# Política de Segurança Cibernética

## Sumário

## 1. OBJETIVO

Esta Política de Segurança Cibernética ("Política") tem como objetivo definir diretrizes, princípios e regras relacionadas à Segurança da Informação na Cora Sociedade de Crédito, Financiamento e Investimento S.A. ("**Cora SCFI**"), Cora Tecnologia Ltda. ("**Cora Tecnologia**") e na Cora Holding Ltda. ("**Cora Holding**"), em conjunto, o "**Grupo Cora**" ou, simplesmente "**Cora**", visando proteger os dados e informações corporativas quanto aos aspectos de confidencialidade, integridade e disponibilidade. Para isso, o **"Grupo Cora"** emprega tecnologias de proteção de dados disponíveis no mercado e realiza uma seleção rigorosa de Pessoas Colaboradoras e Prestadores de Serviço especializados em processamento, armazenamento de dados e computação em nuvem.

## 2. ABRANGÊNCIA

Esta Política deve ser observada por todas as Pessoas Colaboradoras, bem como fornecedores, prestadores de serviço e parceiros, na condução da implementação das medidas previstas.

## 3. DEFINIÇÕES

**Ativos Empresariais:** Recursos e ativos de propriedade da Cora, incluindo, mas não se limitando a e-mail, mensagens instantâneas, internet, ferramentas Web e SaaS, acesso a rede interna, equipamentos, computadores, notebooks, celulares, aplicações, sistemas, bancos de dados, arquivos armazenados em mídias digitais, documentos impressos, ou qualquer outro ativo ou recurso disponibilizado pela Cora.

**Comitê de Riscos:** Grupo de pessoas responsável por analisar os possíveis cenários de incidentes, definir as estratégias de ações e metas a serem adotadas para manter a normalidade das operações, definir os posicionamentos e respostas da organização junto a todos os públicos envolvidos, assegurar a veracidade dos fatos e divulgar as ocorrências com precisão e definir se uma situação consiste ou não em uma crise e, consequentemente, deliberando acerca da sua comunicação aos Órgãos Reguladores.

**Confidencialidade:** Visa garantir que as informações são disponibilizadas ou divulgadas apenas a indivíduos, entidades ou processos autorizados.

**Crise:** Situação que interfere na imagem e reputação da empresa, consistindo em um fato extremo que extrapola o ambiente organizacional e atinge diversos públicos, inclusive grupos que talvez nunca tiveram ligação com a marca, que não são clientes ou consumidores diretos, mas que ainda assim contribuem para a boa recepção da empresa.

**Dados pessoais:** Toda informação ligada a uma pessoa natural que a identifique ou que, em conjunto com outras informações, permita a sua identificação (Ex. nome, CPF, documento de identidade, endereço, dados bancários, data de nascimento, telefone, e-mail, WhatsApp, cargo, função, salário etc.).

**Dados sensíveis:** Conforme definido pelo artigo 5º, inciso II da Lei Geral de Proteção de Dados, configura-se como dado sensível dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

**Diretoria:** Diretoria reunida da Cora, composta pela totalidade de seus Diretores estatutários e/ou administradores, podendo, contudo, em caso de ausência de qualquer dos membros, deliberar validamente com a presença de maioria simples dos presentes.

**Diretoria de Tecnologia:** Responsável perante o Banco Central do Brasil por coordenar a comunicação tempestiva de uma situação de crise, bem como das providências para a resolução desta e o reinício das atividades impactadas. Além disso, é responsável por garantir a efetividade desta Política, incluindo a implementação do plano de ação e resposta a incidentes.

**Disponibilidade:** Visa garantir que as informações são acessíveis e utilizáveis sob demanda por indivíduos, entidades ou processos autorizados.

**DLP:** Sigla em inglês para *Data Loss Prevention*, é o conjunto de ferramentas e processos utilizados para detectar, monitorar e impedir o vazamento, perda ou

uso não autorizado de dados sensíveis, garantindo a proteção das informações da organização contra ameaças internas e externas.

**Incidente:** Qualquer destruição, perda, modificação, divulgação não autorizada ou acesso, de forma acidental ou ilegal, que envolva informações ou ativos empresariais. São exemplos: A perda de dados ou hardware; o roubo de dados ou hardware; acesso não autorizado a dados pessoais; divulgação não autorizada, tentativa fraudulenta de obtenção de informações confidenciais (phishing); etc.

