# POLÍTICA DE CIBERSEGURANÇA

## *CYBERSECURITY POLICY*

### 1. DIRETRIZES

**5.1 DECLARAÇÃO DE INTENÇÃO DA DIREÇÃO**

O *China Construction Bank,* aqui referenciado pelo acrônimo CCB BRASIL, está comprometido em assegurar a disponibilidade, a integridade e a confidencialidade das informações que lhe foram confiadas pelas partes interessadas, incluindo direção, empregados, investidores e outros parceiros de negócios.

O CCB BRASIL é responsável pela definição, aplicação e suporte às Políticas e Normas envolvendo a segurança da informação e seus ativos. No entanto, a responsabilidade pela manutenção e pelo suporte da segurança está implícita nas funções e nas tarefas diárias de todos os empregados, terceiros e prestadores de serviços.

A alta direção do CCB Brasil determina que todos os seus colaboradores atuem no sentido de impedir a ocorrência de problemas de segurança com as informações sob sua posse ou responsabilidade e contribuam para resultados de qualidade nos negócios através do respeito e cumprimento da sua Política de Segurança da Informação;

**5.2 ORGANIZAÇÃO E GESTÃO**

Deverá ser instituído um Comitê para tratar de assuntos relativos à Segurança da Informação dentro do CCB Brasil. O Comitê de Segurança da Informação, aqui referenciado pelo acrônimo CSI, é responsável pelo ciclo de vida das Políticas e Normas de Segurança da Informação, promovendo a sua criação, aprovação, disseminação e revisão, de acordo com as necessidades do negócio ao

### 1. GUIDELINES

**5.1 DECLARATION OF INTENTION OF THE BOARD**

China Construction Bank, here referenced by the acronym of CCB Brasil, is compromised in assure availability, integrity and confidentiality of information entrusted to it by the stakeholders, including the board, employees, investors and other business partners.

CCB Brasil is responsible by definition, application and support to Policies and Standards related to security of information and its assets. However, the responsibility for maintenance and support of security is implicit in the functions and daily tasks of all employees, third part and service providers.

The board of CCB Brasil determines that all employees act to avoid the occurrence of security problems with information under its ownership or responsibility and contribute to quality results in business through respect and enforcement of its Information Security Policy.

**5.2 ORGANIZATION AND MANAGEMENT**

It must be instituted a committee to deal subjects related to Information Security in CCB Brasil. The Information Security Committee is responsible for the lifecycle of Policies and Standards of Information Security, promoting its creation, approval, publish and reviews, in accordance with the needs of the business along its respective lifecycle. This committee must be governed by specific policy and procedures.

longo de seu respectivo ciclo de vida. Este Comitê deverá ser regido por política e procedimentos específicos.

Este Comitê reportará ao Comitê de Governança Corporativa as ações e problemas detectados que envolvem a segurança das informações do CCB Brasil.

As áreas de negócio e técnicas são responsáveis pelo desenvolvimento e implantação de procedimentos detalhados, bem como pelo monitoramento da conformidade com essas Políticas e Normas. A área de Segurança da Informação deverá oferecer supervisão ao negócio através da medição da conformidade.

O departamento de Recursos Humanos (ou a gerência responsável, quando se referir a prestadores de serviços) deverão promover a ação disciplinar adequada em resposta à transgressão das Políticas e Normas, ou má-conduta grave.

**5.3 TREINAMENTO E CONSCIENTIZAÇÃO**

O CCB Brasil deverá assegurar que os usuários estejam cientes das ameaças e das preocupações que possam afetar negativamente a segurança das informações e que sejam orientados para apoiar esta política, por meio de um programa de disseminação da cultura de segurança;

A área de Segurança da Informação deverá providenciar treinamento e conscientização geral de segurança da Informação para os funcionários assim como coordenar e determinar, de acordo com a necessidade, as áreas e o conteúdo do treinamento de segurança e conscientização.

**5.4 COORDENAÇÃO ENTRE ORGANIZAÇÕES**

Deverão ser estabelecidos e mantidos contatos com as autoridades de segurança pública, órgãos reguladores e grupos de segurança, para prestação de contas e compartilhamento de conhecimento e assistência com incidentes de segurança, conforme apropriado.

**5.5 OBRIGAÇÕES DE SEGURANÇA DA INFORMAÇÃO**

**5.5.1 RESPONSABILIDADES DO USUÁRIO**

This committee will report to the Governance Committee its actions and detected problems that involves the security of information of CCB Brasil.

The business and technical areas are responsible for the development and implementation of detailed procedures, as well as for monitoring compliance with these Policies and Standards. The Information Security area should provide business oversight by measuring compliance.

The Human Resources department (or responsible management, when referring to service providers) should promote appropriate disciplinary action in response to Violation of Policies and Norms, or serious misconduct.

