PL-SI-0001 - Política de Segurança da Informação e Cibernética

Versão 3.0 | 11.2023

Classficação: 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

Esta Política se aplica a todos os envolvidos diretamente e indiretamente nos processos e negócios da CRDC, incluindo, mas não se limitando aos colaboradores, alta administração, 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. Todos os ativos são classificados, inventariados e mantidos atualizados, de acordo com a sua criticidade.

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 referencias 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: é a possibilidade de ocorrência de um evento que afete adversamente o atendimento dos objetivos da companhia.

Segurança da Informação e 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 constitua 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; e
- ISO/IEC 27.002 – Código de prática para a gestão da segurança da informação

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:

- Confidencialidade: priorizar as ações que visam garantir que apenas as pessoas autenticadas e autorizadas tomem conhecimento das informações recebidas, manipuladas e enviadas pela CRDC;
- 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
- 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.

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:

(i) Pública: seu acesso não é controlado ou registrado, não exige implementação de mecanismos de Segurança da Informação avançados;

(ii) Interna: informações relacionadas a assuntos internos da CRDC, sendo que seu acesso deve ser realizado exclusivamente por pessoas internas e autorizadas para tal. Embora a CRDC opte por não divulgar as informações classificadas como interna, seu acesso não causa danos sérios a empresa;

(iii) Confidencial: tem caráter sigiloso e não deve ser divulgada. Seu uso é restrito a um determinado número de pessoas, com autorização e para desempenharem as suas atividades diárias. A divulgação não autorizada destas informações pode causar danos diretos ou indiretos a CRDC; e

(iv) Restrita: informação com o mais alto nível de sigilo, tem seu acesso controlado e liberado apenas a um grupo restrito de pessoas previamente designadas. Todos os procedimentos e ferramentas de segurança necessários são adotadas para proteger as informações restritas. Nesta categoria também estão as informações de clientes, principalmente os dados pessoais e sensíveis.

Todo colaborador responsável por gerar ou manipular informações deve classificá-la antes de realizar, ou permitir que realizem, a sua divulgação. Ainda, caso tome conhecimento de que alguma informação recebe tratamento inadequado, deve comunicar imediatamente a área responsável por tal informação e a equipe de

Segurança da Informação e Cibernética. Os detalhes da metodologia e regras adotadas para a classificação das informações estão disponíveis em normativo específico.

7. Manuseio da Informação

A CRDC adota soluções tecnológicas para garantir que os acessos as informações são pessoais e intransferíveis, 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.

a) Impressoras e Copiadoras

A CRDC controla os documentos enviados aos sistemas de impressão, podendo, se necessário, realizar auditorias nos documentos e em seus demandantes. 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) Manipulação de Informações Não Públicas

A CRDC armazena *logs* de auditoria das informações acessadas. A manipulação de informações não publicas deve levar em consideração todos os riscos presentes que possibilitariam seu vazamento, atentando 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 físico: 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 destruídos antes de descartados. Já as mídias rígidas, tais como disco rígido (HD), unidades sólidas (SSD) e pen drive, devem ser apagados pela equipe de Segurança da Informação e Segurança Cibernética, utilizando ferramentas especificas.

8. Diretrizes de segurança da informação e segurança cibernética

A política e todos os demais documentos relacionados estão disponíveis em local acessível a todos os colaboradores, fornecedores, prestadores de serviços, parceiros de negócio e clientes. 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.

a) 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.

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

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. Periodicamente e por amostragem, a equipe de Segurança da Informação e Segurança Cibernética pode realizar auditoria nos usuários disponibilizados.

c) 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.

d) Utilização de Software

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.

e) 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. Detalhes sobre as exceções e o processo de controle estão disponíveis em normativo específico.

f) 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.

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. É proibido o uso de ferramentas não homologadas para a troca de informações não públicas entre colaboradores ou clientes, cabendo as punições previstas no Código de Ética e Conduta CRDC

g) Prevenção Contra Vírus e Softwares Maliciosos

A CRDC possui controles para prevenir que vírus e outros tipos de software maliciosos contaminem e espalhem-se nos sistemas e estações de trabalho de sua rede. Todos os computadores possuem antivírus instalados e monitorados por um sistema de gerenciamento centralizado, garantindo a aplicação de atualizações a todos os equipamentos em período compatível com as boas práticas.

h) 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.

É 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.

i) 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.

j) 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.

k) Monitoramento e Auditoria de 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.