**Informação:** Conjunto de dados, imagens, textos e quaisquer outras formas de representação dotadas de significado dentro de um contexto. Em síntese, é todo conteúdo que possua valor para a companhia, independentemente da forma de armazenamento e do caráter daquele valor, podendo ser financeiro, tecnológico, arquivístico, reputacional, dentre outros.

**Informações sensíveis:** todas as informações e dados de natureza técnica, operacional ou econômica, bem como quaisquer outros dados materiais, pormenores, documentos, desenhos, fotografias, especificações técnicas, recebidas pelas partes ou de terceiros, verbalmente, por escrito, eletronicamente, por meio magnético ou qualquer outro meio.

**Integridade:** visa garantir que as informações são precisas, completas e protegidas de alterações indevidas, sejam elas intencionais ou acidentais.

**Parceiros e Prestadores de Serviço:** pessoa física ou jurídica com a qual a Instituição mantém um relacionamento comercial, no interesse mútuo do desenvolvimento de um produto ou serviço a ser ofertado para seus clientes ou que presta serviço ou fornece bens à Instituição.

**Pessoas Colaboradoras:** todas as pessoas físicas que possuem relação empregatícia com a Cora, prestando serviços de forma não eventual, e que recebem um salário por isso. Para fins desta Política, também serão consideradas Pessoas Colaboradoras aquelas que possuem vínculo societário com a Cora.

**Proprietário da Informação:** pessoa responsável perante a Cora, por um ativo empresarial de informação, devendo protegê-lo quanto aos aspectos de confidencialidade, integridade e disponibilidade.

**Serviços Relevantes:** serviços de processamento, armazenamento de dados e computação em nuvem que, em conformidade com as diretrizes estabelecidas neste documento, (a) tenham por escopo o tratamento de dados e informações (i) de clientes da Cora SCFI e/ou (ii) que possuam relação com a condução das atividades fim da Cora SCFI e (b) representem um nível de criticidade significativo para a Cora SCFI e seus clientes, dada a importância técnica e regulatória da temática, bem como dos controles relacionados.

## 4. DIRETRIZES

Para fins desta Política ficam estabelecidas as seguintes diretrizes gerais:

### 4.1. Gestão de Riscos Cibernéticos

A gestão de riscos cibernéticos é um processo contínuo na Cora. O Time de Cybersecurity é responsável por identificar, analisar, avaliar e tratar ameaças e vulnerabilidades que possam impactar os ativos de informação.

### 4.2. Métricas e Indicadores

A Cora implementa um processo contínuo de acompanhamento e auditoria para controlar e melhorar sua maturidade e conformidade em segurança da informação. A empresa utiliza processos definidos para auditorias internas e externas, além de testes regulares (como testes de penetração e análises de vulnerabilidade) para validar a eficácia dos controles, mantendo trilhas de auditoria (logs) detalhadas.

Para medir o desempenho, a Cora define e monitora Indicadores-Chave de Desempenho (KPIs), tais como o tempo de detecção e resposta a incidentes (MTTD/MTTR), o tempo de correção de vulnerabilidades, a conclusão de treinamentos e os resultados de auditorias de conformidade (ex: ISO 27001). Esses indicadores são revisados periodicamente pela

gestão para ajustar estratégias e direcionar investimentos em segurança cibernética.

### 4.3. Mesa e Tela Limpa

A Cora exige que todos os colaboradores protejam as informações da empresa, sejam elas digitais ou físicas. Isso envolve duas práticas principais:

Tela Limpa: Obriga o bloqueio da estação de trabalho sempre que o colaborador se ausentar, mesmo que por pouco tempo, para evitar acessos não autorizados.

Mesa Limpa: Determina que documentos físicos confidenciais ou internos (impressos, mídias, anotações) devem ser guardados em locais seguros e trancados (como gavetas) quando não estiverem em uso, especialmente ao final do dia.

### 4.4. Uso Aceitável de Ativos Empresariais

A Cora fornece equipamentos para seus colaboradores usarem exclusivamente no trabalho, garantindo a melhor estrutura para suas atividades. O uso pessoal desses equipamentos é permitido, mas deve seguir os limites estabelecidos na Política de Uso de Equipamentos e Recursos Corporativos.