**5.3 TRAINING AND AWARENESS**

CCB Brasil should ensure that users are aware of the threats and concerns that may adversely affect information security and are directed to support this policy through a security culture dissemination program.

The Information Security area should provide general information security training and awareness to employees as well as coordinate and determine, as needed, the areas and content of security training and awareness.

**5.4 COORDINATION BETWEEN ORGANIZATIONS**

Contacts should be established and maintained with public security authorities, regulators and security groups, for accountability and sharing of knowledge and assistance with security incidents, as appropriate.

**5.5 OBLIGATIONS OF INFORMATION SECURITY**

**1.5.1 RESPONSIBILITY OF USERS**

Todo o profissional do CCB BRASIL, prestador de serviços ou fornecedores contratados tem responsabilidade pela Segurança, devendo entender as suas funções e responsabilidades na minimização dos riscos de segurança, comunicando ou escalonando esses riscos, e implementando as medidas de proteção, de forma coerente com as Políticas e Normas de Segurança da Informação do CCB BRASIL.

**5.5.2 OBRIGAÇÕES RELACIONADAS A SEGURANÇA DA INFORMAÇÃO**

É de propriedade do CCB Brasil toda a informação gerada ou tramitada por meio dos seus recursos ou de recursos por ele autorizados;

Todas as informações do CCB Brasil devem ser protegidas contra a modificação, destruição e acesso por pessoas não autorizadas;

As informações do CCB Brasil devem ser utilizadas por seus colaboradores somente para fins profissionais;

O acesso à informação somente deve ser feito através de recursos devidamente autorizados pelo CCB Brasil;

Todas as informações do CCB Brasil deverão ter um gestor que fará sua classificação, de acordo com Política específica;

As informações do CCB Brasil deverão ser armazenadas por tempo determinado pela empresa ou por legislação vigente;

Devem ser tomadas as medidas necessárias para investigar prontamente qualquer possível causa de problemas de segurança ou incidentes de segurança, bem como minimizar os seus danos.

A Área de Segurança da Informação é responsável pela Gestão de Segurança da Informação dentro do CCB Brasil;

**5.5.3 RESPONSABILIDADES DE ACESSO**

CCB BRASIL professionals, contracted service provider or contractor has responsibility for the Security, and must understand its functions and responsibilities in the minimization of security risks, communicating or staggering these risks, and implementing the protection measures, in a manner consistent with the CCB BRASIL Information Security Policies and Standards.

**5.5.2 OBLIGATIONS RELATED TO INFORMATION SECURITY**

É de propriedade do CCB Brasil toda a informação gerada ou tramitada por meio dos seus recursos ou de recursos por ele autorizados;

All information of CCB Brasil must be protected against modification, destruction and access by unauthorized persons;

CCB Brasil information should be used by its employees only for professional purposes;

Access to information should only be done through resources duly authorized by CCB Brasil;

All information of the CCB Brazil must have a manager who will make its classification, according to specific Policy;

CCB Brasil information must be stored for a period of time determined by the company or by current legislation;

The necessary steps should be taken to promptly investigate any possible cause of security problems or safety incidents, as well as to minimize their damage.

The Information Security Area is responsible for Information Security Management within the CCB Brasil;

**5.5.3 ACCESS RESPONSIBILITIES**

Todos os usuários dos sistemas, redes e aplicativos do CCB BRASIL e informações ali contidas, deverão defender e proteger as suas respectivas contas de usuário e senhas.

All users of the systems, networks and applications of CCB BRASIL and information contained therein shall defend and protect their respective user accounts and passwords.

**5.5.4 ESTAÇÃO DE TRABALHO SEM MONITORAÇÃO**

Os computadores deverão solicitar a autenticação do logon no início da sessão e ficar protegidos por um bloqueio de tela (por exemplo: proteção de tela com senha, *Logoff* automático, etc.) ou encerramento automático quando ociosos ou não sendo usados.

**5.5.4 WORKSTATIONS WITHOUT MONITORING**

Computers must request login authentication at the beginning of the session and be protected by a screen lock (for example: screen saver with password, automatic logoff, etc.) or automatic shutdown when idle or not being used.

**5.5.5 CONSCIENTIZAÇÃO DO USUÁRIO**

Todos os funcionários, terceiros e fornecedores deverão participar e/ou apoiar o treinamento de segurança e requisitos de conscientização do CCB BRASIL.

**5.5.5 USERS AWARENESS**

All employees, third parties and suppliers shall participate and support the security training and awareness of CCB Brasil.

