ANEXO XII - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA	Vigência	Documento	I	Informação Interna Internal Information Información Interna
	28/07/2026	CM-PC-002		
	Versão	Página		
	12	1 / 18		

A C&M Software é fornecedor global em softwares para o mercado financeiro, pagamentos instantâneos suportando diversos mercados como FedNow, Pix, SPB, PCR, OpenBanking além plataformas de bmp, pagamentos, e outras soluções inovadoras

Assim, o presente documento, Política de Segurança da Informação e Segurança Cibernética, tem como objetivo atender as melhores práticas e demais legislações correlatas, instituindo princípios e diretrizes de Segurança da Informação e Cibernética, com o propósito de limitar a exposição ao risco a níveis aceitáveis e garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e comunicações que suportam os objetivos estratégicos da C&M Software.

A Política de Segurança da Informação e Segurança Cibernética passará a fazer parte integrante de todos os Contratos celebrados entre a C&M Software e seus Clientes.

C&M SOFTWARE
Departamento Jurídico e Compliance

Histórico das Revisões

Versão	Motivo	Data Revisão	Atualizado por	Divulgação
1	Elaboração	20/07/2018	Márcio Borges	20/07/2018
2	Revisão	09/01/2020	Márcio Borges	09/01/2020
3	Revisão	23/05/2022	Márcio Borges	23/05/2022
4	Revisão	01/02/2023	Márcio Borges	08/02/2023
5	Revisão	02/05/2024	Leandro Souza	06/05/2024
6	Revisão	09/05/2025	Leandro Souza	12/05/2025
7	Adequação ao Normativo 664 BC	03/10/2025	Leandro Souza	05/10/2025
8	Adequação item 8 Normativo 664	27/10/2025	Leandro Souza	27/10/2025
9	Adequação ao Normativo 664	25/11/2025	Leandro Souza	25/11/2025
10	Adequação ao Normativo 498	17/12/2025	Leandro Souza	17/12/2025
11	Inclusão de Políticas adicionais	28/04/2026	Leandro Souza	28/04/2026
12	Adequação sem PSTI	28/07/2026	Leandro Souza	28/07/2026

1. CONCEITOS E DENIFIÇÕES:

1.1. Política de Segurança da Informação e Segurança Cibernética: Salvaguardas e ações para garantir a obtenção e a manutenção das propriedades de segurança da organização e das propriedades do(as) usuários(as) contra riscos de segurança relevantes no ambiente cibernético.

1.2. Confidencialidade: garantia de que a informação somente possa ser acessada por pessoas autorizadas, pelo período necessário.

1.3. Disponibilidade: garantia de que a informação esteja disponível para as pessoas autorizadas quando se fizer necessária.

1.4. Integridade: garantia de que a informação esteja completa, exata, íntegra e que não tenha sido modificada ou destruída indevidamente, de maneira não autorizada ou acidental durante o seu ciclo de vida.

1.5. Recuperação de Dados: conjunto de técnicas e procedimentos específicos para extrair informações em dispositivos de armazenamento digital que não podem mais ser acessados de modo convencional.

1.6. Ativos de Informação: tudo o que pode criar, processar, armazenar, transmitir e até excluir a informação. Podem ser tecnológicos ("software" e "hardware") e não tecnológicos (pessoas, processos e dependências físicas). Os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, fisicamente (salas com acesso controlado) e logicamente (configurações de blindagem ou "hardening", patch management, autenticação e autorização) e ter documentação e planos de manutenção atualizados anualmente.

1.7. Informação: resultado do processamento e organização de dados (eletrônicos ou físicos) ou registros de um sistema. É composta por dados, mas um conjunto de dados não necessariamente é considerado uma informação.

1.8. Sistemas de informação: de maneira geral, são sistemas computacionais utilizados pela C&M Software para suportar suas operações.

1.9. Classificação da Informação: As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis:

Restrita, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações

1.10. Gestão de Riscos: Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da C&M Software, para que sejam recomendadas as proteções adequadas. Os cenários de riscos de segurança da informação são escalonados nos fóruns apropriados, para decisão.

2. OBJETIVOS

2.1. A presente Política de Segurança da Informação e Segurança Cibernética tem por objetivo instituir princípios e diretrizes de Segurança da Informação e Cibernética, com o propósito de limitar a exposição ao risco a níveis aceitáveis e garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e comunicações que suportam os objetivos estratégicos da C&M Software.