### 4.5. Classificação e Tratamento da Informação

Todas as informações e os respectivos recursos tecnológicos que as suportam devem ser classificados em um dos quatro níveis de sigilo (Restrito, Confidencial, Interno ou Público). Isso serve para garantir a proteção correta de cada dado, e todos os colaboradores devem ser responsáveis por aplicar essa classificação de riscos, buscando identificar ameaças e impactos sobre os ativos empresariais.

### 4.6. Criptografia de Dados e Ativos

A Cora exige que todos os dados classificados como Restritos ou Confidenciais sejam protegidos com criptografia forte quando armazenados (dados em repouso). Isso inclui a aplicação obrigatória de criptografia em servidores, endpoints, dispositivos móveis e backups.

Por fim, a Cora mantém um processo formal e restrito para o gerenciamento do ciclo de vida das chaves criptográficas.

## 4.7. Gestão de Identidades e Acessos

A Cora baseia-se nos princípios do Menor Privilégio e da Necessidade de Saber, garantindo que Pessoas Colaboradoras e Prestadores de Serviços tenham acesso somente às informações e sistemas essenciais para suas funções. Cada usuário possui uma identificação única, tornando o acesso pessoal e intransferível, e não é permitido compartilhar senhas ou utilizar contas genéricas e, para aumentar a segurança, deve-se exigir senhas complexas e o múltiplo fator de autenticação (MFA).

A proteção das credenciais e a responsabilidade por todas as ações nas contas são de inteira responsabilidade da Pessoa Colaboradora titular do acesso.

### 4.7.1. Gestão do Ciclo de Vida de Acessos:

Todo o ciclo de concessão, alteração e revogação de acessos é gerenciado por um processo formal e auditável, que permite ao time de Cybersecurity a revisão e ajuste do nível de informação conferida de acordo com a função desempenhada e tenham o acesso revogado imediatamente em caso de desligamento.

### 4.7.2. Revisão Periódica de Acessos:

Para remover acessos desnecessários, devem ser feitas revisões no mínimo semestralmente, sendo a responsabilidade compartilhada: os gestores validam a necessidade dos acessos de suas equipes e Cybersecurity coordena e executa os ajustes.

## 4.8. Ciclo de Vida de Desenvolvimento Seguro (SDLC)

O Ciclo de Vida de Desenvolvimento Seguro (SDLC) da Cora é um processo que integra a segurança em todas as etapas do desenvolvimento de produtos e tecnologias. Esse ciclo é composto por quatro fases principais: (i) Definição de requisitos; (ii) Desenvolvimento e codificação segura; (iii) Análise e testes de segurança e (iv) Adoção de novas tecnologias.

## 4.9. Gestão de Vulnerabilidades

A Cora adota uma postura proativa e metódica para gerenciar eventuais falhas de segurança, combinando monitoramento constante com testes de invasão (pentests) periódicos e um processo formal para corrigir as brechas descobertas, que devem ser classificadas de acordo com o nível de criticidade dentro de prazos predefinidos.

## 4.10. Segurança de Redes e Ambiente

A Cora implementa uma estratégia de defesa em múltiplas camadas para proteger suas redes. Isso envolve o isolamento de sistemas críticos por segmentação, utilizar proteções robustas contra malware como antivírus e filtros e monitorar ativamente o tráfego com logs e sistemas de detecção de intrusão para identificar e bloquear ameaças.

## 4.11. Continuidade de Negócios e Backups

A Cora assegura a recuperação dos seus dados críticos através de backups automáticos, que devem ser armazenados de forma segura, com criptografia e cópias externas ou imutáveis e validados regularmente por testes.

## 4.12. Prevenção de Vazamento de Informações

Para prevenir o vazamento de informações restritas ou confidenciais, a Cora utiliza mecanismos tecnológicos e processuais, como soluções de Prevenção contra Perda de Dados (DLP). Essas ferramentas devem ser usadas para monitorar, detectar e bloquear a extração não autorizada de

dados por meio do fluxo de entrada e saída de dados da rede corporativa, garantindo que as regras aplicadas estejam alinhadas à Política de Classificação e Tratamento das Informações da Cora.

## 5. CONTRATAÇÃO DE SERVIÇOS RELEVANTES

Deve-se assegurar que a parte contratada e eventuais subcontratadas e/ou subordinadas cumpram os requisitos mínimos de governança cibernética no âmbito do gerenciamento de risco operacional por meio de avaliação realizada pela Time de Cybersecurity.

