos regulares para clientes e participante;
c. **Comunicações proativas:** compartilhamento de informações sobre indicadores de comprometimento aos participantes por meio de canais oficiais;
d. **Canal de suporte e esclarecimento:** estabelecimento de um canal dedicado para dúvidas e orientações relacionadas à segurança no uso de produtos e serviços.

23. RESPONSABILIDADES

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

23.1 Diretoria e Gestores de equipe

Responsáveis por cumprir e fazer cumprir as determinações presentes nesta política, informando à área responsável pelo Sistema de Gestão de Segurança da Informação e Cibernética 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 Segurança da Informação e Cibernética;
b. fiscalizar regularmente o cumprimento desta política e demais normas nos locais de trabalho sob sua responsabilidade;
c. assinar o termo de compromisso da Política de Segurança da Informação e Cibernética;
d. participar, quando necessário, de investigações relacionadas a incidentes;
e. autorizar a liberação de acesso a informações sob sua responsabilidade, sempre observando a política;
f. revisar, sempre que solicitado, as liberações de acesso concedidas;
g. participar, junto à Diretoria responsável, da elaboração de matrizes de risco dos sistemas de informação sob sua gestão; e
h. atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política de Segurança da Informação e Cibernética, mediante a assinatura do Termo de Compromisso e Ciência e o Termo de Confidencialidade.

23.2 Gestão de Segurança da Informação e Cibernética

Responsável por estabelecer as políticas, padrões, procedimentos e controles, visando proteger as informações e garantir os princípios adotados pela CRDC. Deve ainda:

a. Entender, gerenciar, reportar e escalar os riscos de Segurança da Informação e Cibernética;

b. Atender aos processos de auditorias e controles internos relacionados à Segurança da Informação e Cibernética;
c. Realizar a gestão de riscos de Segurança da Informação e Cibernética em fornecedores, prestadores de serviços e parceiros de negócios;
d. Realizar a análise e detecção de vulnerabilidades nos ambientes da CRDC;
e. Garantir a execução de testes periódicos de vulnerabilidades;
f. Implementar e monitorar sistemas de detecção e prevenção de invasão;
g. Atuar em resposta aos incidentes de Segurança Cibernética;
h. Estabelecer, implementar, operar, monitorar e garantir a melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI);
i. Definir e formalizar os objetivos, controles e estratégia de governança da Segurança da Informação e Cibernética;
j. Estabelecer e disseminar, em conjunto com as demais equipes da Companhia, a cultura de Segurança da Informação e Cibernética;
k. Propor os investimentos necessários para a Segurança da Informação e Cibernética;
l. Apoiar os responsáveis pelos ativos na redução do risco de acesso indevido ou comprometimento das informações por pessoas não autorizadas;
m. Suportar o processo de revisão dos perfis de acesso, juntamente com os gestores dos sistemas;
n. Realizar auditorias internas, garantir que os controles de segurança atendam aos requisitos regulatórios e elaborar relatórios de conformidade quando necessário;
o. Identificar e avaliar os potenciais riscos de Segurança da Informação e Cibernética, bem como suas causas e consequências. Apoiar na definição e implantação de medidas corretivas para redução de seu nível de exposição.

23.3 Equipe de Segurança da Informação e Cibernética

A equipe de Segurança da Informação deve realizar uma gestão contínua dos riscos relacionados à segurança da informação, envolvendo a identificação, avaliação e mitigação de riscos cibernéticos e de segurança protegendo a organização de ameaças internas e externas, deve ainda:

