CAPITAL CONSIG

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

SUMÁRIO

1. INTRODUÇÃO

Em um cenário global de crescente complexidade e sofisticação das ameaças cibernéticas, a

proteção contra-ataques, acessos indevidos, vazamentos de dados e indisponibilidade de serviços torna-se requisito estratégico para a continuidade dos negócios e para a manutenção da confiança de clientes, parceiros, acionistas e da sociedade.

A Capital Consig reconhece que a segurança cibernética vai além de uma obrigação regulatória, constituindo-se em um compromisso ético e organizacional que contribui para a segurança e a eficiência do sistema financeiro. Ao adotar controles eficazes, a instituição assegura não apenas conformidade com as normas nacionais e internacionais, como também a preservação de sua reputação, a mitigação de riscos operacionais e a proteção de informações de natureza estratégica.

Sendo assim, a presente Política Institucional de Segurança da Informação e Segurança Cibernética da Capital Consig ("Política") estabelece as diretrizes, os princípios, os procedimentos e as práticas da instituição na proteção de seus ativos digitais, informações sensíveis e infraestrutura tecnológica.

2. OBJETIVOS

Esta Política tem como objetivo geral estabelecer as diretrizes e a governança dos procedimentos, medidas e ações necessárias para garantir proteção, confidencialidade, integridade, disponibilidade e autenticidade dos dados e dos sistemas de informação da Capital Consig.

De modo específico, esta Política visa a:

- assegurar que o acesso aos dados e aos sistemas utilizados pela Capital Consig sejam restritos a indivíduos autorizados;
- estabelecer os procedimentos e os controles adotados para reduzir a vulnerabilidade da Capital Consig a incidentes e atender aos demais objetivos de segurança cibernética;
- dispor sobre os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;
- assegurar o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da Capital Consig;
- estabelecer as diretrizes para definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da Capital Consig;
- estabelecer diretrizes para a classificação dos dados e das informações quanto à relevância, definindo os parâmetros a serem utilizados na avaliação da relevância dos incidentes; e
- estabelecer os mecanismos para disseminação da cultura de segurança da informação e segurança cibernética da Capital Consig; e
- cumprir com todos os requisitos legais e regulamentares, garantindo que a Capital Consig opere em conformidade com as normas em vigor.

3. ABRANGÊNCIA E APLICAÇÃO

Esta Política é aplicável a:

- todos os integrantes do corpo funcional da Capital Consig, incluindo diretores, demais gestores, colaboradores, estagiários e prestadores de serviços em geral;
- fornecedores, parceiros comerciais e correspondentes no País;
- quaisquer terceiros que, de forma direta ou indireta, permanente ou pontual, necessitem ter acesso a informações, sistemas ou recursos tecnológicos da Capital Consig.

A adesão às disposições aqui estabelecidas é condição indispensável para o exercício das atividades profissionais relacionadas à Capital Consig. Dessa forma, contratos de trabalho, de prestação de serviços e de parceria devem conter cláusulas específicas de observância a esta Política. O descumprimento das regras poderá implicar em sanções disciplinares, rescisões contratuais e até responsabilizações administrativas, civis e criminais, conforme a gravidade da infração.

4. BASE NORMATIVA

Esta Política foi concebida e deverá ser implementada para assegurar o cumprimento de normas de ordem pública que dispõem sobre segurança, proteção, confidencialidade, integridade e disponibilidade de dados e sistemas de informação utilizados por instituições sujeitas à supervisão do Banco Central do Brasil.

