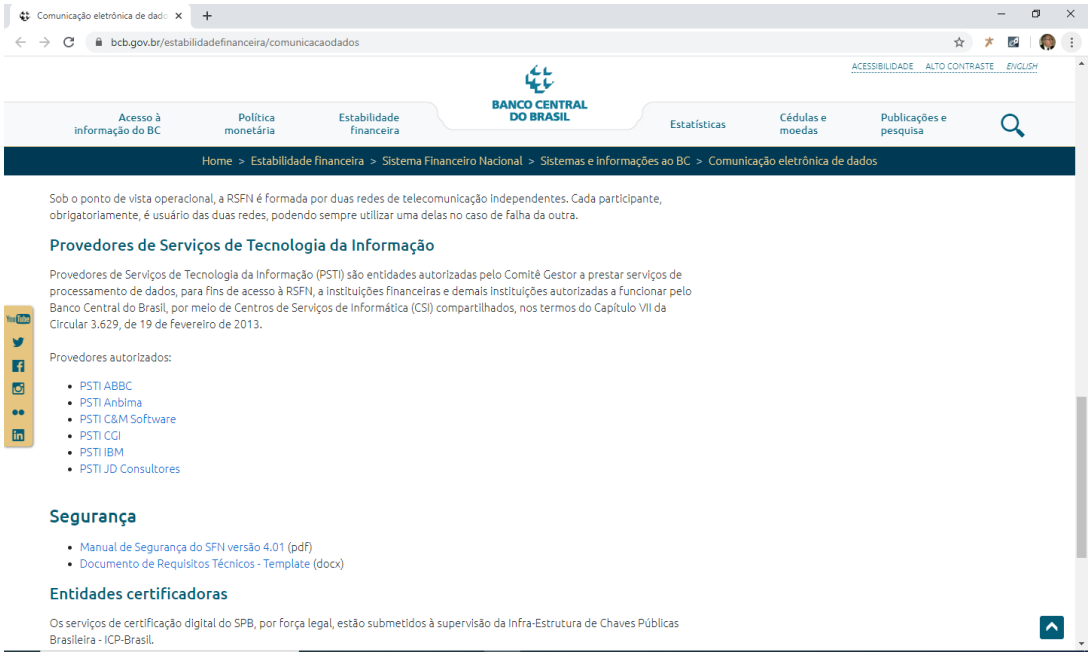
ANEXO XII – POLÍTICA SE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Vigência	Documento
	07/11/2019	CM-PC-002
	Versão	Página
	01	1 / 8

POLÍTICA SE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

A C&M Software é Provedora de Serviços de Tecnologia da Informação (PSTI) homologada pelo Banco Central do Brasil desde 2001, nos termos da Circular n° 3.629, cumprindo rigorosos procedimentos de segurança da informação e cibernética no âmbito da Rede do Sistema Financeiro Nacional (RSFN):

https://www.bcb.gov.br/estabilidadefinanceira/comunicacaodados



Ademais, a C&M Software observa e observará em todos os seus contratos comerciais as disposições contidas na Resolução nº 4.658, de 26/04/2018 e Circular nº 3.909, de 16/08/2018.

Assim, o presente documento, Política de Segurança da Informação e Segurança Cibernética, tem como objetivo atender as normativas do Banco Central do Brasil 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.

ANEXO XII – POLÍTICA SE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA	Vigência	Documento
	07/11/2019	CM-PC-002
	Versão	Página
	01	2 / 8

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.

Lembramos que SPB/x tem sistemática própria de funcionamento (tais como processos específicos de contingência e recuperação, de segurança e integridade, de registro, confirmação e aceitação de operações, etc.), com auditorias realizadas pelo próprio BACEN aos prestadores de tecnologia da informação integrantes do sistema de pagamentos, possuindo normativa específica, estando sob a égide da Circular BACEN n° 3.682/2013, não incidindo as disposições da Resolução 4.658 de 26/04/2018 do BACEN e Circular nº 3.909, de 16/08/2018.

1. CONCEITOS E DEFINIÇÕES:

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.

1.11. **Dado Pessoal Sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

1.12. **Controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

1.13. **Operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

1.14. **Encarregado**: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

1.15. **Tratamento**: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

1.16. **Consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

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.

3. ABRANGÊNCIA

3.1. Esta Política aplica-se a todos os Colaboradores e Prestadores de Serviços 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.

5. SEGURANÇA DA INFORMAÇÃO

5.1. Toda informação deve ter um proprietário identificado (controlador, operador ou encarregado), o qual deve ser o responsável pela utilização desta 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, e/ou segregados quando do interesse da segurança do sistema.

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. CONTINUIDADE DOS NEGÓCIOS

9.1. 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.

9.2. Cópias de segurança das informações vitais devem estar armazenadas em local seguro e de adequada distância física devendo-se também ser realizados testes periódicos com o conteúdo das mídias de *backup*, visando garantir a sua recuperação em caso de indisponibilidade do ambiente original.

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.

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. VIGÊNCIA

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