DAPPER
Sociedade de Crédito Direto

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

CÓDIGO PSC – 01

VERSÃO 01 – OUTUBRO 2023

Sumário

1. OBJETIVOS

Esta Política de Segurança Cibernética e da Informação; com base Resolução CMN nº 4.893, de 26 de fevereiro de 2021 e na Lei nº 13.709, de 14 de agosto de 2018, a LGPD – Lei Geral de Proteção de Dados; estabelece os princípios, conceitos, valores e práticas adotados pela **DAPPER SOCIEDADE DE CRÉDITO DIRETO S/A**, visando assegurar a confidencialidade, a integridade e a disponibilidade dos seus dados ou por ela controlados, e dos sistemas de informação por ela utilizados, permitindo à DAPPER SCD prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético, e proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural

2. PÚBLICO-ALVO

Este documento é dirigido a todos os clientes, acionistas, diretores, conselheiros, administradores, colaboradores (empregados ou não), menores aprendizes, estagiários, correspondentes, prestadores de serviços de terceiros, e a todas e quaisquer pessoas que terão acesso aos dados da DAPPER SCD ou por ela controlados, e aos sistemas por ela a serem utilizados.

3. DOS PRINCÍPIOS

As ações da DAPPER SCD serão regidas pelos seguintes princípios:

3.1 Confidencialidade

Limitação do acesso à informação, sendo permitido o acesso somente às pessoas autorizadas e em circunstâncias que se apresentem efetivamente necessárias, protegendo informações que devem ser acessíveis apenas por um determinado grupo de usuários contra acessos não autorizados.

3.2 Disponibilidade

Garantia de acesso às pessoas devidamente autorizadas à informação sempre que for necessário, prevenindo interrupções das operações da DAPPER SCD por meio de um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança.

3.3 Integridade

Garantia da veracidade, fidelidade e integridade da informação e dos métodos de seu processamento e eventual tratamento da informação, pois esta não deve ser alterada enquanto está sendo transferida ou armazenada, impedindo que a informação fique exposta ao manuseio por pessoa não autorizada e impedindo alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

4. DAS DIRETRIZES DE SEGURANÇA CIBERNÉTICA

A Segurança Cibernética na DAPPER SCD seguirá as seguintes diretrizes:

- As informações serão tratadas de forma ética, sigilosa e de acordo com as leis vigentes e normas internas, evitando mau uso e exposição indevida;

- As informações e os dados serão utilizados de forma transparente e apenas para as finalidades para os quais foram coletados;
- Os procedimentos e os controles abrangerão a autenticação, a criptografia, a prevenção, a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes, varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores, e a manutenção de cópias de segurança dos dados e das informações;
- A identificação daqueles que tem acesso às informações da DAPPER SCD será única, pessoal e intransferível, qualificando-os como responsáveis pelas ações realizadas;
- Somente os indivíduos autorizados terão acesso às informações e recursos de informação que sejam imprescindíveis para o pleno desempenho das suas atividades;
- A senha será utilizada como assinatura eletrônica, sendo pessoal e intransferível, e deverá ser mantida secreta, sendo proibido seu compartilhamento;
- O/A Diretor(a) da DAPPER SCD, responsável pela Política de Segurança Cibernética designado no UNICAD - Sistema de Informações sobre Entidades de Interesse do Banco Central, será responsável pelo registro e controle dos efeitos de incidentes relevantes e os riscos às informações;
- Deverá ser reportado ao/à Diretor(a) da DAPPER SCD, responsável pela Política de Segurança Cibernética, fatos ou ocorrências que possam colocar em risco as informações;
- As responsabilidades quanto à Segurança Cibernética serão amplamente divulgadas a todos aqueles considerados público-alvo da política, que deverão entender e assegurar o cumprimento do conteúdo disposto.

5. DAS DIRETRIZES PARA TRATAMENTO DA INFORMAÇÃO

A informação receberá proteção adequada em observância aos princípios e diretrizes da Segurança Cibernética e da Informação da DAPPER SCD em todo o seu ciclo de vida, que compreenderá: Geração, Manuseio, Armazenamento, Transporte e Descarte.