Entre outros, merecem destaque os seguintes atos normativos aplicáveis à Capital Consig:

- **Lei Complementar nº 105, de 2001**, que dispõe sobre o sigilo das operações financeiras, determinando cuidados específicos na proteção de informações de clientes e contrapartes;
- **Lei nº 13.709, de 2018** (Lei Geral de Proteção de Dados – LGPD), que regula o tratamento de dados pessoais, impondo obrigações quanto à segurança, privacidade e uso adequado das informações;
- **Resolução CMN nº 4.557, de 2017**, que disciplina a estrutura de gerenciamento de riscos e de capital, impondo requisitos relacionados à gestão de riscos operacionais, incluindo os de tecnologia da informação; e
- **Resolução CMN nº 4.893, de 2021**, que dispõe sobre a política de segurança cibernética e os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem por instituições autorizadas a funcionar pelo Banco Central do Brasil

Ademais, a Capital Consig adota como referência as disposições:

- da **ISO/IEC 27001**, que especifica os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI); e
- da **ISO/IEC 27001**, que especifica um conjunto de diretrizes e um código de prática para a seleção e implementação de controles de segurança da informação.

5. PRINCÍPIOS FUNDAMENTAIS

A Política de Segurança de Informação e Segurança Cibernética da Capital Consig, bem como todos os atos e medidas dela decorrentes ou a ela associadas estão baseados nos seguintes princípios:

- **Confidencialidade**: os dados e sistemas de informação devem ser acessados apenas por pessoas devidamente autorizadas;
- **Integridade**: os dados e registros constantes dos sistemas da Capital Consig devem ser mantidos íntegros, completos e imunes a alterações não autorizadas;
- **Disponibilidade**: os sistemas, aplicações e informações da Capital Consign devem estar acessíveis às pessoas autorizadas, sempre que necessário às operações;
- **Autenticidade**: os sistemas de informação da Capital Consig deverão assegurar a identidade de usuários, transações e sistemas, prevenindo fraudes e usurpações; e
- **Responsabilidade compartilhada**: todos, da alta administração aos prestadores de serviços terceirizados, têm o dever de conhecer, cumprir e zelar pela efetividade das medidas previstas desta Política, reconhecendo que a prevenção de incidentes cibernéticos é um compromisso coletivo

6. GOVERNANÇA E RESPONSABILIDADES

A estrutura de governança em segurança cibernética da Capital Consig está organizada em diferentes instâncias, de forma a assegurar que não haja lacunas nem sobreposições de responsabilidades.

A **Diretoria Executiva** é o órgão competente para aprovar esta Política, prover recursos financeiros, humanos e tecnológicos suficientes, supervisionar a efetividade dos controles e cobrar resultados. É também de sua responsabilidade manter alinhamento entre a estratégia institucional e os padrões regulatórios.

A **Área de *Compliance***, vinculada diretamente à Diretoria Executiva, é a unidade interna responsável pela coordenação da conformidade desta Política às normas legais e regulamentares em vigor, sendo responsável por implementar controles técnicos e organizacionais, conduzir

avaliações de risco, coordenar comunicações obrigatórias com autoridades reguladoras e propor revisões periódicas desta Política.

A **Área de Tecnologia da Informação (TI)** é a unidade interna competente para executar controles técnicos, monitorar sistemas e assegurar a operação segura dos ambientes tecnológicos.

A **Área de Recursos Humanos** é a unidade competente para, em conjunto com a Área de Tecnologia da Informação, definir os perfis de acesso dos usuários, consoante o nível de responsabilidade e a especificidade de uso de cada um.

Por fim, todos os **colaboradores**, independentemente de sua posição hierárquica, devem cumprir integralmente esta Política, participar de treinamentos, comunicar prontamente incidentes e cooperar com investigações internas.

7. PROCEDIMENTOS E CONTROLES

A Capital Consig adota diversos procedimentos e controles para a gestão de riscos de segurança de informação e riscos cibernéticos, de modo a assegurar a efetividade de seus princípios fundamentais e o cumprimento da legislação em vigor. A seguir, descrevemos os principais deles.

7.1 Gestão de ativos tecnológicos

Consideram-se ativos tecnológicos os equipamentos físicos (*hardwares*) e os programas ou aplicações (*softwares*) relacionados à atuação da Capital Consig.