2.1.1. Definirá as diretrizes e responsabilidades que devem subsidiar a elaboração de normas, procedimentos e padrões de proteção da informação, abrangendo sua geração, utilização, armazenamento e distribuição;

2.1.2. Garantirá a disponibilidade, integridade e confidencialidade da informação, independente do meio de armazenamento;

2.1.3. Garantirá que a informação seja utilizada por quem a necessita para a execução de suas atividades diárias;

2.1.4. Evitará que usuários possam fazer o uso da informação de forma mal-intencionada, para obtenção de benefícios próprios;

2.1.5. Estabelecerá padrões para subsidiar a elaboração do Termo de Ciência sobre o uso da informação;

2.1.6. Estabelecerá subsídios para as implementações de cláusulas específicas nos contratos que visam garantir que a informação tenha a devida proteção;

2.1.7. Atenderá aos objetivos de Controles Internos.

2.1.8. Estabelecer os princípios e diretrizes estratégicas de Segurança da Informação e Cibernética para a C&M SOFTWARE.

2.1.9. Definir a estrutura hierárquica de governança das políticas de segurança.

2.1.10. Atender aos requisitos legais, regulatórios e contratuais aplicáveis.

2.1.11. Fornecer o arcabouço para a criação, manutenção e revisão das instruções normativas específicas.

3. ABRANGÊNCIA

3.1 Esta Política aplica-se a todos os Colaboradores, Estagiários, Prestadores de Serviços, e quaisquer indivíduos que tenham acesso aos ativos de informação da C&M Software.

4. ESTRUTURA NORMATIVA

4.1. A estrutura normativa da Segurança da Cibernética da C&M Software é composta por um conjunto de documentos, relacionados a seguir.

4.1.1. Política: define a estrutura, as diretrizes e os papéis referentes à segurança da informação e cibernética;

4.1.2. Normas: estabelecem regras, definidas de acordo com as diretrizes da Política, a serem seguidas em diversas situações em que a informação é tratada;

4.1.3. Procedimentos: instrumentam as regras dispostas nas Normas, permitindo a direta aplicação nas atividades da C&M Software.

4.2. A estrutura de governança da segurança da informação é composta pelos seguintes níveis de documentação:

4.2.2. **Política de Segurança da Informação e Cibernética (PSI - Este documento):** Documento de mais alto nível, aprovado pela Diretoria, que estabelece a estratégia, os princípios fundamentais e o framework de controles.

4.2.3. **Instruções Normativas (IN-SI-XXX):** Documentos de políticas específicas que detalham os controles, requisitos, regras e responsabilidades operacionais para temas específicos de segurança. São aprovados pelo Comitê de Segurança de TI.

4.2.3. **Procedimentos e Planos Operacionais (POPXXX):** Documentos de caráter técnico ou operacional que instrumentalizam a execução das Instruções Normativas.

4.2.4 **Plano de continuidade de Negocios (PCN0001), Procedimento de Continuidade de Negocios (PO01):** Documentos referentes ao plano de continuidade de negócios.

4.2.5 **Riscos (RO-MMM-AAAA):** Análise de Risco da C&M Software.

4.2.6 **LGPD (LGPD0001):** Lei Geral de Proteção de Dados.

4.3. FRAMEWORK DE CONTROLES E REFERÊNCIAS A POLÍTICAS ESPECÍFICAS

Os controles de segurança implementados pela C&M SOFTWARE para atender aos requisitos regulatórios e de negócio estão detalhados nas Instruções Normativas listadas abaixo. Este framework serve como um mapa de referência centralizado.