6. DAS DIRETRIZES PARA CLASSIFICAÇÃO DE DADOS E DAS INFORMAÇÕES

As informações e os dados sob responsabilidade da DAPPER SCD serão classificados conforme adequação das estruturas organizacionais aos princípios e às diretrizes da política de segurança cibernética e da informação, considerando a relevância, a confidencialidade e as proteções necessárias nos seguintes níveis:

6.1 Dado NÃO Pessoal

Informação não relacionada à pessoa física ou jurídica identificada/identificável:

- Público: aquele explicitamente aprovado por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio. Possuem caráter informativo geral e são direcionadas ao público em geral;
- Interno: destinado ao uso interno da DAPPER SCD disponível a todos os usuários. O acesso às informações dessa natureza, ainda que não autorizado, não afetará os negócios, seus funcionários ou seus clientes, contudo, é considerado incidente de segurança de baixa relevância e, portanto, seu responsável está sujeito às sanções cabíveis. Essas informações não exigem proteções especiais, salvo aquelas entendidas como mínimas para impedir o acesso não autorizado;

- Restrito: dados com acesso autorizado a apenas um usuário específico ou um grupo de usuários. Diferem dos dados internos uma vez que que não estão disponíveis para todos os usuários e sua eventual divulgação poderia afetar significativamente os negócios, funcionários, terceiros, clientes ou outros.

6.2 Dado Pessoal

Informação relacionada a pessoa física ou jurídica identificada/identificável:

- Dado pessoa física ou jurídica sensível: dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, dado protegido pelo sigilo das operações ativas e passivas e serviços prestados ou dado que possa ser utilizado para fins discriminatórios, ilícitos ou abusivos, quando vinculados a uma pessoa natural. A divulgação de tais dados é proibida, salvo se necessária e decretada por órgãos competentes, para apuração de ocorrência de qualquer ilícito, conforme dispõe o Art. 1º, parágrafo 4º, da Lei Complementar nº 105, de 10 de janeiro de 2021, que trata sobre o sigilo das operações de instituições financeiras. Os dados sensíveis deverão ser protegidos de forma mais rígida, incluindo iniciativas de rastreabilidade da informação e controle de acesso diferenciado, devendo ser compatível com as funções desempenhadas e com a sensibilidade das informações. Para tanto, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. Uma vez classificada a informação deve ser protegida e receber tratamento e armazenamento adequados;
- Dado pessoal não sensível: dado pessoal que não seja classificado como sensível pelo art. 5º, inciso II, da Lei nº 13.709/18 e que, portanto, não possa ser utilizado para fins discriminatórios, ilícitos ou abusivos;

7. DAS DIRETRIZES PARA A ELABORAÇÃO DE CENÁRIOS DE INCIDENTES CONSIDERADOS NOS TESTES DE CONTINUIDADE DE NEGÓCIOS

Serão elaborados cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados pela DAPPER SCD, que tenham ou possam ter a capacidade de causar interrupção nos seus processos de negócios.

Para tanto, serão consideradas a ausência de ativos, humanos ou tecnológicos, que assegurem a confiabilidade, a integridade, a disponibilidade, a segurança e o sigilo dos dados e dos sistemas de informação, como:

- Vazamento de dados;
- Indisponibilidade de recursos computacionais;
- Problemas relacionados a software, banco de dados, servidor de aplicação e rede;
- Quebra da integridade dos dados, via alteração ou injeção fraudulenta de dados/informações em sistemas e/ou bases de dados;
- Fraudes eletrônicas, incluindo a realização de transações fraudulentas em sistemas de informação da DAPPER SCD;
- Desastres ou catástrofes, naturais ou não;
- Danos físicos relevantes a instalações ou equipamentos críticos, intencionais ou não;
- Falhas no fornecimento de energia elétrica.

8. DAS DIRETRIZES PARA A DEFINIÇÃO DE PROCEDIMENTO E DE CONTROLES VOLTADOS À PREVENÇÃO E AO TRATAMENTO DOS

INCIDENTES A SEREM ADOTADOS POR EMPRESAS PRESTADORAS DE SERVIÇOS

Na elaboração de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços; considerando as características do serviço a ser prestado e níveis de complexidade, abrangência e precisão; serão analisados cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados, e dos sistemas de informação utilizados.