a. Realizar revisões contínuas e ajustar as estratégias de segurança conforme necessário;
b. Monitorar ativamente a segurança dos dados e ativos da CRDC, utilizando ferramentas de detecção de intrusão e outros mecanismos de segurança;
c. Monitorar e garantir a conformidade da CRDC com as regulamentações aplicáveis;
d. Implementar e gerenciar controles adequados de gestão de acesso aos sistemas e dados da CRDC, garantindo que o princípio do menor privilégio seja seguido;
e. Implementar controles de segurança para proteger os dados sensíveis e pessoais da Instituição, incluindo criptografia de dados em repouso e em trânsito;
f. Garantir que a coleta, armazenamento e processamento de dados estejam em conformidade com a LGPD e com as políticas internas de privacidade;
g. Desenvolver e executar programas contínuos de conscientização e treinamento em segurança da informação focando em tópicos como *phishing*, senhas seguras, e comportamento seguro na utilização de tecnologias;
h. Auditar e monitorar os parceiros e fornecedores para garantir que eles cumpram as políticas de segurança da informação e cibernética da CRDC;
i. Gerenciar vulnerabilidades de segurança de forma contínua, realizando varreduras regulares para identificar falhas e garantir que os patches e atualizações de segurança sejam aplicados;
j. Realizar testes de penetração e auditorias regulares, avaliando a robustez das defesas cibernéticas;
k. Analisar e monitorar ameaças cibernéticas emergentes e técnicas de ataque sofisticadas, aplicando as defesas adequadas; e
l. Desenvolver e implementar um plano de resposta a incidentes, coordenando ações de mitigação, comunicação interna e externa e a documentação de todos os eventos de segurança.

23.4 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;

23.5 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 os acompanhamentos dos planos de ação ofertados pela área em decorrência dos eventuais apontamentos e recomendações.

23.6 Tecnologia da Informação

Atua em conjunto com a equipe de Segurança da Informação e Cibernética, sendo suas principais responsabilidades:

a. Não realizar mudanças de tecnologia, infraestrutura e sistemas sem o devido alinhamento com a equipe de Segurança da Informação e Cibernética;
b. Aplicar as práticas sugeridas pela equipe de Segurança da Informação e Cibernética nos padrões de desenvolvimento de sistemas e infraestruturas;
c. Garantir a disponibilidade do parque tecnológico, bem como a sua atualização com os padrões de segurança implementados, dentro dos prazos compatíveis com os níveis de riscos;
d. Comunicar imediatamente a equipe de Segurança da Informação e Cibernética sobre qualquer comportamento suspeito do parque tecnológico; e
e. Segregar níveis de acesso para cada grupo, sejam eles internos, terceiros prestadores de serviço ou parceiros, seguindo o princípio do menor privilégio para execução das atividades relacionadas ao contrato de prestação de serviço.

23.7 Produtos

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

a. Incluir os requisitos de Segurança da Informação e Cibernética na especificação dos sistemas;
b. Garantir que o processo de desenvolvimento é executado conforme as normas específicas aplicáveis;
c. Reportar novas vulnerabilidades a equipe de Segurança da Informação e Cibernética;
d. Garantir que os envolvidos na concepção do produto receberam o treinamento de Segurança da Informação e Cibernética;
e. Auditar periodicamente os prestadores de serviço envolvidos no desenvolvimento do produto;
f. Garantir o envolvimento da equipe de Segurança da Informação e
g. Cibernética nas definições do produto; e
h. Garantir a priorização das atividades de gestão de vulnerabilidades dos sistemas desenvolvidos pela CRDC atendendo o acordo de nível de serviço (SLA) de correção por nível de criticidade.

23.8 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 soluções sugeridas pela equipe de Segurança da Informação e Cibernética.

a. receber e aprovar o relatório anual das evoluções, incidentes e metas de Segurança da Informação e cibernética.
b. avaliará o tratamento adotado e as ações de melhoria proposta para os incidentes de Segurança da Informação e Cibernética;
c. alinhar as estratégias, as políticas, os processos, as decisões, os produtos e serviços da TI às necessidades do negócio;
d. estabelecer formatos organizacionais que direcionem o trabalho para a satisfação de demandas, gerando valor dentro de prazos e custos compatíveis;

e. estabelecer processos de gestão que apoiem a definição, a execução e o monitoramento da estratégia de Segurança da Informação e Cibernética; e
f. promover o engajamento dos dirigentes, gestores, usuários, técnicos e demais envolvidos na implementação e manutenção dos processos de Segurança da Informação e Cibernética.