**5.5.6 USO ACEITÁVEL DOS ATIVOS**

Os sistemas, redes, correio eletrônico, telefones e a conexão com a Internet do CCB BRASIL são fornecidos para utilização durante as atividades profissionais. Todo funcionário, terceiros ou fornecedores devem cumprir com as normas de uso aceitável. A utilização dos sistemas de informação, redes, correio eletrônico, telefones e demais sistemas de mensagens do CCB BRASIL estará sujeita ao monitoramento pela Segurança da Informação, de forma a assegurar o cumprimento das Políticas e Normas estabelecidas neste documento, de acordo com legislação ou regulamentos aplicáveis.

**5.5.6 ACCEPTABLE USE OF ASSETS**

CCB Brasil systems, networks, e-mail, telephones and Internet connection are provided for use during professional activities. All employees, third parties or suppliers must comply with the rules of acceptable use. The use of CCB Brasil's information systems, networks, electronic mail, telephones and other messaging systems shall be subject to monitoring by Information Security in order to ensure compliance with the Policies and Standards established in this document, in accordance with legislation or regulations applicable.

**5.5.7 USO ACEITÁVEL DOS SISTEMAS DE INFORMAÇÃO**

Todos os usuários dos sistemas de informação são obrigados a utilizar os sistemas de maneira legalmente responsável. O CCB BRASIL possui medidas de segurança projetadas para proteger os seus sistemas de informação sendo de responsabilidade dos usuários a adesão a tais medidas.

Nos computadores e redes do CCB BRASIL, somente deverão ser instalados software e hardware licenciados e aprovados pelo time de Segurança da Informação. Para a devida aprovação, todo e qualquer software e hardware

**5.5.7 ACCEPTABLE USE OF INFORMATION SYSTEMS**

All users of information systems are required to use the systems in a legally responsible manner. CCB Brasil has security measures designed to protect its information systems and it is the responsibility of the users to comply with such measures.

In the computers and networks of CCB Brasil, only software and hardware licensed and approved by the Information Security team must be installed. For proper approval, all software and hardware must be evaluated

deverá ser avaliado quanto aos aspectos comerciais, legais e de TI, além de requisitos de segurança e serem avaliados quanto ao risco. Tais análise e avaliações de risco deverão ser documentadas.

for business, legal and IT aspects, as well as security requirements and be evaluated for risk. Such risk analysis and assessments should be documented.

Todo software e hardware aprovados deverão ser incluídos ao Inventário de Ativos do CCB BRASIL. Nenhuma informação do CCB BRASIL pode ser armazenada ou processada em sistemas não aprovados, a menos que estejam classificadas como público ou devidamente aprovado, de acordo com política específica.

All approved software and hardware shall be included in the Asset Inventory of CCB Brasil. No information from CCB Brasil may be stored or processed on non-approved systems, unless they are classified as public or properly approved, in accordance with specific policy.

**5.5.8 DIREITO DE BUSCA E MONITORAMENTO**

O CCB BRASIL reserva-se o direito de monitorar, inspecionar e pesquisar constantemente os seus sistemas de informação, com o objetivo de reafirmar o cumprimento das suas políticas internas, bem como a legislação e regulamentos aplicáveis, e igualmente o monitoramento de segurança do empregado, também sujeito às leis e regulamentos locais.

**5.5.8 SEARCH AND MONITORING RIGHT**

CCB Brasil reserves the right to monitor, inspect and constantly research its information systems, in order to reaffirm compliance with its internal policies, as well as applicable legislation and regulations and equally the right to security monitor employees, also subject to local laws and regulations.

**5.6 CLASSIFICAÇÃO DE ATIVOS**

Toda informação do CCB BRASIL deve ter um responsável principal para:

- Classificar e rotular qualquer informação que ele tenha criado ou sob a sua responsabilidade.
- Reclassificar a informação quando houver mudança de valor ou risco inerente.
- Divulgar a informação apenas conforme a necessidade.
- Aderir aos termos do contrato com o fornecedor quando estiver de posse da informação.
- Prover assistência e assegurar que exista um plano de contingência adequado.
- Autorizar o acesso do usuário apenas conforme a necessidade específica.
- Decidir sobre os usos adequado da informação.
- Assegurar a precisão dos dados, através da implantação de controles suficientes para fornecer o alto nível de integridade dos dados (ou seja, validação de dados).

**5.6. ASSET CLASSIFICATION**

All information of CCB Brasil must have a responsible for:

- Classify and label any information created or under his responsibility.
- Reclassify information when there is a change in value or inherent risk.
- Disseminate information only as needed.
- Adhere to the terms of the contract with the supplier when in possession of the information.
- Provide assistance and ensure that there is an adequate contingency plan.
- Authorize access to users only according to the specific need.
- Decide on the appropriate uses of information.
- Ensure data accuracy by implementing sufficient controls to provide the high level of data integrity (ie, data validation).

- Estabelecer os controles adequados de segurança da informação.

**5.7 GESTÃO DE RISCOS**

O CCB BRASIL possui processo de gestão de riscos de segurança, de acordo com a política interna de Gestão de Riscos, visando mitigar os riscos identificados nos processos considerados críticos da empresa.