Os ativos tecnológicos, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados, possuírem um proprietário, descartados de forma segura e serem protegidos contra acessos indevidos. Todos os ativos devem contar com licença de uso por seus fabricantes ou fornecedores.

Todos esses ativos devem contar com proteção, que pode ser física (como por exemplo por meio de salas com acesso controlado) e/ou lógica (ex: configurações de blindagem ou *hardening*, *patch management*, autenticação, autorização e monitoramento).

Os ativos devem ser tratados de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, promovendo o uso adequado e prevenindo exposição indevida das informações

7.2 Classificação da informação

Dentro da Capital Consig, toda informação deve ser classificada de acordo com a confidencialidade, observada a seguinte escala:

- **Informação pública**: acessível a qualquer pessoa, interna ou externamente (ex: informações em site institucional, releases públicos e comunicados oficiais);
- **Informação privada**: acessível apenas internamente na Capital Consig, por meio de compartilhamento entre colaboradores, mas não destinados ao público externo (ex: ;
- **Informação restrita:** acessível a áreas específicas ou pessoas autorizadas na Capital Consig, devido ao impacto que seus vazamentos podem causar (ex: dados financeiros ainda não divulgados, planos estratégicos, pareceres técnicos ou jurídicos sobre temas sensíveis); e
- **Informação confidencial:** é aquela altamente controlada, por ser crítica para a operação, eis em que sua divulgação pode causar prejuízo financeiro, legal ou reputacional (ex: dados de clientes, credenciais de acesso, segredos comerciais, informações cobertas por sigilo legal).

De acordo com a classificação da confidencialidade devem ser estabelecidas as proteções necessárias durante todo o ciclo de vida da informação, o qual compreende geração, manuseio, armazenamento, transporte e descarte.

7.3 Gestão de acessos

As concessões, revisões e exclusões de acesso a sistemas de informação devem ser efetivadas exclusivamente por meio de ferramentas próprias ou contratadas pela Capital Consig e que tenham sido previa e expressamente autorizados pela Diretoria Executiva.

A Área de Tecnologia da Informação, em conjunto com a Área de Recursos Humanos, deverá elaborar submeter à Diretoria Executiva o "**Manual de Acesso a Sistemas de Informação**" da Capital Consig, que deverá considerar, no mínimo, as seguintes diretrizes:

- os acessos devem ser rastreáveis, a fim de permitir a identificação individual do usuário que tenha acessado ou alterado as informações, permitindo sua responsabilização;
- a identificação de qualquer usuário deve ser única, pessoal e intransferível, razão pela qual a senha de acesso deve ser tratada como informação confidencial, pessoal e intransferível, sendo proibido seu compartilhamento
- a concessão de acessos deve obedecer ao critério de menor privilégio, segundo o qual os usuários devem ter acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades e devidamente autorizados;

- todo e qualquer acesso deve ser concedido por tempo determinado, mediante solicitação formal em sistema ou ferramenta própria, que deverá possuir rotina de relatório ou auditoria que seja capaz de registrar, no mínimo: o nome do solicitante, a data e hora da solicitação e da concessão do acesso e o nome do responsável pela liberação do acesso;

- independentemente do prazo fixado, a Área de Tecnologia da Informação, em conjunto com a Área de Recursos Humanos, deve efetuar a reavaliação regular da necessidade da manutenção do acesso de cada usuário, atuando inclusive para a revogação automática de acesso em caso de desligamento do usuário da empresa;

- a segregação de funções deve permear todos os processos e operações críticas da Capital Consig, devendo-se evitar que um único responsável possa executar e controlar com exclusividade todo o processo ou toda a operação durante todo seu ciclo de vida.