23.9 COLABORADORES

A segurança da informação e cibernética é responsabilidade de todos os envolvidos nas atividades da CRDC. Todos precisam conhecer, incorporar e fazer cumprir os termos desta política e normas que a suportam, além de observar as seguintes responsabilidades:

a. compreender o papel da Segurança da Informação e Cibernética e seu impacto em suas atividades diárias;
b. notificar seu superior hierárquico, a área de Segurança da Informação e Cibernética, ou ainda a área de Compliance, caso perceba qualquer anormalidade em seu ambiente de trabalho;
c. assinar o termo de compromisso com a Política de Segurança da Informação e Cibernética;
d. manter a confidencialidade das senhas e credenciais de acesso e nunca as compartilhar. Utilizar autenticação multifatorial (MFA) sempre que disponível.
e. comunicar imediatamente qualquer incidente de segurança ao time de Segurança da Informação e cibernética;
f. garantir que informações sensíveis, como dados de clientes e dados financeiros, sejam armazenadas e transmitidas de maneira segura;
g. não usar ativos da organização para fins pessoais ou não autorizados e evitar a instalação de software não autorizado nos dispositivos corporativos;
h. contribuir e disseminar a cultura de proteção e segurança cibernética; e
i. participar e incentivar a participação de seus pares, nos treinamentos de Segurança da Informação e Cibernética.

23.10 FORNECEDORES, PRESTADORES DE SERVIÇOS E PARCEIROS DE NEGÓCIOS

Os fornecedores, prestadores de serviços e parceiros de negócio, caso obtenha acesso a qualquer informação ou ativo da CRDC, deve conhecer, cumprir, fazer cumprir e incorporar todos os termos desta política e normas que a suportam, deve ainda:

a. Proteger todos os dados fornecidos pela CRDC, especialmente dados sensíveis, conforme exigido pela legislação (como a LGPD) e pelas políticas;
b. implementar medidas de segurança adequadas para proteger os sistemas e serviços fornecidos, incluindo a aplicação de criptografia, monitoramento de redes e a realização de auditorias de segurança regulares;
c. informar à CRDC sobre qualquer vulnerabilidade ou incidente de segurança que possa afetar os serviços prestados ou os dados da organização;
d. permitir auditorias periódicas de segurança da informação, incluindo auditorias de sistemas e processos;
e. estabelecer um plano de resposta a incidentes, garantindo que os serviços possam ser restaurados rapidamente em caso de falhas de segurança e que os incidentes sejam comunicados à CRDC imediatamente;
f. estabelecer controles para prevenir, detectar e reportar atividades fraudulentas que possam comprometer os negócios ou a segurança da Instituição.

23.11 Provedores Críticos de Serviços

São considerados provedores críticos de serviços (PSC) aqueles que prestam serviços essenciais para a continuidade das operações básicas da CRDC, incluindo sistemas, infraestrutura, serviços em nuvem, segurança cibernética. Nesses casos a CRDC adota um tratamento mais rigoroso uma vez que o impacto de uma falha nesses serviços pode prejudicar a continuidade de seus negócios.

Os PSCs além de concordar e aceitar os termos impostos para fornecedores, prestadores de serviços e parceiros de negócios, devem ainda:

a. cumprir todas as regulamentações de segurança da informação, privacidade e proteção de dados, conforme as exigências da legislação brasileira, incluindo as normas aplicáveis do Banco Central do Brasil e a Lei Geral de Proteção de Dados (LGPD);