**5.8 GERENCIAMENTO DE VULNERABILIDADES**

O CCB BRASIL realiza análises de vulnerabilidades nos ativos e sistemas de processamento do CCB BRASIL, conforme política interna de Gestão de Vulnerabilidade, considerando os seguintes itens:

- Sistemas/aplicações de segurança
- Sistemas/aplicações de produção e teste
- Computador de mesa e demais sistemas/aplicações dedicados ao usuário
- Ambiente de rede

**5.9 INVENTÁRIO DE ATIVOS**

O CCB BRASIL mantém inventário atualizado dos ativos de informação do CCB BRASIL contendo recursos de hardware, software, aplicações de negócio, equipamentos de rede, recursos humanos, instalações físicas e itens relevantes para o CCB BRASIL como terceiros e fornecedores.

**5.10 TRANFERÊNCIA DAS INFORMAÇÕES**

A transferência eletrônica ou física de informações entre o CCB BRASIL e terceiros deverá ser controlada de maneira planejada para assegurar a sua proteção e armazenamento adequado. Essas empresas, por receberem a informação do CCB BRASIL deverão demonstrar que dispõem de políticas e práticas planejadas para assegurar a disponibilidade, integridade, confidencialidade e capacidade de recuperação dos ativos de informação, de forma a atender ou exceder as políticas e práticas internas do CCB BRASIL.

- Establish appropriate information security controls.

**5.7 RISK MANAGEMENT**

CCB Brasil has a process of management of security risks, in accordance with the internal policy of Risk Management, aiming to mitigate the risks identified in the processes considered critical of the company.

**5.8 VULNERABILITY MANAGEMENT**

CCB Brasil performs vulnerability analysis on its assets and processing systems, according to the internal policy of Vulnerability Management, considering the following items:

- Security systems and applications
- Production and test systems and applications
- Desktop computer and other systems and applications dedicated to the users
- Network environment

**5.9 ASSET INVENTORY**

CCB Brasil maintains updated inventory of CCB Brasil information assets containing hardware, software, business applications, network equipment, human resources, physical facilities and items relevant to CCB Brasil as third parties and suppliers.

**5.10 INFORMATION TRANSFER**

The electronic or physical transfer of information between CCB Brasil and third parties must be controlled in a planned manner to ensure its adequate protection and storage. These companies, because they receive the information from CCB Brasil, must demonstrate that they have policies and practices designed to ensure the availability, integrity, confidentiality and resilience of information assets, in order to meet or exceed the internal policies and practices of CCB Brasil.

**5.11 SEGURANÇA FÍSICA**

Os requisitos de segurança física deverão ser definidos com base na tolerância para o nível de risco identificado através da avaliação de risco das instalações, além de um padrão razoável de cuidado. As políticas e procedimentos deverão delinear as etapas necessárias para preservar a integridade e segurança das instalações do CCB BRASIL, mantendo o nível máximo de segurança.

**5.12 DESCARTE DE EQUIPAMENTOS E DESTRUÇÃO DE INFORMAÇÕES**

Toda mídia deverá ser descartada quando se tornar desnecessária. A mídia não deverá ser reutilizada, doada para caridade ou descartada sem a devida autorização da área Tecnologia da Informação. Para minimizar o risco de divulgação acidental de informação sigilosa, a área Tecnologia da Informação deverá garantir a execução de uma forma segura de descarte (ou seja, incineração, fragmentação ou limpeza completa), destruindo completamente e de maneira irreversível toda e qualquer informação do CCB BRASIL. O descarte seguro deverá ser feito de acordo com as diretrizes de classificação da informação.

A reutilização, venda ou doação assistencial de computador fora de uso, poderá ocorrer, se não houver qualquer risco de exposição de dados sigilosos, ou danos organizacionais potenciais à informação previamente abrigada nesses sistemas.

**5.13 GERENCIAMENTO DE MÍDIA REMOVÍVEL**

Todas as mídias removíveis deverão ser utilizadas de maneira condizente com os critérios estabelecidos pela classificação da informação. O proprietário pela informação deverá assegurar que a mídia seja armazenada em ambiente fisicamente protegido.

Deverão ser providenciadas fragmentadoras e recipientes para o descarte da mídia físicas confidencial, nas áreas da empresa, onde necessário.

**5.14 CONTROLE DE ACESSO FÍSICO**

**5.11 PHYSICAL SECURITY**

Physical security requirements should be defined based on the tolerance for the level of risk identified through the risk assessment of the facility as well as a reasonable standard of care. The policies and procedures shall outline the steps necessary to preserve the integrity and security of CCB Brasil facilities, maintaining the maximum level of safety.