Caso necessário, serão estabelecidos com a prestadora de serviços outros procedimentos e controles de prevenção e ao tratamento dos incidentes a serem adotados, de forma a suprir as possíveis lacunas relativas à prevenção, detecção e redução da vulnerabilidade a incidentes relacionados com o ambiente cibernético.

9. DAS DIRETRIZES PARA DEFINIÇÃO DOS PARÂMETROS A SEREM UTILIZADOS NA AVALIAÇÃO DE RELEVÂNCIA DOS INCIDENTES

Os parâmetros a serem utilizados na avaliação da relevância dos incidentes considerarão a frequência e o impacto dos cenários de incidentes, que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da DAPPER SCD.

10. PROCEDIMENTOS E CONTROLES

Para reduzir a vulnerabilidade a incidentes e atender aos demais objetivos de segurança cibernética, a DAPPER SCD, inclusive no desenvolvimento de sistemas de informação seguros e novas tecnologias, adotará os seguintes procedimentos e controles:

10.1 Autenticação

A autenticação é um processo que busca verificar a identidade digital do usuário de um sistema quando ele requisita um login (abreviação para o termo em inglês "*logging in*", que significa "se conectar") em um programa, aplicativo ou computador. A autenticação normalmente depende de um ou mais "fatores de autenticação". A DAPPER SCD utilizará mecanismos de autenticação baseados no conhecimento (com login e senha) em vários níveis, delimitando e controlando o acesso às informações. Todas as informações armazenadas estarão protegidas por sistemas que exigem a autenticação prévia para o acesso. Os acessos à arquivos na rede também exigirão autenticação central. A DAPPER SCD adotará políticas para atualização periódica de senhas, bem como padrões de força para as senhas. As senhas serão armazenadas de forma criptografada na base de dados. Os seguintes acessos exigirão autenticação:

- Sistema de e-mails;
- Consultas a base de dados (em todos os canais);
- Sistemas ERP (Planejamento de Recursos Empresariais);
- APIs (Interface de Programação de Aplicação) de Integração;
- Diretórios e arquivos na rede;
- Estação de Trabalho.

10.2 Criptografia

A criptografia é um conjunto de técnicas que transformam dados em códigos que só podem ser decifrados por quem tenha a chave de acesso. Assim, a criptografia garante a proteção dessas informações e permite que apenas quem tem direito cedido ao acesso (autenticação) consiga visualizar seu conteúdo. A DAPPER SCD classificará suas informações de acordo com o seu sigilo.

Para a base de dados, a maioria dos SGBD (Sistemas Gerenciadores de Base de Dados) comercializados, possuem suporte nativo à criptografia de informações.

10.3 Prevenção e detecção de intrusão

Todos os recursos do sistema de informação expostos à Internet deverão ser acompanhados e protegidos por um IDS/IPS (Sistema de detecção de intrusos). Sempre que o IDS/IPS detectar ou responder a uma tentativa externa mal-intencionada, suficientemente grave para ameaçar os recursos do sistema de informações protegidas, uma análise estruturada e procedimento de resposta deverá ser acionado.

10.4 Prevenção de vazamento de informações

Deverão ser implementados em todos os sistemas o controle para prevenção de perda de dados, responsável por garantir que dados confidenciais não sejam extraviados, furtados, mal utilizados ou vazados na web por usuários não autorizados.

10.5 Testes e varreduras periódicos para detecção de vulnerabilidades

Os testes e varreduras periódicos serão executados através de softwares com tecnologia “Scanner Ativo”, que realizará varreduras nos sistemas e máquinas em busca de pontos sensíveis ou vulnerabilidades.

10.6 Proteção contra software malicioso

Serão implementados controles tecnológicos para a proteção dos equipamentos de processamento de informação que executem algum tipo de software (tanto de usuário final como servidores), para a prevenção, detecção, correção e erradicação de códigos executáveis maliciosos, assim como a verificação da atualização das ferramentas de proteção baseadas em assinaturas para que estejam nas últimas atualizações disponíveis.

