MANUAIS DE CONTROLES INTERNOS

5.3. POLÍTICA DE SEGURANÇA CIBERNÉTICA

VERSÃO “SITE”

COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO CECREB

SUMÁRIO

5. OPERACIONAL

5.3. POLÍTICA DE SEGURANÇA CIBERNÉTICA

5.3.1. INTRODUÇÃO

A política de segurança cibernética tem como objetivo atender a resolução CMN – Conselho Monetário Nacional nº 4.658/18 e estabelecer os princípios, conceitos, valores e práticas, sobre os requisitos da contratação de serviços de processamentos e armazenamento de dados e de computação em nuvem que devem ser adotados pelos administradores, colaboradores da CECREB.

A diretoria executiva é responsável pela implementação de um sistema de supervisão que demonstre que os controles de segurança cibernética estão sendo devidamente executados e alinhados, conforme as exigências do Banco Central do Brasil.

5.3.2 PRINCIPIOS DA SEGURANÇA CIBERNÉTICA

Os princípios básicos da segurança cibernética são: confidencialidade, integridade e disponibilidade das informações. Outras características são: controle de acesso e riscos cibernéticos. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos:

a) **Confidencialidade**: proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas voluntária ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários.

b) **Integridade**: garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica

exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

c) **Disponibilidade**: prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.

d) **Acesso controlado**: O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece há descuido ou possível quebra da confidencialidade das senhas de acesso à rede

e) **Riscos Cibernéticos**: Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

5.3.3. APLICAÇÕES DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, diretores e conselheiros, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador se manter atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação da

diretoria sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

5.3.4. CONTROLES DA SEGURANÇA DA INFORMAÇÃO

São exigidos alguns controles básicos de segurança da informação:

a) política de segurança cibernética e plano de ação que precisam ser aprovados pelo conselho de administração ou diretoria;

b) confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados;

c) controles que considerem o porte da instituição, seu perfil de risco, seu modelo de negócio, seus produtos e a sensibilidade dos dados;

d) controles e procedimentos com rastreabilidade para a garantia da proteção de informações sensíveis. e. classificação de dados ou de informações;

e) diretor responsável pela política de segurança cibernética, pela execução do plano de ação e pela gestão de incidentes;

f) implementação de programas de capacitação em segurança;

g) comunicação para clientes e usuários;

h) comprometimento da alta administração.

5.3.5. REGISTROS DE INCIDENTES RELEVANTES

O registro de incidentes, toma uma importância muito grande na resolução normativa. É exigido a existência e formalização dos seguintes controles relacionados ao registro de incidentes:

a) identificação da causa e impactos dos incidentes.

b) planos de ação e planos de resposta para incidentes.

c) área específica para os registros de incidentes.

d) plano de continuidade de negócio e relatório anual – andamento plano de ação e resposta para incidentes.

e) revisão anual pela direção ou conselho administração.

f) tem que ser adotada por empresas prestadoras de serviços para a instituição, que manuseiem informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição.

5.3.6. PRINCÍPIOS DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela CECREB pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

A CECREB, por meio da diretoria, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

5.3.7. REQUISITOS DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Para a uniformidade da informação, a política deverá ser comunicada a todos os colaboradores, diretores e conselheiros da CECREB a fim de seja cumprida dentro e fora da empresa.

> Deverá haver um membro de conselho de administração e da diretoria como responsáveis pela gestão da segurança cibernética, doravante designado como Comitê de Segurança Cibernética.

Esse Comitê será composto pelo presidente do conselho de administração e o diretor presidente da CECREB, mais profissionais indicados pelos prestadores de

serviços contratados pela CECREB para administrar e realizar a gestão das rotinas e processos de Tecnologia. (RC Consulting e Prodaf Informática)

Tanto a política quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança Cibernética.

Deverá constar em todos os contratos da CECREB o acordo de confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

A responsabilidade em relação à segurança cibernética deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade.

Todo incidente que afete a segurança cibernética deverá ser comunicado inicialmente à diretoria e caso julgue necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança cibernética, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, desktops nos acessos à internet,

no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela CECREB ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

A CECREB exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta política será implementada na CECREB por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta Política de Segurança Cibernética acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

5.3.8. DAS RESPONSABILIDADES ESPECIFICAS

5.3.8.1. COLABORADORES EM GERAL

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a CECREB e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

5.3.8.2. COLABORADORES EM GERAL EM REGIME DE EXCESSÃO (TEMPORÁRIOS)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança Cibernética.