**5.12 DISCARD OF EQUIPMENT AND INFORMATION WIPE**

All media should be discarded when it becomes unnecessary. The media should not be reused, donated to charity or discarded without the proper authorization of the Information Technology area. In order to minimize the risk of accidental disclosure of sensitive information, the Information Technology area should guarantee the execution of a safe way of disposal (ie, incineration, fragmentation or complete cleaning), destroying completely and irreversibly any and all information of the CCB Brasil. Safe disposal should be done in accordance with the classification guidelines.

The reuse, sale, or donation of end-of-use computer may occur if there is no risk of exposure to sensitive data or potential organizational damage to previously held information in such systems

**5.13 REMOVABLE MEDIA MANAGEMENT**

All removable media should be used in a consistently manner with the criteria established by the classification of the information. The owner of the information shall ensure that the media is stored in a physically protected environment.

Shredders and containers for the disposal of confidential physical media should be provided in the areas of the company, where necessary.

**5.14 PHYSICAL ACCESS CONTROL**

O CCB BRASIL projeta áreas para serem fisicamente protegidas contra o acesso de pessoas não autorizadas. A proteção física incluir o uso de controles de segurança manuais e tecnológicos, delimitando o acesso às áreas controladas. As áreas controladas são ser monitoradas ininterruptamente, através de controles de segurança manuais e tecnológicos.

O acesso às áreas internas deverá ser limitado apenas ao pessoal autorizado, de acordo com a necessidades.

**5.15 GERENCIAMENTO NAS COMUNICAÇÕES E OPERAÇÕES**

**5.15.1 DOCUMENTAÇÃO DOS PROCEDIMENTOS OPERACIONAIS**

Os processos e procedimentos para administrar e executar as operações de segurança e controle do CCB BRASIL deverão ser documentados e mantidos para promover a coerência com o ambiente operacional da empresa.

**5.15.2 GERENCIAMENTO DE MUDANÇAS**

Modificações e aperfeiçoamentos dos sistemas de informação do CCB BRASIL deverão ser administrados através do processo controlado de gerenciamento de mudanças.

**5.16 MONITORAMENTO E REGISTRO (LOG) DOS SISTEMAS**

O CCB BRASIL possui processo para monitorar e capturar informações, relacionadas à interação entre os usuários e ativos de informação. Os eventos específicos são registrados para identificar os incidentes de segurança, estabelecer as responsabilidades individuais e a própria reconstrução do evento.

**5.17 MONITORAMENTO DE USO DOS SISTEMAS**

O CCB BRASIL possui procedimentos para o monitoramento de eventos de log conhecidos como atividades suspeitas ou exceções ao comportamento normal.

CCB Brasil designs areas to be physically protected from unauthorized access. Physical protection includes the use of manual and technological security controls, delimiting access to controlled areas. Controlled areas are monitored uninterruptedly through manual and technological safety controls.

Access to internal areas should be limited to authorized personnel only, as required.

**5.15 COMMUNICATION AND OPERATIONAL MANAGEMENT**

**5.15.1 OPERATIONAL PROCEDURES DOCUMENTATION**

The processes and procedures for administering and executing security and control operations of CCB Brasil should be documented and maintained to promote consistency with the company's operating environment.

**5.15.2 CHANGE MANAGEMENT**

Modifications and improvements to the CCB BRASIL information systems should be managed

**5.16 MONITORING AND RECORD (LOG) OF SYSTEMS**

CCB Brasil has process to monitor and capture information related to the interaction between users and information assets. Specific events are logged to identify security incidents, establish individual responsibilities, and rebuild the event itself.

**5.17 MONITORING OF THE USE OF SYSTEMS**

CCB Brasil has procedures for monitoring log events known as suspicious activities or exceptions to normal behavior.

**5.18 PROTEÇÃO DE INTRUSO E GERENCIAMENTO DE INCIDENTES**

As responsabilidades e procedimentos estabelecidos de acordo com política interna de Gestão de Incidentes deverá ser projetada para evitar, detectar, atuar e resolver os incidentes que possam afetar a confidencialidade, disponibilidade ou integridade dos sistemas, informações ou processos de negócio do CCB BRASIL. Como parte do processo de resolução, a análise do incidente deverá auxiliar a estabelecer as medidas preventivas, ou como suporte a uma eventual ação legal.

**5.19 PROCESSO DE RESPOSTA A INCIDENTES**

Processos e procedimentos deverão ser estabelecidos para responder às violações de segurança, eventos e incidentes anormais ou suspeitos, com o objetivo de minimizar o dano aos ativos de informação e permitir a identificação e punição de seus autores, em acordo com a política de Gestão de Incidentes.

**5.20 SOFTWARE DE ANTIVÍRUS E CÓDIGO MALICIOSO**

Os controles de detecção e prevenção, projetados para proteger o CCB BRASIL contra software de código malicioso e vírus, deverão ser instalados em todos os ativos relacionados à informação da empresa.