10.7 Mecanismos de rastreabilidade para informações sensíveis

Com padronização de recebimento dos dados, a rastreabilidade das informações sensíveis será garantida através do acesso controlado dos usuários ao sistema de informação, sendo que as senhas ficarão armazenadas de forma criptografada na base de dados. Através do controle de acesso individual, as consultas na base de dados permitirão o registro e rastreio das informações.

10.8 Controles de acesso

A DAPPER SCD utilizará mecanismos de controle de acesso por autenticação e todos os sistemas listados no item “10.1 Autenticação”, que permitirá acesso às informações apenas aos usuários autorizados, de acordo com o nível de sigilo e acesso.

10.9 Segmentação de rede de computadores

A segmentação de rede é uma estratégia de segurança que será utilizada para proteger os dados de ataques cibernéticos, visto que permite a divisão da rede em subseções para que seja possível controlar a concessão de acessos dos usuários, de acordo com suas necessidades no trabalho. As redes da DAPPER SCD serão segmentadas de acordo com o tipo de informação e local de acesso.

10.10 Manutenção de cópia de segurança dos dados e das informações

Serão realizados “backups”, cópia de segurança dos dados e das informações, na qual serão registradas todas as decisões sobre armazenamento de dados, que assim serão definidos:

- Quais dados serão copiados;
- Frequência de realização do processo;
- Tipo de backup a ser realizado;
- Prazo pelo qual os arquivos de backup deverão ser mantidos;
- Funcionários envolvidos no processo.

10.11 Registro, análise da causa e do impacto, e controle dos efeitos de incidentes relevantes

Para que seja possível a melhoria contínua dos procedimentos relacionados à segurança cibernética, permitindo que sejam realizadas as adequações necessárias à correção de vulnerabilidades nas medidas e procedimentos relativos à segurança, serão realizados o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da DAPPER SCD, abrangendo, inclusive, informações recebidas de empresas prestadoras de serviços a terceiros, sendo elaborado relatório próprio pela área responsável.

10.12 Gestão de Prestadores de Serviço

Quando da contratação de prestadores de serviço, inclusive serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, a DAPPER SCD adotará as seguintes práticas de governança corporativa e de gestão:

10.12.1 Abrangência

Deverão ser consideradas para fins de aplicação do disposto na política, aquelas empresas prestadoras de serviços a terceiros que tiverem acesso aos dados da DAPPER SCD, ou por ela controlados, aos sistemas por ela utilizados ou ainda aos ambientes físicos ou tecnológicos, que possam ser utilizados para acessar os dados e sistemas;

10.12.2 Cláusulas contratuais

Os contratos com empresas prestadoras de serviços a terceiros deverão conter cláusulas de confidencialidade e responsabilidades entre as partes, bem como cláusulas que garantam que os profissionais das empresas prestadoras de serviços a terceiros:

- Protejam e zelem pelo sigilo das informações da DAPPER SCD;
- Tenham conhecimento e cumpram esta política;
- Cumpram as leis e normas que regulamentam a propriedade intelectual e a proteção de dados, em especial a Lei nº 13.709 e a Resolução nº 4.893;
- Utilizem os dados, os sistemas, bem como os ambientes físico e tecnológico da DAPPER SCD, ou por ela controlados, apenas para as finalidades objeto do contrato de prestação de serviço;
- Comuniquem imediatamente qualquer violação desta Política e/ou outras Normas.

10.12.3 A DAPPER SCD somente contratará prestadores de serviços que demonstrarem a adoção dos seguintes procedimentos de prevenção e tratamento de incidentes:

- Adoção de software de proteção contra softwares maliciosos, mantendo-o sempre ativado e atualizado;
- Adoção de Firewall, mantendo-o sempre ativado e atualizado;
- Adoção de processo de manutenção de cópias de segurança dos dados e das informações, seja ele realizado para servidor físico ou em nuvem, a ser executado no mínimo semanalmente;
- Adoção de mecanismos de controles de acesso e de autenticação que permitam identificar e rastrear o usuário que tiver acesso aos sistemas ou dados da DAPPER SCD e seus clientes no ambiente cibernético;
- Adoção de mecanismos de criptografia que permitam criptografar os dados pessoais de clientes e os dados pertencentes à DAPPER SCD armazenados pelo prestador de serviço ou enviado por meios de comunicação;
- Adoção de mecanismos de segmentação da rede pela qual o prestador de serviço acessa aos sistemas, dados ou dos clientes da DAPPER SCD;