Controle / Domínio de Segurança	Objetivo do Controle	Instrução Normativa Correspondente	Responsável Principal
Gestão de Ativos	Garantir a identificação, classificação, manuseio e descarte seguro dos ativos de informação.	IN-SI-014 - Gestão de Ativos	Suporte / Seg. da Informação
Classificação da Informação	Estabelecer níveis de sigilo e tratamentos adequados para as informações.	IN-SI-001 - Classificação, Rotulagem e Manuseio	Gestores da Informação
Uso Aceitável de Ativos	Definir as regras para o uso seguro dos ativos computacionais.	IN-SI-002 - Uso Aceitável de Ativos	Todos os Usuários
Gestão de Identidade e Acesso	Controlar o acesso lógico aos sistemas e dados com base no princípio do menor privilégio.	IN-SI-003 - Gestão de Identidade e Controle de Acesso	Seg. da Informação / Suporte
Uso de Equipamentos Pessoais (BYOD)	Estabelecer regras para o uso seguro de dispositivos pessoais no ambiente corporativo.	IN-SI-004 - Uso de Equipamentos Computacionais Pessoais	Seg. da Informação
Acesso à Internet e Mídias Sociais	Definir diretrizes para navegação segura e conduta em redes sociais.	IN-SI-005 - Acesso à Internet e Comportamento em Mídias Sociais	Todos os Usuários
Uso de E-mail e Mensageiros	Estabelecer regras para o uso seguro dos serviços de comunicação corporativa.	IN-SI-006 - Uso de Serviços de E-mail e Comunicadores Instantâneos	Todos os Usuários
Acesso Remoto	Garantir a segurança e o monitoramento de conexões externas à rede corporativa.	IN-SI-007 - Acesso Remoto	Seg. da Informação
Resposta a Incidentes	Estruturar o processo de identificação, contenção, erradicação e recuperação de incidentes.	IN-SI-008 - Resposta a Incidentes	Seg. da Informação / CSTI
Monitoramento	Estabelecer a base legal e os princípios para o monitoramento de ativos e serviços.	IN-SI-009 - Monitoramento de Ativos e Serviços	Seg. da Informação

Controle / Domínio de Segurança	Objetivo do Controle	Instrução Normativa Correspondente	Responsável Principal
Proteção contra Malware	Definir as defesas e procedimentos contra códigos maliciosos.	IN-SI-010 - Proteção contra Códigos Maliciosos	Seg. da Informação / Suporte
Backup e Recuperação	Garantir a disponibilidade dos dados através de cópias de segurança e planos de restore.	IN-SI-011 - Backup e Restore	Suporte
Gestão de Mudanças	Controlar mudanças no ambiente de TI para evitar impactos negativos na segurança e disponibilidade.	IN-SI-013 - Gestão de Mudanças	Operações
Gestão de Patches	Estabelecer o processo para identificação e aplicação tempestiva de atualizações de segurança.	IN-SI-015 - Gestão de Patches e Atualizações	Operações / Seg. da Informação
Gestão de Ameaças e Vulnerabilidades	Identificar, classificar, priorizar e remediar vulnerabilidades técnicas.	IN-SI-016 - Gestão de Ameaças e Vulnerabilidades	Seg. da Informação / Operações
Arquitetura de Segurança	Definir os princípios e padrões para o projeto seguro de sistemas e redes.	IN-SI-017 - Arquitetura de Segurança de Sistemas	Operações / Seg. da Informação
Gestão de Redes e Dispositivos	Estabelecer os controles para a operação segura da infraestrutura de rede.	IN-SI-018 - Gerenciamento de Redes e Dispositivos de Segurança	Operações / Seg. da Informação
Desenvolvimento Seguro	Estabelecer Processos para desenvolvimento seguro.	IN-SI-012 – Desenvolvimento Seguro	Seg. da Informação / Desenvolvimento
Gestão de Certificados Digitais	Estabelecer processos para gestão de certificados digitais.	IN-SI-023 – Gestão de Certificados digitais	Seg. da Informação / Operações
Segurança em integrações API	Estabelecer processos para segurança em conexões de APIs	IN-SI-024 Segurança em Integrações APIs	Seg. da Informação / Operações
Inteligência de Ameaças Cibernéticas	Estabelecer processos para inteligência contra ameaças cibernéticas.	IN-SI-025 – Inteligência de Ameaças Cibernéticas	Seg. da Informação
Controle de Vulnerabilidades no Desenvolvimento	Estabelecer controle de vulnerabilidade no desenvolvimento de produtos	IN-SI-019 – Controle de Vulnerabilidades no desenvolvimento.	Seg. da Informação / Desenvolvimento
Retenção de Arquivos de Lote	Estabelecer regras para retenção temporária de arquivos em lote.	IN-SI-020 – Política de Retenção de Arquivos de Lote	Operações