b. criar e manter um plano de resposta a incidentes que seja compatível com os procedimentos da CRDC, incluindo o gerenciamento de falhas de segurança, ataques cibernéticos ou vazamentos de dados;
c. adotar e manter controles de segurança adequados, como criptografia de dados, autenticação multifatorial e monitoramento de ativos, para proteger informações sensíveis e garantir a integridade dos sistemas que interagem com a CRDC;
d. realizar avaliações periódicas de riscos de segurança cibernética, identificar vulnerabilidades e tomar ações corretivas para mitigar os riscos;
e. disponibilizar relatórios periódicos que demonstrem a conformidade com os controles de segurança cibernética estabelecidos, incluindo auditorias internas, exames de segurança e resultados de testes de penetração;
f. implementar planos de continuidade de negócios (PCN) e recuperação de desastres (DR) para garantir a continuidade dos serviços essenciais. Testes regulares devem ser realizados para validar a eficácia dos planos, a CRDC pode solicitar relatórios para análise e acompanhamento;
g. garantir que qualquer dado sensível ou confidencial da CRDC seja compartilhado e processado de forma segura, utilizando criptografia e outras práticas de segurança;
h. notificar imediatamente a CRDC, usando os canais previstos em contrato, sobre quaisquer incidentes de segurança cibernética que afetem os serviços prestados ou os dados;
i. permitir auditorias de segurança periódicas pela CRDC ou por auditores independentes, garantindo a conformidade com as políticas de segurança da informação e cibernética, com as leis e normas vigentes e cooperando na correção de quaisquer falhas ou vulnerabilidades identificadas;
j. assinar contratos formais com a CRDC, incluindo acordos de nível de serviço (SLAs) que estabeleçam os requisitos de segurança, desempenho e tempos de resposta a incidentes, e garantir que esses compromissos sejam cumpridos;
k. fornecer treinamentos regulares de segurança da informação aos seus funcionários, garantindo que todos compreendam a importância da proteção de dados;

24. VIOLAÇÕES E SANÇÕES

Os princípios de Segurança da Informação e Cibernética estabelecidos nesta política refletem os interesses e a aderência da alta administração da CRDC e, devem ser observados por todos os colaboradores, fornecedores, prestadores de serviços, parceiros de negócios e clientes na execução de suas funções e consumo dos serviços contratados.

Os colaboradores devem cumprir as disposições expressas nesta política, independentemente de seu cargo, função, área de atuação ou localidade. Aqueles que descumprirem quaisquer dispositivos estabelecidos nesta política ou em seu conjunto de normativos, estará sujeito a imposição de sanções, a serem definidas pelo Comitê de Ética e Conduta, e penalidades descritas nas legislações vigentes.

Aos fornecedores, prestadores de serviço e parceiros de negócios, inclui-se também a rescisão de contratos e penas de responsabilidade civil e criminal na máxima extensão que a lei permitir.

Periodicamente, são realizadas campanhas de conscientização ou treinamentos, presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação.

Todos os colaboradores, fornecedores, prestadores de serviços e parceiros de negócios, no ato de sua contratação, recebem uma cópia desta Política, bem como eventual documentação de suporte aplicável, que estabelece, além dos procedimentos de segurança a serem seguidos, as regras sobre o correto uso dos sistemas e dispositivos disponibilizados.

Para formalizar a ciência e a concordância com os termos da política e demais normas aplicáveis, todos os colaboradores assinam um termo de responsabilidade se comprometendo com as disposições vigentes e suplementares.

25. CONTROLE DE VERSIONAMENTO

Versão	Data	Área responsável	Descrição
1.0	06/2021	Segurança da Informação	Emissão da Política de Segurança Cibernética.

2.0	08/2023	Segurança da Informação	Mudança do modelo de documento, e agrupamento dos normativos internos: PL-TI-SE-0001 - Política de Segurança Cibernética CRDC_v1.0 e PL-TI-SE-0002 - Política de Segurança da Informação CRDC - Conscientização de Usuários_v3.0.
3.0	11/2023	Segurança da Informação	Revisão para fins de aprovação pelo Conselho de Administração da CRDC.
4.0	01/2025	Segurança da Informação	Revisão periódica, definição de diretrizes e revisão de responsabilidades

26. APROVAÇÃO

Declaramos que a presente versão é cópia fiel da Política de Tecnologia da Informação e Cibernética aprovada na Reunião Ordinária do Conselho de Administração de 03/01/2025.