O CCB BRASIL deverá estar em conformidade com os acordos de licença de software, sendo proibida a aquisição e o uso de software não autorizado. O software antivírus deverá ser instalado e configurado em todos os computadores, PCs, laptops e demais dispositivos móveis relacionados, além de servidores de rede, correio eletrônico, e servidores de Internet para varredura de arquivos infectados, novos e antigos.

**5.21 IDENTIFICAÇÃO E COMUNICAÇÃO**

O CCB Brasil deverá assegurar que um canal de comunicação seja estabelecido, com atendimento em tempo integral, eficiente e autônomo para atender e orientar nos casos de incidentes que possam colocar em risco a segurança das informações do CCB Brasil, bem

**5.18 INTRUDER PROTECTION AND INCIDENT MANAGEMENT**

Responsibilities and procedures established in accordance with internal Incident Management policy should be designed to avoid, detect, act and resolve incidents that may affect the confidentiality, availability or integrity of systems, information or business processes of CCB Brasil. As part of the resolution process, the analysis of the incident should assist in establishing preventive measures, or in support for possible legal action.

**5.19 INCIDENT RESPONSE PROCESS**

Processes and procedures should be established to respond to security breaches, abnormal or suspicious events and incidents, in order to minimize the damage to information assets and allow the identification and punishment of their perpetrators, in accordance with the Incident Management policy.

**5.20 ANTIVIRUS AND ANTI MALWARE SOFTWARES**

Detection and prevention controls, designed to protect CCB Brasil against software malicious code and viruses, should be installed in all assets related to company information.

CCB Brasil shall comply with the software license agreements, and the acquisition and use of unauthorized software is prohibited. Antivirus software should be installed and configured on all computers, PCs, laptops and other related mobile devices, as well as network servers, e-mail, and Internet servers for scanning for infected files, new and old.

**5.21 IDENTIFICATION AND COMUNICATION**

CCB Brasil shall ensure that a communication channel is established with full-time, efficient and autonomous assistance to assist and guide in the event of incidents that may put at risk the security of information of CCB Brasil, as well as its assets. Any security incident should be reported through this channel.

como seu patrimônio. Todo incidente de segurança deverá ser comunicado através desse canal.

**5.22 SEGREGAÇÃO DE FUNÇÕES**

As funções e responsabilidades incompatíveis deverão ser separadas, para minimizar a possibilidade de acesso ou uso indevido e não autorizado de informação da empresa, ativos relacionados à informação, ou processos comerciais.

**5.23 SEGREGAÇÃO DE AMBIENTES**

Os ambientes de desenvolvimento, testes e produção deverão ser segregados para minimizara possibilidade de modificações não autorizadas ao ambiente de produção.

**5.24 PLANEJAMENTO DE CAPACIDADE**

Os ativos relacionados à informação do CCB BRASIL deverão contar com a capacidade e recursos adequados, disponibilizados para atender às demandas das operações de seus negócios.

**5.25 BACKUP E RETENÇÃO**

O CCB BRASIL deverá garantir periodicamente backups dos ativos de informação, para propósitos de recuperação operacional, assim como estar em conformidade com os planos de recuperação da continuidade dos negócios, e que tais backups sejam retidos, de acordo com os requisitos de negócios e regulatórios.

**5.26 CONTROLES CRIPTOGRAFICOS**

O CCB deverá utilizar controles criptográficos e um sistema de gerenciamento de chaves associado sempre que o grau de sensibilidade da informação, baseada na sua classificação definida, for considerado necessário.

**5.27 SEGURANÇA DA REDE**

O CCB BRASIL deverá providenciar os recursos de segurança de rede, de acordo com o grau mais adequado para a natureza dos dados sendo transmitidos.

**5.22 SEGREGATION OF DUTIES**

Incompatible roles and responsibilities should be segregated to minimize the possibility of unauthorized access or use of company information, information-related assets, or business processes.

**5.23 SEGREGATION OF ENVIRONMENTS**

Development, testing, and production environments should be segregated to minimize the possibility of unauthorized modifications to the production environment.

**5.24 CAPACITY PLANNING**

The information-related assets of CCB Brasil must have the adequate capacity and resources available to meet the demands of its business operations.

**5.25 BACKUP AND RETENTION**

CCB Brasil shall periodically guarantee backups of information assets for operational recovery purposes, as well as comply with business continuity recovery plans, and that such backups are retained in accordance with business and regulatory requirements.

**5.26 CRYPTOGRAPHIC CONTROLS**

The CCB shall use cryptographic controls and an associated key management system whenever the degree of sensitivity of the information, based on its defined classification, is deemed necessary.

**5.27 SECURITY OF THE NETWORK**

CCB Brasil shall provide the network security features according to the most appropriate degree for the nature of the data being transmitted.