Controle / Domínio de Segurança	Objetivo do Controle	Instrução Normativa Correspondente	Responsável Principal
Proteção de Dados Pessoais	Estabelecer regras para uso e trânsito de dados pessoais nos sistemas da CMSW	IN-SI-021 – Política de proteção de dados Pessoais	Seg. da Informação
Gestão de Risco e Fraude no PSTI	Estabelecer regras para mitigar riscos e fraudes na CMSW	IN-SI-022 – Politica de gestão de risco e fraude do PSTI	Seg. da Informação
Plano de Continuidade de Negócio	Estabelecer e divulgar o plano de continuidade de negócios.	PCN0001 – Plano de Continuidade de Negócios.	Operações
Gestão de Riscos	Estabelecer processos e acompanhamento mensal de Gestão de Riscos.	Documentos Mensais	Seg. da Informação
Retenção e Gestão de Logs	Estabelecer processos pare retenção segura e gestão de logs sistêmicos	IN-SI-026 – Retenção e Gestão de Logs	Operações
LGPD	Política de LGPD da CMSW com base na lei federal	LGPD0001 – Lei Geral de Proteção de Dados	Seg. da Informação
Controles Específicos de PSTI (BCB)	Atender aos requisitos adicionais da Resolução BCB 498 para PSTIs.	Múltiplas (listadas acima, com foco nos itens 9.1 a 9.13 desta PSI)	Seg. da Informação / Operações
Uso de Equipamentos Moveis	Uso de dispositivos moveis no ambiente corporativo	IN-SI-024 – Uso de Equipamentos Moveis	Seg. da Informação
Auditorias Internas e Externas	Auditorias nos ambientes da C&M Software	IN-SI-028 – Política de Auditorias	Seg. da Informação / Presidencia

5. SEGURANÇA DA INFORMAÇÃO

5.1. Toda informação deve ter um proprietário identificado, o qual deve ser o responsável pela utilização da mesma na execução de atividades específicas do seu trabalho.

5.2. A informação deverá ser classificada e protegida, de acordo com seu grau de sigilo, integridade e disponibilidade, obedecendo também os controles internos em vigor.

5.3. As ações que afetam a segurança da informação devem ser registradas e armazenadas em arquivos magnéticos, sempre requerendo-se cópia de segurança e seguindo uma metodologia de avaliação do grau de risco oferecido.

5.4. As informações que se tornarem sem utilidade aos negócios da empresa devem ser destruídas, independentemente do meio em que residam e sempre respeitando a legislação que rege a prescrição de determinado documento.

5.5. Somente a Diretoria da C&M Software pode autorizar a divulgação pública de informações pertencentes às divisões da C&M Software, independente do canal de comunicação a ser utilizado: mídia impressa, eletrônica ou qualquer outro meio.

5.6. As informações (em formato físico ou lógico) e os ambientes tecnológicos utilizados pelos usuários são de exclusiva propriedade da C&M Software, não podendo ser interpretados como de uso pessoal;

5.7. Todos os Colaboradores e prestadores de serviços devem ter ciência de que o uso das informações e dos sistemas de informação pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação e Cibernética, podendo estas servir de evidência para a aplicação de medidas disciplinares, processos administrativos e/ou legais;

5.8. Todo processo, sempre que possível, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de uma pessoa ou equipe.

6. CONTROLE DE ACESSO LÓGICO (GESTÃO DE ACESSO)

6.1. As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da C&M Software. Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o Colaborador, prestador de serviço, para que seja responsabilizado por suas ações.

6.2. Aos Colaboradores e prestadores de serviços da C&M Software é fornecida identificação pessoal para cada respectivo acesso aos recursos tecnológicos. Essa identificação, geralmente representada por um código e senha, é pessoal e intransferível. A correta utilização da identificação é de responsabilidade do usuário.

6.3. As informações e os recursos tecnológicos (sistemas informatizados e equipamentos) serão disponibilizados apenas a quem necessitar utilizá-los no exercício de suas atividades profissionais.

6.4. Os equipamentos de informática devem ser dotados de dispositivos de segurança contra acessos não autorizados.

6.5. É proibida a conexão de equipamentos particulares à rede de computadores da C&M Software sem a formal autorização do Departamento de Suporte e da Diretoria da C&M Software.