## 6. GESTÃO E RESPOSTA A INCIDENTES DE SEGURANÇA CIBERNÉTICA

A Cora adota um Plano de Ação e Resposta a Incidentes estruturado para lidar com ameaças à segurança. O processo começa com a identificação e relato de incidentes potenciais, que devem ser objeto de comunicação imediata ao time de Cybersecurity. Em seguida, é realizada a triagem e classificação para validar a ocorrência e definir sua gravidade.

Ações de contenção devem ser imediatamente aplicadas para isolar os sistemas e evitar a propagação do dano. Após a contenção, uma investigação detalhada busca a causa raiz, os vetores de ataque e a exposição dos dados, o que fundamenta a aplicação de ações corretivas para resolução do problema e preventivas para evitar recorrências.

O processo segue para a restauração dos serviços afetados. Após a resolução, é gerado um relatório pós-mortem detalhando o ocorrido e as lições aprendidas, e esses registros devem ser mantidos para retenção por no mínimo 5 (cinco) anos. Por fim, uma análise crítica periódica desses incidentes é usada para a melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI).

## 7. CULTURA DE SEGURANÇA E CONSCIENTIZAÇÃO

Com o intuito de permitir que as diretrizes contidas nesta Política e os procedimentos dela derivados tenham efetividade, bem como disseminar a cultura de segurança da informação e avaliar o nível de maturidade e conhecimento das

Pessoas Colaboradoras, a Cora possui e disponibiliza um programa de conscientização, treinamento e avaliação em Segurança Cibernética.

Além disso, a Cora se compromete a divulgar materiais para os clientes, prestadores de serviços e parceiros, com o intuito de disseminar a cultura de segurança cibernética e fornecer orientações sobre a utilização segura de produtos e serviços financeiros.

## 8. COMUNICAÇÃO DE EVENTOS E CANAIS DE COMUNICAÇÃO

As questões relacionadas a esta Política, ou aos eventuais procedimentos dela derivados deverão ser enviadas ao Time de Cybersecurity, por meio dos canais adequados.

Toda Pessoa Colaboradora e Prestadores de Serviços tem a obrigação de informar o Time de Cybersecurity sobre qualquer evento, potencial ou efetivo, do qual tenha conhecimento, a fim de que as medidas mitigadoras possam ser adotadas tempestivamente pela Cora.

## 9. VIGÊNCIA E REVISÃO

Esta Política entrará em vigor na data de sua aprovação pela Diretoria da Cora, e será revisada, no mínimo, anualmente ou em prazo menor, que poderá ocorrer:

a. em função de modificação nas normas legais e regulamentares aplicáveis, de forma a implementar as adaptações que forem necessárias; ou

b. quando, no processo de avaliação da estrutura adotada, for constatada a necessidade de alterações.

Cabe à Diretoria a aprovação de qualquer modificação ou revisão desta Política.

## 10. REGULAMENTAÇÃO APLICÁVEL

- Resolução CMN nº 4.893, de 26 de fevereiro de 2021;
- Resolução CMN nº 4.557, de 23 de fevereiro de 2017;

- Norma ABNT NBR ISO 22301 – Sistema de Gestão de Continuidade de Negócios;
- Norma ABNT NBR ISO 31000 – Gestão de Riscos; e
- Lei nº 13.709, de 14 de agosto de 2018;

## 11. DOCUMENTOS RELACIONADOS

- Política de Gerenciamento Contínuo e Integrado de Riscos;
- Política de Uso de Equipamentos e Recursos Corporativos;
- Política de Classificação e Tratamento das Informações;
- Política de Gestão de Acessos;
- Política de Gestão e Resposta a Incidentes de Segurança Cibernética;
- Política de Privacidade de Dados; e
- Manual de Procedimento de Resposta a Incidentes Cibernéticos e Incidentes envolvendo Dados Pessoais.

## 12. HISTÓRICO DE ALTERAÇÕES

| Versão | Data | Alterações |
|---|---|---|
| Versão 1 | 31/08/2021 | Versão inicial |
| Versão 2 | 30/03/2022 | Revisão |
| Versão 3 | 15/12/2023 | Atualização |
| Versão 4 | 28/03/2024 | Atualização do item 3. |

| | | |
|---|---|---|
| Versão 5 | 28/03/2025 | Atualização no item 4.2, 4.3 e 4.7. |
| Versão 6 | 22/12/2025 | Revisão integral do documento |