**5.28 USE OF ACCESS PASSWORDS**

CCB Brasil is responsible for ensuring that all passwords of standard network equipment are changed at the time

**5.28 USO DE SENHAS DE ACESSO**

O CCB BRASIL está encarregado de assegurar que todas as senhas padrão de equipamento de rede sejam substituídas no momento da instalação, assim como prover um sistema adequado para gerenciamento de senhas de acesso e de sistemas respeitando os requisitos de complexidade, tamanho mínimo e histórico de senhas.

**5.29 ACESSO AOS SISTEMAS**

Deve ser usado um processo formal para administrar os privilégios de acesso durante o ciclo de vida, desde o registro até a revogação.

**5.30 SISTEMA DE GERENCIAMENTO DE SENHAS**

Aplicativos ou qualquer outro recurso do CCB BRASIL, que hospede ou forneça acesso aos dados, deverão estar alinhadas as normas aplicáveis de gerenciamento de senha.

**5.31 ACESSO REMOTO**

Todos os usuários, inclusive terceiros, com acesso remoto aos sistemas do CCB BRASIL, são responsáveis pela segurança da conexão a todos os sistemas e recursos de informação da empresa.

**5.32 AMBIENTE EM NUVEM**

Em alinhamento a estratégia e diretrizes da organização, o CCB Brasil não utiliza serviços em nuvem. Entretanto, fornecedores que prestam serviços diretos ou indiretos podem utilizar ambiente em nuvem para prestação de serviços, dessa forma eles deverão ser estabelecidos conforme as diretrizes de segurança da informação para garantir a disponibilidade, confidencialidade e integridade das informações do CCB BRASIL quando estiverem armazenadas, disponibilizadas e acessíveis em ambiente Cloud (Nuvem).

**5.33 DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS**

Garantir que a criação de novos produtos, a seleção de mecanismos de segurança e a aquisição de bens ou

of installation, as well as providing a suitable system for managing access and system passwords in compliance with the requirements of complexity, minimum size and password history.

**5.29 ACCESS TO SYSTEMS**

A formal process should be used to administer access privileges throughout the lifecycle, from registration to revocation.

**5.30 PASSWORD MANAGEMENT SYSTEM**

Applications or any other resources of CCB Brasil, which hosts or provides access to the data, should be in line with applicable password management standards.

**5.31 REMOTE ACCESS**

All users, including third parties, with remote access to the systems of CCB Brasil, are responsible for the security of the connection to all systems and information resources of the company.

**5.32 CLOUD COMPUTING**

In line with the strategy and guidelines of the organization, CCB Brasil does not use cloud services. However, suppliers providing direct or indirect services can use the cloud environment to provide services, so they must be established according to the information security guidelines for guarantee the availability, confidentiality and integrity of CCB BRASIL information when it is stored, made available and accessible in a Cloud environment.

**5.33 DEVELOPMENT AND MAINTENANCE OF SYSTEMS**

Ensure that the creation of new products, the selection of security mechanisms and the acquisition of technology goods or services take into account the balancing of the following aspects: risk, technology, cost, quality, speed and impact on the business;

Security considerations should be included in all phases of the systems development lifecycle, especially to ensure

serviços de tecnologia levem em consideração o balanceamento dos seguintes aspectos: risco, tecnologia, custo, qualidade, velocidade e impacto no negócio;

As considerações de segurança devem ser incluídas em todas fases do ciclo de vida do desenvolvimento dos sistemas, especialmente para assegurar que as políticas de segurança do CCB BRASIL sejam abordadas em tempo hábil e com eficiência de custos.

**5.34 TERCEIRIZAÇÃO E AQUISIÇÃO**

É responsabilidade do CCB Brasil manter a segurança da informação mesmo quando a responsabilidade pelo processo (ou mesmo parte dele) for terceirizada para uma outra entidade, provendo auditorias periódicas, buscando a certificação do cumprimento dos requisitos de segurança da informação;

Os acordos ou contratos de terceirização devem incluir os requisitos do CCB BRASIL para administração de seus ativos de informação, de acordo com as polícias de segurança da informação.

Os requisitos de segurança do CCB BRASIL relativos a partes externas devem ser abordados e documentados em contrato entre as partes. Cláusulas contratuais devem ser estabelecidas, para proteger a segurança da informação mantida ou acessada pelos fornecedores.

**5.35 CONFORMIDADE COM REQUISITOS LEGAIS E CONTRATUAIS**

O CCB Brasil deve garantir o atendimento das leis que regulamentam suas atividades de forma a obter sua aderência;

Garantir que sejam atendidas as normas internas e externas sobre quebra de sigilo de qualquer dado ou informação do CCB Brasil, sob pena de responsabilidade e consequências legais pertinentes.