9. Registro, Resposta e Tratamento a Incidentes de Segurança Cibernética

a) Classificação de incidentes de Segurança da Informação e Cibernética

O modelo de classificação de incidentes de Segurança da Informação e Cibernética na CRDC é dividido dois níveis: no primeiro nível é definido se o incidente é crítico ou não crítico, já no segundo nível o incidente é classificado conforme a relevância dos ativos afetados.

Incidentes de nível crítico demandam ações imediatas para o restabelecimento dos serviços e proteção do ambiente, sendo necessário, na maioria dos casos, o acionamento dos recursos de contingência. Os problemas não críticos geralmente afetam recursos específicos e não geram danos maiores os serviços prestados, porém o tratamento imediato é importante para evitar a escalada do nível de risco.

A decisão sobre a ação a ser adotada para contornar o risco cabe ao responsável pela Segurança da Informação e Cibernética, alinhado com o Comitê de Crises.

Os detalhes sobre o modelo de classificação dos incidentes, bem como os processos de detecção e tratamento dos eventos são detalhados em normativo específico.

b) Gestão de vulnerabilidades

Com o objetivo de eliminar ou diminuir as vulnerabilidades a CRDC adota soluções de *hardware* e *software* para a proteção de suas informações, e ainda realiza auditorias periódicas em seus processos. A equipe de Segurança da Informação e Cibernética é responsável por identificar, reportar, monitorar e auditar a solução aplicada para o tratamento das vulnerabilidades.

A CRDC, em sua norma especifica para o desenvolvimento de sistemas, define os cuidados e ações esperadas para garantir a entrega de sistemas eficientes e seguros. Em produção o monitoramento é constante e periodicamente são realizados testes de intrusão, cujo resultado será comparado com testes anteriores para medir a efetividade dos planos de ação adotados.

Com periodicidade bimestral ou sempre que necessário, a equipe de segurança apresenta ao Comitê de Segurança da Informação e Cibernética um relatório de classificação de vulnerabilidades e ações de contorno e mitigação.

Com periodicidade anual será apresentado ao Conselho de administração Relatório anual de incidentes, demonstrando:

- a efetividade dos planos de ação adotados;
- os incidentes relevantes;
- o resultado dos testes de invasão; e
- o resumo dos resultados obtidos na implementação das rotinas e procedimentos adotados e as tecnologias a serem implementadas na prevenção e tratamento dos incidentes de segurança da informação e cibernética.

c) Registro dos incidentes de Segurança da Informação e Segurança Cibernética

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.

d) Gestão de continuidade de negócios

A CRDC adota estratégias de Gestão de Continuidade de Negócios (GCN) adequadas a criticidade e relevância dos serviços prestados. Para definir as estratégias e garantir sua execução em situações de crise, foi instituído pela Diretoria, o Comitê de Crises. Este grupo é responsável por definir as ações e orientar a atuação dos demais colaboradores em situações que ameaçam ou impactam a continuidade dos negócios. A GCN é detalhada em um conjunto de normativos específicos.

10. Disseminação da Cultura de Segurança da Informação

A CRDC 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. 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.

11. 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.

12. Responsabilidades

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

a) 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:

- Entender, gerenciar, reportar e escalar os riscos de Segurança da Informação e Cibernética;
- Atender aos processos de auditorias e controles internos relacionados à Segurança da Informação e Cibernética;
- Realizar a gestão de riscos de Segurança da Informação e Cibernética em fornecedores, prestadores de serviços e parceiros de negócios;
- Realizar a análise e detecção de vulnerabilidades nos ambientes da CRDC;
- Garantir a execução de testes periódicos de vulnerabilidades;
- Implementar e monitorar sistemas de detecção e prevenção de invasão;
- Atuar em resposta aos incidentes de Segurança Cibernética;
- Estabelecer, implementar, operar, monitorar e garantir a melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI);
- Definir e formalizar os objetivos, controles e estratégia de governança da Segurança da Informação e Cibernética;
- Estabelecer e disseminar, em conjunto com as demais equipes da Companhia, a cultura de Segurança da Informação e Cibernética;
- Propor os investimentos necessários para a Segurança da Informação e Cibernética;
- Apoiar os responsáveis pelos ativos na redução do risco de acesso indevido ou comprometimento das informações por pessoas não autorizadas;
- Suportar o processo de revisão dos perfis de acesso, juntamente com os gestores dos sistemas; e
- 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.

b) 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:

