Política de Segurança Cibernética

1. OBJETIVO

Esta Política de Segurança Cibernética ("Política") tem como objetivo definir as regras relacionadas à Segurança da Informação da Cora Sociedade de Crédito, Financiamento e Investimento S.A. ("Cora SCFI"), da Cora Tecnologia Ltda. ("Cora Tecnologia") e da 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.

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 Crises: 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.

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

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

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.

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. Métricas e Indicadores

A Cora realiza o acompanhamento constante de métricas e indicadores a fim de controlar, auditar e aumentar o nível de maturidade e conformidade em segurança da informação.

4.2. Comprometimento

Todas as Pessoas Colaboradoras, consultores e prestadores de serviço da Cora, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e guarda dos ativos tecnológicos e informações das quais são usuários, dos ambientes tecnológicos que possuam, respeitando as Políticas e controles implantados.

4.3. Classificação e Tratamento da Informação

Todas as informações e os respectivos recursos tecnológicos que as suportam devem ser classificados de acordo com grau de sigilo e receber o tratamento que garanta a proteção durante todo o ciclo de vida.

4.4. Gestão de Riscos

A área de Cybersecurity presta apoio com recomendações de controles e proteções de segurança cibernética às áreas envolvidas no desenvolvimento de novos produtos e serviços da Cora, bem como na avaliação de riscos, buscando identificar ameaças e impactos sobre os ativos empresariais.

4.5. Gestão de Acessos

O acesso aos ativos empresariais da Cora deve ser controlado, registrado e monitorado, com base nos princípios da necessidade de conhecer e do privilégio mínimo para o desempenho das atividades profissionais para garantir que as informações não sejam divulgadas, modificadas, excluídas ou tornadas indisponíveis indevidamente.

4.6. Monitoramento

A Cora reserva-se o direito de monitorar o acesso e utilização de seus equipamentos, sistemas e ambientes tecnológicos, de forma que ações indesejáveis ou não autorizadas sejam detectadas proativamente e posteriormente tratadas.

4.7. Treinamento 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.

4.8. Desenvolvimento Seguro

Todo o ciclo de vida do desenvolvimento de aplicações da Cora deve seguir as melhores práticas de desenvolvimento a fim de produzir softwares seguros, assim, buscando a mitigação do surgimento de vulnerabilidades de segurança em todas as etapas do processo.

4.9. Contratação De Serviços Terceirizados

Deve-se assegurar que a parte contratada, e eventual(is) subcontratada(s) e/ou subordinada(s) cumpram os requisitos mínimos de governança cibernética no âmbito do gerenciamento de risco operacional por meio de avaliação realizada pela equipe de Cybersecurity.

5. GESTÃO DE INCIDENTES

Todas as Pessoas Colaboradoras, consultores e prestadores de serviço da Cora, em qualquer vínculo, função ou nível hierárquico têm a obrigação de reportar imediatamente quaisquer incidentes de segurança que tomarem conhecimento, de modo com que estes possam ser registrados, avaliados e tratados pela área responsável.

5.1. Avaliação, Categorização e Comunicação de Incidentes

A fim de possibilitar uma análise mais precisa e eficaz da gravidade dos incidentes, bem como a implementação de ações apropriadas para mitigação e resposta adequada destes, a Cora estabeleceu parâmetros para avaliar e categorizá-los. Os incidentes de

Segurança Cibernética classificados como relevantes devem ser reportados, de imediato, ao Comitê de Crises da Cora.

6. COMUNICAÇÃO DE EVENTOS E CANAIS DE COMUNICAÇÃO

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

Toda Pessoa Colaboradora tem a obrigação de informar a referida Área sobre qualquer evento, potencial ou efetivo, do qual tenha conhecimento, a fim de que as medidas mitigadoras possam ser adotadas tempestivamente pela Cora.

7. MEDIDAS DISCIPLINARES

A violação das diretrizes definidas nesta Política, bem como de seus procedimentos e documentos correlatos, sujeita a aplicação de sanções pelos responsáveis, na forma prevista no Código de Ética e Conduta da Cora, nas normas e legislações vigentes.

A Pessoa Colaboradora que deliberadamente deixar de notificar violações a esta Política também estará sujeita às medidas mencionadas acima.

8. 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.

9. 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.

10. DOCUMENTOS RELACIONADOS

Política de Privacidade

11. 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.