Especificamente quanto às senhas, o "**Manual de Acesso a Sistemas de Informação**" da Capital Consig, deverá prever, no mínimo, as seguintes exigências:

- a senha deve conter pelo menos oito caracteres, incluindo necessariamente letras maiúsculas, minúsculas, números e caracteres especiais;

- para acessos que forem considerados críticos, será obrigatória a autenticação multifator (MFA), acrescentando uma camada adicional de proteção;

- as senhas de usuários comuns devem ser renovadas a cada 180 dias, enquanto as de contas privilegiadas devem ser alteradas a cada 90 dias;

- será proibida a reutilização das últimas seis senhas de cada usuário;

- após cinco tentativas consecutivas de login inválido, a conta será bloqueada, somente podendo ser desbloqueada pela Área de Tecnologia da Informação mediante autenticação secundária;

- para credenciais de acesso que forem consideradas críticas, deverá ser utilizado cofre corporativo de senhas, ao qual só poderão ter acesso as pessoas prévia e expressamente autorizadas pela Área de Tecnologia da Informação;

- todas as alterações de senha serão registradas em logs de auditoria, monitorados permanentemente pela Área de Tecnologia da Informação.

- Qualquer negligência ou uso indevido de senhas sujeitará o usuário a medidas disciplinares.

7.4 Gestão e avaliação periódica de riscos

A Capital Consig adota a Abordagem Baseada em Risco (ABR), direcionando controles reforçados às áreas de maior criticidade, assegurando racionalidade e eficiência no uso dos recursos.

Os riscos devem ser identificados por meio de processos estabelecidos para análise de ameaças, identificação de vulnerabilidades, análise de probabilidades e impactos sobre os ativos da Capital Consig, para que sejam recomendadas as proteções adequadas. A instituição considera tanto riscos internos – relacionados a falhas humanas, erros operacionais e vulnerabilidades de sistemas – quanto riscos externos – como ataques de malware, *phishing*, engenharia social, *ransomware* e ameaças persistentes avançadas (APTs).

Produtos, processos e tecnologias devem ter a adequada gestão dos riscos de Segurança da Informação, para redução dos riscos à níveis aceitáveis, independentemente de estarem dentro da infraestrutura tecnológica da Capital Consig, de parceiros ou de prestadores de serviços.

As tecnologias em uso pela instituição devem estar em versões suportadas pelos seus fabricantes e devidamente atualizadas, de acordo com os processos de gestão de patches. Eventuais exceções devem ser aprovadas pela Diretoria Executiva.

A Capital Consig se compromete a realizar testes periódicos de vulnerabilidade e de intrusão (*pentests*) em seus sistemas, redes e aplicações críticas. Esses testes deverão identificar, avaliar e mitigar eventuais fragilidades que possam ser exploradas por agentes mal-intencionados ou resultar em falhas de segurança, protegendo assim os ativos informacionais e dados sensíveis da instituição. Os *pentests* devem simular cenários reais de ataque, dentro dos limites legais e contratuais, seguindo boas práticas de mercado e padrões internacionais reconhecidos.

Os testes de vulnerabilidade serão realizados pelo menos uma vez por ano e, adicionalmente, sempre que houver alterações relevantes no ambiente tecnológico (ex: atualização de sistemas, implementação de novos serviços, fusões/aquisições) ou no perfil de ameaças verificado no sistema financeiro nacional.

Todos os resultados e recomendações provenientes dos testes deverão ser documentados, tratados com prioridade e acompanhados até sua resolução. O relatório final de cada teste deve ser levado ao conhecimento da Diretoria Executiva da Capital Consig.

7.5 Gestão de riscos em Prestadores de Serviços e Parceiros

Os prestadores de serviços e parceiros contratados pela Capital Consig devem ser previamente submetidos a processo de avaliação de reputação, risco e capacidade técnica (*due diligence*) e serão classificados considerando critérios previstos no "Manual de Contratação de Serviços de Tecnologia da Informação", a ser proposto pela área de Tecnologia da Informação à aprovação da Diretoria Executiva.