7. SISTEMAS INFORMATIZADOS E EQUIPAMENTOS

7.1. Os recursos de tecnologia, “softwares” e “hardwares”, utilizados pela C&M Software, devem estar devidamente autorizados, homologados e/ou serem de propriedade da C&M Software, mesmo que em regime de comodato.

7.2. Os responsáveis pela aquisição, locação, desenvolvimento e implantação de recursos tecnológicos devem submeter às soluções tecnológicas a serem implementadas ao Departamento de Suporte para análise dos aspectos de segurança com o objetivo de avaliar os riscos operacionais por elas oferecidos.

7.3. Os contratos devem ser analisados quanto aos riscos às informações da empresa e devem possuir cláusulas de responsabilidade no cumprimento das medidas de segurança e da continuidade dos negócios adotados pela C&M Software.

8. CONECTIVIDADE

8.1. As conexões eletrônicas efetuadas na rede interna e entre redes internas e externas devem se restringir às atividades relacionadas aos negócios da C&M Software.

8.2. As conexões entre as redes devem ser dotadas de mecanismos de segurança que protejam, adequadamente, os ambientes internos envolvidos e as informações neles contidas.

8.3. A transferência e o armazenamento de informação, independente do meio físico ou lógico utilizado, devem sempre estar protegidos de acordo com o estabelecido na classificação da informação.

8.4. As transações eletrônicas devem ser dotadas de mecanismos que garantam a integridade, a confidencialidade e o não repúdio.

9. CONTROLES ESPECÍFICOS DE PSTI

9.1. Criptografia e Proteção Contra Ameaças

- Devem ser implementados mecanismos de criptografia para dados em repouso e em trânsito.
- Serão utilizados sistemas de prevenção e detecção de intrusão, ferramentas de prevenção de vazamento de informações e proteção contra softwares maliciosos. além de SOC externo, para monitoramento e medidas imediatas.
- Implementado via IN-SI-010, IN-SI-17, e IN-SI-018.

9.2. Rastreabilidade de Transações

- Todas as transações deverão possuir trilhas de auditoria fim-a-fim, com geração e retenção de logs que permitam identificar falhas ou comportamentos atípicos.
- As informações terão tempo de retenção definido contratualmente conforme tipo de processamento, com armazenamento seguro e acesso controlado para conciliação e gestão de riscos.
- Implementado via IN-SI-008, IN-SI-009.

9.3. Gestão de Cópias de Segurança

- Serão mantidos planos de backup com rotinas regulares, testes periódicos de restauração e retenção de acordo com os requisitos legais, contratuais e operacionais.
- Implementado via IN-SI-011.

9.4. Avaliação e Correção de Vulnerabilidades

- Testes de vulnerabilidades e varreduras periódicas de rede e sistemas.

- Testes de intrusão regulares, com tratamento e mitigação tempestiva de falhas identificadas.
- Monitoramento para identificar dispositivos não autorizados conectados à rede.
- Implementado via IN-SI-015, IN-SI-016.

9.5. Controle de Acesso
- Acesso restrito apenas a usuários e dispositivos autorizados.
- Revisão periódica de permissões, especialmente para terceiros.
- Autenticação multifator obrigatória para acessos externos e para ambientes críticos (Pix e STR).
- Implementado via IN-SI-003, IN-SI-007.

9.6. Proteção de Rede
- Regras de firewall, monitoramento de conexões e bloqueio de tentativas indevidas de acesso.
- Critérios específicos para acessos fora do horário convencional.
- Monitoramento de eventos atípicos (VPN, acessos privilegiados), com implementação de controles adicionais quando necessário.
- Implementado via IN-SI-017, IN-SI-018.

9.7. Segregação de Ambientes
- Separação física e lógica entre ambientes de desenvolvimento, homologação e produção.
- Ambientes Pix e STR devem permanecer isolados logicamente e fisicamente dos demais sistemas, não serão utilizados recursos de nuvem na solução.
- Implementado via IN-SI-017

9.8. Gestão de Certificados Digitais
- Monitoramento e guarda seguram dos certificados digitais.
- Validação periódica junto às autoridades certificadoras, incluindo checagem de certificados revogados.
- Implementado via IN-SI-002, IN-SI-023

9.9. Integração com Terceiros (APIs e Interfaces Eletrônicas)
- Definição de requisitos técnicos e de segurança específicos para integração.
- Monitoramento comportamental e de performance das operações.
- Implementação de mecanismos de conciliação e detecção de uso indevido, manipulação ou extração de dados.