11. CONTRATAÇÃO DE PRESTADOR(ES) DE SERVIÇOS RELEVANTES DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Na contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, além das práticas de governança corporativa

e de gestão referidas acima, a DAPPER SCD adotará as seguintes práticas de governança corporativa e gestão:

11.1 Abrangência

Além dos serviços relevantes de processamento e armazenamento de dados, para fins de política, os serviços de computação em nuvem abrangerão a disponibilidade da DAPPER SCD, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à DAPPER SCD implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos ou adquiridos por ela;
- Implantação ou execução de aplicativos desenvolvidos pela DAPPER SCD, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

11.1.1 Avaliação da relevância do serviço a ser contratado

Previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, a DAPPER SCD avaliará a relevância do serviço a ser contratado, considerando:

- Os riscos a que estará exposta;
- A criticidade do serviço;
- A sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado;
- A classificação da informação a ser tratada pelo prestador.

11.1.2 Critérios de decisão quanto à contratação

A DAPPER SCD estabelecerá como critérios de decisão quanto à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, a capacidade do potencial prestador de serviço de assegurar:

- O cumprimento da legislação e da regulamentação em vigor;
- O acesso aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processadas ou armazenadas;
- A aderência às certificações exigidas por lei para a prestação do serviço a ser contratado;
- O acesso aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados;
- O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A identificação e a segregação dos dados dos clientes da DAPPER SCD por meio de controles físicos ou lógicos;
- A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da DAPPER SCD;
- O acesso às informações a serem fornecidas visando verificar o cumprimento do disposto em cláusulas referentes à:

- indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
- adoção de medidas de segurança para a transmissão e armazenamento dos dados;
- manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;
- aderência do prestador de serviço às certificações exigidas por lei;
- concessão de acesso aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços aqui contratados, quando aplicável;
- concessão de acesso às informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- confidencialidade, integridade e disponibilidade dos dados da DAPPER SCD, bem como pelo cumprimento da legislação e da regulamentação em vigor;
- prestação dos serviços, armazenamento, processamento e gerenciamento dos dados unicamente nos países e regiões previamente estabelecidos e comprometendo-se a não mudar a localização indicada sem a prévia autorização;
- transferência dos dados recebidos para a prestação do serviço ao novo prestador de serviços ou à DAPPER SCD, em caso de extinção do contrato, e a excluir os dados recebidos para a

prestação do serviço, após a transferência dos dados e a confirmação da integridade e da disponibilidade;

- não promoção de subcontratação de serviços sem autorização prévia;
- concessão de acesso ao Banco Central do Brasil aos contratos e aos acordos firmados para a prestação dos serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;
- obrigação de mantê-la permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;
- obrigação em caso de disposição através de Resolução e Normativas do Banco Central do Brasil e/ou demais órgãos competentes:

a) conceder pleno e irrestrito acesso ao órgão competente aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações, que estejam em seu poder;

b) enviar notificação prévia de forma expressa sobre a intenção de interromper a prestação de serviços, com pelo menos 30 (trinta dias) de antecedência da data prevista para a interrupção, observado que o prestador de serviço se obriga

a aceitar eventual pedido de prazo adicional de mais (30) trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;

c) enviar notificação prévia de forma expressa sobre a intenção de interromper a prestação de serviços, com pelo menos 30 (trinta dias) de antecedência da data prevista para a interrupção, quando a motivação da interrupção dos serviços prestados for causada por inadimplência da DAPPER SCD.