De acordo com a classificação, o prestador de serviço ou parceiro passará por avaliação mais detalhada, que poderá incluir validação *in loco* dos controles de segurança da informação, avaliação remota das evidências ou outras avaliações, além do acompanhamento de eventuais correções e melhorias implementadas pelos prestadores de serviços e parceiros.

Especificamente nos casos de serviços de processamento e armazenamento de dados e de computação em nuvem, bem como de outros serviços ou sistemas terceirizados considerados pela Diretoria Executiva como críticos para a operação da Capital Consig, a Área de Tecnologia deverá, previamente à contratação, verificar a capacidade do potencial prestador de serviço de assegurar:

- o cumprimento da legislação e da regulamentação em vigor;
- o acesso da Capital Consig 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 a certificações exigidas pela Capital Consig para a prestação do serviço a ser contratado;
- o acesso da Capital Consig 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 Capital Consig 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 Capital Consig.

7.6 Proteção de perímetro

Para proteção da infraestrutura de sua infraestrutura contra ataques externos, a Capital Consig utilizará, o mínimo, ferramentas e controles contra ataques de indisponibilidade (DDoS), *spam*, *phishing*, APT/*Malware*, invasão de dispositivos de rede e servidores e ataques a aplicação.

Para mitigação do risco de vazamento de informações a Capital Consig utiliza ferramentas preventivas instaladas em dispositivos móveis, estações de trabalho e servidores, no serviço de correio eletrônico, no serviço de navegação *web*, no serviço de impressão, além do uso de criptografia para dados em repouso e em transporte.

Visando a elevar a proteção, não é permitida a conexão física ou lógica à rede corporativa da instituição, por equipamentos particulares não gerenciados ou não homologados pela Capital Consig.

7.7 Proteção contra ataques internos

Para proteção de sua infraestrutura contra ataques internos, a Capital Consig utiliza ferramenta de *antimalware* homologada contra ameaças cibernéticas.

7.8 Proteção de dados e privacidade

A Capital Consig mantém estrito compromisso com a proteção de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709, de 2018). A instituição possui política própria para isso e adota mecanismos técnicos e organizacionais para prevenir acessos não autorizados, vazamentos ou tratamentos indevidos de dados pessoais de clientes, colaboradores, parceiros e terceiros.

A coleta, armazenamento, uso e compartilhamento de dados obedecem a princípios de finalidade, adequação, necessidade e transparência. As informações são classificadas por grau de criticidade e protegidas mediante controles de criptografia, anonimização e segregação de acessos.

Informações específicas sobre esse tema constam da "**Política de Proteção de Dados e Privacidade**" da Capital Consig.

8. TRATAMENTO DE INCIDENTES

A Área de Tecnologia da Informação monitora a segurança do ambiente tecnológico da Capital Consig, para garantir a pronta identificação, contenção, investigação e mitigação de

ocorrências que possam comprometer a confidencialidade, integridade, disponibilidade ou autenticidade de suas informações e sistemas.

A Capital Consig dispõe de um "**Plano de Ação e Resposta a Incidentes Cibernéticos**", elaborado pela Área de Tecnologia da Informação e aprovado pela Diretoria Executiva. Além disso, a instituição designa um de seus diretores como responsável por esta Política e pelo cumprimento do referido plano.

Os incidentes identificados passam por um processo de avaliação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação e demais informações necessárias. Tais incidentes são então classificados com relação ao impacto, de acordo com os critérios adotados pela Capital Consig. Para a definição de seu grau de relevância serão considerados aspectos como impacto ao sistema financeiro e comprometimento de dados de clientes e do público em geral, conforme descrito no Plano de Ação supramencionado.

A partir dessas análises, são adotadas as medidas corretiva necessárias para a resolução do incidente, bem como as medidas preventivas a fim de reforçar os controles internos, evitar recorrências e aprimorar continuamente a maturidade do programa de segurança cibernética.