- As integrações eletrônicas com instituições financeiras deverão atender aos requisitos operacionais e de segurança definidos pela C&M Software, garantindo interoperabilidade, controle de acesso, rastreabilidade e proteção de dados.
- Todo sistema de terceiro conectado à infraestrutura da C&M Software estará sujeito à validação técnica e certificação periódica, conforme definido no item 9.10.
- O resultado das certificações deverá ser reportado à área de Segurança da Informação e armazenado para consulta e auditoria.
- Implementado via IN-SI-004, IN-SI-016, IN-SI-024

9.10. Certificação Técnica de Soluções e Interfaces Eletrônicas

- Os sistemas computacionais utilizados por meio de interfaces eletrônicas (APIs, web services, canais de mensageria ou similares), deverão ser submetidos a certificação técnica periódica, que comprove sua conformidade com os requisitos operacionais e de segurança estabelecidos pela C&M Software.
- Essa certificação abrangerá, no mínimo:
    a) Testes periódicos de segurança (vulnerabilidade, penetração, stress e fuzzing de interfaces);
    b) Testes operacionais de desempenho, disponibilidade e aderência a especificações técnicas;
    c) Testes de integração entre os sistemas e os serviços providos pelo PSTI;
    d) Análise de conformidade criptográfica, de autenticação e rastreabilidade das mensagens;
    e) Emissão de relatório de conformidade técnica ou plano de ação corretiva com prazos e responsáveis.
- Os testes e a certificação deverão ocorrer no mínimo uma vez por ano ou sempre que houver alterações relevantes nas integrações, nos serviços providos ou nos requisitos regulatórios aplicáveis.
- A manutenção das evidências dos testes, relatórios e planos de ação é obrigatória por período mínimo de 5 anos, podendo ser auditada por auditores independentes.
- Implementado via IN-SI-016.

9.11. Inteligência Cibernética

- Monitoramento ativo de informações de interesse (clientes, chaves, credenciais, vulnerabilidades) em fontes abertas, Deep e Dark Web, bem como em grupos privados de comunicação, para antecipação e mitigação de riscos.
- Implementado via IN-SI-009, IN-SI-008, IN-SI-025

9.12. Continuidade de Negócios

- Os ambientes operacionais tecnológicos, centralizados ou distribuídos, cuja parada de operação implicar em riscos de perdas financeiras, riscos legais ou de imagem da C&M Software, devem ter seus planos de contingência formalizados, revistos e testados periodicamente, permitindo o pronto reestabelecimento das operações.
- Implementado via PCN001, PO01

9.13. Gestão de Certificação Técnica e Evidências de Conformidade

- A C&M Software manterá um processo documentado para a definição, execução, registro e revisão dos testes técnicos destinados à certificação das soluções integradas aos serviços providos.
- Esse processo incluirá:
- Definição dos escopos de teste e critérios de conformidade;
- Periodicidade mínima e gatilhos de revalidação;
- Responsáveis internos e externos pela execução e aprovação dos testes;
- Armazenamento seguro dos resultados e evidências.
- A área de Segurança da Informação será responsável por coordenar, revisar e aprovar os laudos técnicos antes da certificação final.
- Implementado via processos documentados em todas as IN-SIs.

9.14. Controles Internos e Conformidade

- A C&M Software mantém políticas abrangentes de controles internos e conformidade, aplicável a todas as áreas da instituição, incluindo operações, desenvolvimento, segurança da informação, suporte, compliance, jurídico e áreas de negócio.
- Os controles internos são desenhados para cobrir todos os riscos relevantes do negócio, incluindo riscos operacionais, de segurança da informação e cibernética, continuidade de negócios, fraudes, compliance regulatório.
- Os controles internos são implementados e operacionalizados por meio das instruções normativas e planos específicos, tais como IN-SI-011, IN-SI-015, IN-SI-016, IN-SI-017, IN-SI-022, IN-SI-023, IN-SI-024, IN-SI-025, PCN001, entre outros, que definem procedimentos, responsabilidades, registros e evidências.
- A política de controles internos e conformidade é revisada, no mínimo, anualmente, ou sempre que houver alterações relevantes no perfil de risco, na estrutura da C&M Software ou na regulamentação aplicável.
- Os controles internos e as medidas de contingência são testados e revisados periodicamente, em linha com o disposto no PCN001 (Plano de Continuidade de Negócios) e nas instruções normativas técnicas, garantindo a efetividade dos mecanismos de prevenção, detecção, resposta e recuperação.