**5.36 PESSOAL E PROVISÃO DE RECURSOS**

As considerações relativas à segurança que apoiam os requisitos do CCB BRASIL devem ser endereçadas através

that security policies of CCB Brasil are addressed in a timely and cost-effective manner.

**5.34 OUTSOURCING AND ACQUISITION**

It is responsibility of CCB Brasil to maintain information security even when the responsibility for the process (or even part of it) is outsourced to another entity, providing periodic audits, seeking to certify compliance with information security requirements;

The outsourcing agreements or contracts must include the requirements of CCB Brasil for the administration of its information assets, according to the information security police.

Security requirements of CCB Brasil for external parts must be addressed and documented in a contract between the parties. Contractual clauses should be established to protect the security of information maintained or accessed by suppliers.

**5.35 COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS**

CCB Brasil must guarantee compliance with the laws that regulate its activities in order to obtain their adherence;

Ensure that the internal and external norms regarding the breach of confidentiality of any data or information of the CCB Brasil are in compliance, under penalty of responsibility and pertinent legal consequences.

**5.36 PERSONAL AND RESOURCES PROVISION**

Security considerations that support the requirements of CCB Brasil should be addressed through the initial hiring process and in the description of the responsibilities of the staff position, or informed according to the work to be performed.

**5.37 NON-DISCLOSURE AGREEMENT**

The employee shall read, understand and act in accordance with the relevant contractual terms applicable to his or her position.

do processo inicial de contratação e na descrição das responsabilidades do cargo da equipe, ou informadas de acordo com o trabalho a ser executado.

**5.37 ACORDO DE CONFIDENCIALIDADE**

O empregado deverá ler, entender e atuar de acordo com os termos contratuais importantes e aplicáveis a sua posição.

O empregado será solicitado a assinar uma documentação relacionada à segurança, a ser fornecida pela área de Recursos Humanos assim que for contratado. Tais documentos expressarão as responsabilidades gerais da segurança. Para terceiros o acordo de confidencialidade deve constar nos contratos entre as partes.

**5.38 GESTÃO DE CONTINUIDADE DOS NEGÓCIOS**

O CCB BRASIL deve proteger adequadamente os seus ativos, informações e processos de negócio críticos contra os efeitos de falhas e desastres de grandes proporções, através do desenvolvimento e implantação de uma estratégia abrangente de continuidade de negócios específica para os objetivos e prioridades da empresa e que possa demonstrar através de testes ter a capacidade de suporte necessário à recuperação das atividades do CCB BRASIL.

**5.39 GESTÃO DE TERCEIROS**

Quando houver necessidade de que terceiros tenham acesso aos sistemas e recursos da informação do CCB BRASIL, sejam estes consultores, parceiros comerciais, revendedores, etc., os riscos da concessão de acesso deverão ser identificados e controlados.

O CCB BRASIL reserva-se o direito de auditar as atividades e práticas de acesso de terceiros nos contratos aplicáveis. O CCB BRASIL reserva-se o direito de realizar essa auditoria, incluindo inspeções on-site em prazos razoáveis de negócio.

**5.40 GESTÃO DE DADOS PRIVADOS**

The employee will be asked to sign security-related documentation, provided by the Human Resources area, once hired. Such documents shall express the general responsibilities of security. For third parties the non-disclosure agreement must be included in the contracts between the parties.

**5.38 BUSINESS CONTINUITY MANAGEMENT**

CCB Brasil must adequately protect its critical assets, information and business processes from the effects of major failures and disasters by developing and deploying a comprehensive business continuity strategy specific to the goals and priorities of the company and, by demonstrating through tests, to have the necessary support capacity to recover the activities of CCB Brasil.

**5.39 THIRD-PARTY MANAGEMENT**

Where there is a need for third parties to have access to information systems and resources of CCB Brasil, whether these are consultants, commercial partners, resellers, etc., the risks of granting access should be identified and controlled.

CCB Brasil reserves the right to audit third party access activities and practices in the applicable agreements. CCB Brasil reserves the right to perform this audit, including on-site inspections within reasonable business terms.

**5.40 PRIVATE DATA MANAGEMENT**

CCB Brasil shall guarantee the privacy of users, so that all data collected and shared with third parties, which imply the personal identification of the user, are duly communicated and authorized by the owner of the information.

All information collected and received is used according to the need indicated in the request for service provision and there are controls implemented to protect

O CCB BRASIL deverá garantir a privacidade dos usuários, de maneira que todos os dados coletados e compartilhados a terceiros, que impliquem na identificação pessoal do usuário, são devidamente comunicados e autorizado pelo proprietário da informação.

Todas as informações coletadas e recebidas são utilizadas de acordo com a necessidade indicada na sua solicitação para prestação de serviços e existem controles implementados para proteger as informações contra acesso não autorizado ou processamento indevido.

information from unauthorized access or improper processing.