Sempre que aplicável, a Capital Consig realiza a comunicação tempestiva às autoridades regulatórias competentes, como o Banco Central do Brasil. Em situações que envolvam dados pessoais, são adotados os procedimentos previstos na Lei Geral de Proteção de Dados (LGPD), incluindo, quando necessário, a notificação aos titulares afetados e à Autoridade Nacional de Proteção de Dados (ANPD), em linguagem clara e acessível, assegurando transparência e respeito aos direitos fundamentais de privacidade e proteção de dados.

A Área de Tecnologia da Capital Consig elabora relatórios anuais contendo os incidentes relevantes ocorridos no período, ações realizadas de prevenção e resposta aos incidentes e resultados dos testes de continuidade. Tal relatório é apresentado à Diretoria Executiva Conselho de Administração, conforme determinações legais e regulamentares.

9. DISSEMINAÇÃO DA CULTURA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

A Alta Administração da Capital Consig tem o firme compromisso com a disseminação dos princípios e diretrizes de segurança da informação e de segurança cibernética. Por isso, estimula e promove iniciativas que possam contribuir para esse propósito, entre as quais:

- programas de capacitação de seus colaboradores, presenciais e/ou telepresenciais;

- programas de avaliação periódica de pessoal; e
- divulgação de campanhas de conscientização relacionadas a confidencialidade, integridade e disponibilidade da informação, veiculadas por e-mail, portal corporativo, e-learning, em mídias ou redes sociais aos colaboradores e clientes.

10. SANÇÕES E MEDIDAS DISCIPLINARES

O cumprimento desta Política é de observância obrigatória por todos os colaboradores, administradores, prestadores de serviços, fornecedores e parceiros da Capital Consig. O descumprimento, seja por ação ou omissão, ensejará a aplicação de medidas disciplinares proporcionais à gravidade da infração e aos riscos gerados para a instituição.

As sanções podem variar desde advertências formais e treinamentos corretivos obrigatórios até desligamento do colaborador, rescisão contratual com terceiros e comunicação imediata às autoridades competentes, incluindo Banco Central do Brasil, Conselho Monetário Nacional e demais órgãos de supervisão, quando a gravidade ou a natureza do incidente assim o exigir.

O processo de apuração seguirá rito formal conduzido pela área de Compliance e Segurança da Informação, assegurando imparcialidade, ampla defesa e registro documental de todas as etapas. Essa abordagem visa equilibrar o caráter educativo e corretivo das medidas, promovendo a cultura de conformidade e reforçando a importância da segurança cibernética como responsabilidade coletiva.

11. REVISÃO DA POLÍTICA

Esta Política consiste em um conjunto dinâmico e evolutivo de normas e procedimentos, devendo ser sempre revista de modo a assegurar sua constante aderência ao ambiente regulatório e às melhores práticas de mercado.

Esta Política estará sujeita a revisão ordinária, com periodicidade mínima anual, ou a revisões extraordinárias, que poderão ser efetivadas sempre que houver mudanças relevantes no ambiente de risco, evolução tecnológica, alteração de exigências regulatórias ou transformação na estrutura organizacional da Capital Consig.

A responsabilidade pela revisão desta Política é da Diretoria Executiva da Capital Consig, que poderá consultar instâncias colegiadas, como o Comitê de Riscos e Compliance, para validação das alterações. Todas as revisões deverão ser devidamente documentadas em quadro de acompanhamento de atualizações, que indique número da versão, data de aprovação, principais alterações, responsável(is) pela atualização e previsão para a próxima revisão.

12. HISTÓRICO DE ATUALIZAÇÕES

Versão	Data de Aprovação	Alterações Principais	Responsável pela Atualização	Próxima Revisão Prevista
1	-	-	Diretoria Executiva	-
2	16/09/2025	Reestruturação completa do texto	Diretoria Executiva	16/09/2025