- A C&M Software manterá mecanismo formal de revisão e adequação contínua aos dispositivos desta Resolução BCB nº 498 e a todos os requisitos técnicos da RSFN, incluindo o Catálogo de Serviços do SFN, o Manual de Redes do SFN e o Manual de Segurança do SFN, por meio de:
  – análise de impacto regulatório e técnico sempre que houver atualização normativa ou de manuais;
  – atualização de configurações, integrações e sistemas envolvidos;
  – registro e guarda de evidências das adequações realizadas (relatórios, atas, planos de ação, testes).

10. RESPONSABILIDADES

10.1. De forma geral, cabe a todos os Colaboradores e prestadores de serviços:

10.1.1. Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da C&M Software;

10.1.2. Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela C&M Software;

10.1.3. Assegurar que os recursos tecnológicos, as informações e sistemas a sua disposição sejam utilizados apenas para as finalidades aprovadas pela C&M Software;

10.1.4. Cumprir as leis e as normas que regulamentam a propriedade intelectual;

10.1.5. Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.) incluindo a emissão de comentários e opiniões em blogs e redes sociais;

10.1.6. Não compartilhar informações confidenciais de qualquer tipo.

10.2. Cabe ao Departamento de Suporte:

10.2.1. Prover todas as informações de gestão de Segurança da Informação solicitadas pelas Diretorias;

10.2.2. Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os Colaboradores e prestadores de serviços;

10.2.3. Promover ações de conscientização sobre Segurança da Informação para os Colaboradores e prestadores de serviços;

10.2.4. Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da C&M Software;

10.2.5. Estabelecer procedimentos relacionados à instrumentação da segurança da informação da C&M Software.

10.3. Cabe à área de Segurança da Informação e Cibernética:

- Planejar e supervisionar os testes de certificação técnica previstos nesta Política;
- Avaliar e aprovar relatórios de conformidade técnica;
- Garantir que todas as interfaces eletrônicas e sistemas estejam devidamente certificados conforme o item 9.10.

11. VIOLAÇÕES E PENALIDADES

11.1. Os Departamentos e as Unidades competentes reportarão às Diretorias Administrativa e Operações da C&M Software os casos e as evidências de não cumprimento à Política de Segurança da Informação e Cibernética.

11.2. É de responsabilidade dos Departamentos Administrativo e de Suporte zelar pelo cumprimento da Política de Segurança da Informação e Cibernética, executando a devida comunicação das ocorrências recebidas e/ou detectadas.

11.3. Caberá a Diretoria a decisão de aplicar as sanções disciplinares previstas, nas normas internas da C&M Software e na legislação vigente no Brasil.

12. RESPONSABILIDADES GERAIS

12.1. **Diretoria:** Aprovar esta política e fornecer os recursos necessários para sua implementação.

12.2. **Comitê de Segurança de TI (CSTI):** Aprovar as Instruções Normativas; revisar o estado da segurança; decidir sobre incidentes graves.

12.3. **Área de Segurança da Informação:** Coordenar a elaboração, revisão e implementação das políticas; monitorar a eficácia dos controles; liderar a resposta a incidentes.

12.4. **Departamento de Suporte/Operações:** Implementar e executar os controles técnicos definidos nas Instruções Normativas.

12.5. **Todos os Colaboradores e Prestadores de Serviço:** Conhecer e cumprir esta política e as Instruções Normativas aplicáveis às suas funções.

13. REVISÃO E GESTÃO DAS POLÍTICAS

13.1. Esta PSI será revisada anualmente, ou conforme mudanças significativas no ambiente de risco ou regulatório.

13.2. As Instruções Normativas serão revisadas, no mínimo, anualmente, sob coordenação da Área de Segurança da Informação.

13.3. Toda alteração nas Instruções Normativas deve ser comunicada às partes interessadas.

14. VIGÊNCIA

14.1. A presente Política passa a vigorar a partir da data de sua publicação por prazo indeterminado.