11.1.3 Cláusulas Contratuais

Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

- a indicação dos países e da região em cada país onde os serviços poderão ser prestados;
- a adoção de medidas de segurança para a transmissão e armazenamento dos dados;
- a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;
- a obrigatoriedade, em caso de extinção do contrato, de:
    - transferência dos dados ao novo prestador de serviços ou à DAPPER SCD;
    - exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos;
    - o acesso da DAPPER SCD contratante às informações fornecidas pela empresa contratada, visando a verificar o cumprimento dessas obrigações;

- o acesso às informações relativas às certificações e aos relatórios de auditoria especializada;
- o acesso a informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

- a obrigação da empresa contratada a notificar a DAPPER SCD sobre a subcontratação de serviços relevantes;
- a permissão de acesso ao Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;
- a adoção de medidas adotadas pela DAPPER SCD em decorrência de determinação do Banco Central do Brasil e demais órgãos competentes; e
- a obrigação da empresa contratada manter a DAPPER SCD permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação em vigor.

11.1.4 Comunicação da contratação ao Banco Central do Brasil

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deverão ser comunicadas ao Banco Central do Brasil, devendo a comunicação conter a denominação da empresa a ser contratada, os serviços relevantes a serem contratados e a indicação dos países e das regiões em cada país, onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados.

A referida comunicação de contratação ou de eventuais alterações contratuais devem ser realizadas, no máximo, até 10 (dez) dias após a ocorrência. Para a contratação de serviços relevantes de processamento, armazenamento de dados

e de computação em nuvem prestados no exterior deverão ser observados requisitos dispostos no Capítulo III, Resolução nº 4.893, de 26 de fevereiro de 2021.

11.1.5 Documentação

Deverão ser documentadas as práticas de governança corporativa e de gestão adotadas, proporcionais à relevância do serviço a ser contratado e aos riscos aos quais a DAPPER SCD se expõe.

Da mesma forma, deverá ser também documentada a verificação da capacidade do potencial prestador de serviço de assegurar:

- o cumprimento da legislação e da regulamentação em vigor;
- o acesso da DAPPER SCD aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- a sua aderência às certificações exigidas pela DAPPER SCD para a prestação do serviço a ser contratado;
- o acesso da DAPPER SCD aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- a identificação e a segregação dos dados dos clientes da DAPPER SCD por meio de controles físicos ou lógicos; e
- a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da DAPPER SCD.

12. COMUNICAÇÃO DE INCIDENTES DE SERGURANÇA À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A DAPPER SCD comunicará à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados, a ocorrência de incidente de segurança, seja ele relativo ao ambiente cibernético ou não, que possa acarretar risco ou dano relevante aos titulares. A referida comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

- a descrição da natureza dos dados pessoais afetados;
- as informações sobre os titulares envolvidos;
- a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comerciais e industriais;
- os riscos relacionados ao incidente;
- as causas do incidente;
- o impacto do incidente;
- os motivos da demora, no caso de a comunicação não ter sido realizada e forma imediata;
- as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente.

13. COMUNICAÇÃO DE INCIDENTES RELEVANTES RELACIONADOS AO AMBIENTE CIBERNÉTICO AO BANCO CENTRAL DO BRASIL

A DAPPER SCD comunicará ao Banco Central do Brasil as ocorrências de incidentes relevantes e das interrupções dos serviços que configurem uma situação de crise pela Instituição financeira, bem como das providências para o reinício das suas atividades.

14. MECANISMOS PARA DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA NA DAPPER SCD

Para a disseminação da cultura de segurança cibernética a DAPPER SCD adotará os seguintes mecanismos:

- Disseminação dos princípios e diretrizes da Segurança Cibernética por meio de programas de conscientização, capacitação e avaliação periódicas de pessoal;
- Divulgação e compartilhamento, de forma que seu conteúdo possa ser consultado a qualquer momento, da política e as regras de segurança da informação e segurança cibernética para todo o público-alvo abrangido pela política;
- A prestação de informações a clientes e usuários sobre as precauções na utilização de produtos e serviços financeiros, em sua página na internet;
- A divulgação ao público, na página da DAPPER SCD na internet, de resumo contendo as linhas gerais da política de segurança cibernética.

15. PROGRAMA DE SEGURANÇA CIBERNÉTICA

Conforme sua criticidade, o programa de segurança cibernética será dividido em:

- Ações críticas: correções emergências e imediatas para mitigar riscos iminentes;
- Ações de Sustentação: Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro e permitindo que ações de longo prazo/estruturantes possam ser realizadas;
- Ações Estruturantes: Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos, voltadas para o futuro da DAPPER SCD.