- Viabilizar treinamentos à sua equipe, assim como o acesso a todos os materiais fornecidos pela área de Segurança da Informação e Cibernética;
- Fiscalizar regularmente o cumprimento desta política e demais normas nos locais de trabalho sob sua responsabilidade;
- Assinar o termo de compromisso da Política de Segurança da Informação e Cibernética;
- Participar, quando necessário, de investigações relacionadas a incidentes;
- Autorizar a liberação de acesso a informações sob sua responsabilidade, sempre observando a política;
- Revisar, sempre que solicitado, as liberações de acesso concedidas;
- Participar, junto à Diretoria responsável, da elaboração de matrizes de risco dos sistemas de informação sob sua gestão; e
- 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.

c) Riscos e *Compliance*

Responsável por suportar às áreas da CRDC para manter uma efetiva estrutura de gestão de riscos, controles internos e *Compliance*.

d) Tecnologia da Informação

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

- Não realizar mudanças de tecnologia, infraestrutura e sistemas sem o devido alinhamento com a equipe de Segurança da Informação e Cibernética;
- Aplicar as práticas sugeridas pela equipe de Segurança da Informação e Cibernética nos padrões de desenvolvimento de sistemas e infraestruturas;
- 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;
- Comunicar imediatamente a equipe de Segurança da Informação e Cibernética sobre qualquer comportamento suspeito do parque tecnológico; 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.

e) 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:

- Incluir os requisitos de Segurança da Informação e Cibernética na especificação dos sistemas;
- Garantir que o processo de desenvolvimento é executado conforme as normas específicas aplicáveis;
- Reportar novas vulnerabilidades a equipe de Segurança da Informação e Cibernética;
- Garantir que os envolvidos na concepção do produto receberam o treinamento de Segurança da Informação e Cibernética;
- Auditar periodicamente os prestadores de serviço envolvidos no desenvolvimento do produto;

- Garantir o envolvimento da equipe de Segurança da Informação e Cibernética nas definições do produto; e
- 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.

f) Comitê de Tecnologia e Segurança da Informação

Responsável por aprovar as estratégias, os objetivos e ações propostas para mitigar os riscos envolvidos na segurança da informação e cibernética. Anualmente receberá o relatório de incidentes de segurança da informação e cibernética e avaliará o tratamento adotado e as ações de melhoria propostas.

g) Colaboradores, Fornecedores, Prestadores de Serviços e Parceiros de negócios

A segurança da informação e cibernética é responsabilidade de todos os funcionários, fornecedores, prestadores de serviços e parceiros de negócios. Todos precisam conhecer, incorporar e fazer cumprir os termos desta política e normas que a suportam, além de observar as seguintes responsabilidades:

- Compreender o papel da Segurança da Informação e Cibernética e seu impacto em suas atividades diárias;
- 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;
- Assinar o termo de compromisso com a Política de Segurança da Informação e Cibernética;
- Contribuir e disseminar a cultura de proteção e segurança cibernética; e
- Participar e incentivar a participação de seus pares, nos treinamentos de Segurança da Informação e Cibernética.

h) Clientes e Usuários das Soluções CRDC

As informações estão disponíveis aos clientes da CRDC apenas mediante um processo de autenticação, seja por usuário e senha ou pelo uso de certificados digitais.

Os usuários de acesso ao sistema são pessoais e intransferíveis, sendo que seu uso é de responsabilidade do proprietário. As integrações via API são autenticadas por usuários exclusivos, disponibilizados aos clientes no momento da implantação, havendo ainda a necessidade da importação do *Token* de autenticação da API. São responsabilidades dos usuários ainda:

- A proteção das informações disponibilizadas por seu acesso. Garantindo que suas permissões não serão utilizadas para acessar, modificar, destruir ou divulgar indevidamente informações sigilosas;
- Que seu usuário é impessoal e intransferível, nunca fornecer sua senha a terceiros, mesmo aos colaborados da CRDC;
- Que os recursos tecnológicos disponíveis sejam utilizados, apenas para os fins claramente designados no processo de contratação dos serviços; e
- Notificar imediatamente a CRDC caso identifique qualquer anomalia, descumprimento ou violação de seu ambiente de trabalho.

13. Controle de Versionamento

Versão	Data	Área responsável	Descrição
1.0	28.06.21	Desenvolvimento	Emissão da Política de Segurança Cibernética.
2.0	17.08.2023	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	28.11.2023	Segurança da Informação	Revisão para fins de aprovação pelo Conselho de Administração da CRDC.

14. Aprovação

Declaramos que a presente é cópia fiel da Política de Segurança da Informação e Cibernética aprovada na Reunião Ordinária do Conselho de Administração de 28.11.2023.