16. GOVERNANÇA COM AS ÁREAS DE NEGÓCIO E TECNOLOGIA

As iniciativas e projetos das áreas de negócio e tecnologia estarão alinhadas com as diretrizes e arquiteturas da Segurança Cibernética, garantindo a confidencialidade, integridade e disponibilidade das informações.

17. SEGURANÇA NO DESENVOLVIMENTO DE SISTEMAS DE APLICAÇÃO

O processo de desenvolvimento de sistemas de aplicação deverá garantir aderência às políticas de segurança da DAPPER SCD e às boas práticas de segurança.

18. RELATÓRIO ANUAL SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

A DAPPER SCD elaborará relatório anual sobre a implementação do plano de ação e de resposta a incidentes, tendo como data-base o dia 31 de dezembro de cada ano. O relatório deverá ser submetido ao comitê de risco, quando existente, e apresentado ao conselho de administração ou, na sua inexistência, à diretoria até 31 de março do ano seguinte ao da data-base, devendo abordar:

- A efetividade da implementação das ações desenvolvidas pela DAPPER SCD para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e
- Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

19. MANUTENÇÃO DA DOCUMENTAÇÃO

Deverão ficar à disposição do Banco Central do Brasil pelo prazo de 5 (cinco) anos:

- o documento relativo à política de segurança cibernética;
- o documento relativo ao plano de ação;
- o documento relativo ao plano de resposta a incidentes;
- os relatórios anuais de que tratam sobre a política;
- a documentação referente às práticas de governança corporativa e de gestão e a verificação da capacidade do potencial prestador de serviço;
- os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem, contado o prazo a partir da extinção do contrato;
- os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle da implementação e da efetividade:
    - da política de segurança cibernética, contado o prazo a partir da implementação;
    - do plano de ação, contado o prazo a partir da implementação;
    - do plano de resposta a incidentes, contado o prazo a partir da implementação; e
    - dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, contado o prazo a partir da implementação.

20. DA DIVULGAÇÃO

A Política de Segurança Cibernética e da Informação, e as demais políticas e normas complementares da DAPPER SCD, serão divulgadas ao Público-Alvo, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas, e com a sensibilidade das informações, devendo estar disponíveis em local acessível aos colaboradores e protegidas contra alterações. Além disso, será divulgado aos clientes um resumo contendo as linhas gerais da política de segurança cibernética, na página da DAPPER SCD na internet.

21. MEDIDAS DISCIPLINARES

As violações em relação a esta política estarão sujeitas às sanções disciplinares que estarão previstas nas normas internas da DAPPER SCD, e na legislação vigente no Brasil e nos países onde as empresas estiverem localizadas, tais como: advertências (verbais e/ou escritas), suspensões e demissões com e sem justa causa.

22. REVISÃO ANUAL

A POLÍTICA DE SEGURANÇA CIBERNÉTICA DAPPER SOCIEDADE DE CRÉDITO DIRETO S/A será revisada anualmente.

23. REVISÕES EXCEPCIONAIS

A política poderá ser atualizada mensalmente após a aprovação de funcionamento da DAPPER SCD pelo Banco Central, para que sejam integradas ao seu escopo as respectivas modificações a serem implementadas no curto e médio prazo, conforme plano de ação da DAPPER SCD. No longo prazo, as revisões anuais poderão contemplar novas modificações.

24. COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

A Diretoria da DAPPER SCD, ao aprovar a Política de Segurança Cibernética e da Informação, instituirá um compromisso para com a melhoria contínua dos procedimentos relacionados com a segurança cibernética e da informação, buscando sempre manter a DAPPER SCD em conformidade com normas legais e regulamentares sobre os referidos temas, guiada pelos princípios, conceitos, valores e práticas aqui elencados, com o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados da DAPPER SCD ou por ela controlados, e dos sistemas de informação por ela utilizados, permitindo à DAPPER SCD prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético protegendo os direitos fundamentais de liberdade e de privacidade.