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

5.3.8.3. DOS GESTORES DE PESSOAS, PROCESSOS E/OU DIRETORES

Ter postura exemplar em relação à segurança cibernética, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da política da CECREB.

Exigir dos colaboradores a assinatura do Termo de Responsabilidade, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da CECREB.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política.

5.3.9. DOS CUSTODIANTES DA INFORMAÇÃO

5.3.9.1. TECNOLOGIA DA INFORMAÇÃO

Testar a eficácia dos controles utilizados e informar a diretoria da CECREB.

Acordar com o diretor da CECREB o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta política.

O diretor da CECREB pode, pela característica de seus privilégios como usuário, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente. Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a CECREB.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário;
- os usuários (logins) de terceiros serão de responsabilidade do diretor

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

A diretoria da CECREB deverá:

a) realizar “auditorias” periódicas de configurações técnicas e análise de riscos;
b) responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais;
c) garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

d) garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

e) monitorar o ambiente de TI, gerando indicadores e históricos de:

i. uso da capacidade instalada da rede e dos equipamentos;

ii. tempo de resposta no acesso à internet e aos sistemas críticos da CECREB;

iii. períodos de indisponibilidade no acesso à internet e aos sistemas críticos da CECREB;

iv. incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);

v. atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

5.3.9.2. SEGURANÇA CIBERNÉTICA

O Comitê de Segurança Cibernética será composta pelo presidente do conselho de administração e pelo diretor presidente da CECREB, e empresas prestadoras de serviço.

i. Propor as metodologias e os processos específicos para a segurança cibernética, como avaliação de risco e sistema de classificação da informação.

ii. Propor e apoiar iniciativas que visem à segurança dos ativos de informação da CECREB.

iii. Publicar e promover as versões da política e aprovadas pelo Comitê de Segurança da Cibernética.

iv. Promover a conscientização dos colaboradores em relação à relevância da segurança cibernética para o negócio da CECREB, mediante reuniões presenciais individuais e coletivas, bem como documentos e qualquer outra forma oficial de divulgação.

v. Apoiar a avaliação e a adequação de controles específicos de segurança cibernética para novos sistemas ou serviços.

vi. Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Cibernética.

vii. Apresentar as atas e os resumos das reuniões do Comitê de Segurança Cibernética, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.

viii. Manter comunicação efetiva com o Comitê de Segurança Cibernética sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a CECREB.

ix. Realizar contratações de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior deverá adotar procedimentos visando certificar-se de que a empresa contratada atende as práticas de Governança Corporativa.

x. Proceder a uma avaliação da relevância dos serviços prestados por empresas com possibilidades de serem contratadas, quanto a adoção de controles que mitiguem efeitos de eventuais vulnerabilidades na liberação de novas versões de aplicativos no caso de serem executados através de internet.

xi. Buscar alinhamento com as diretrizes corporativas da instituição.

5.3.10. SEGURANÇA DA TECNOLOGIA

A CECREB conta com um software licenciado com todos os módulos comerciais. Isso garante uma série de filtros de segurança e controle de tráfego de pacotes. Configurado com padrão bloqueio, que rejeita qualquer pacote que não esteja listado em lista de autorização. Além disso conta com módulos de prevenção contra invasão, QoS, controle de banda, filtro de navegação e relatórios de acesso, controle por aplicativos, entre outros.

5.3.11. MONITORAMENTO DO AMBIENTE

Para garantir as regras mencionadas nesta política, a CECREB poderá:

i. implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

ii. tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do diretor ou por determinação do Comitê de Segurança da Informação;

iii. realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

iv. instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

5.3.12. RESPONSABILIDADES DA CECREB

A CECREB poderá obter dados cadastrais de seus cooperados, em algumas situações específicas, tais como associação, atualização de dados, cadastro de endereço de e-mail, participação em promoções ou sorteios.

Os dados fornecidos pelos cooperados serão mantidos em absoluto sigilo e, por esta razão, a CECREB assegura que eles não serão, sob nenhuma hipótese, vendidos, alugados, cedidos, nem de outra forma repassados a terceiros.

Além das disposições contidas neste documento, a CECREB afirma a sua conduta ética obrigando-se a cumprir, com rigor, as disposições legais vigentes no Brasil que tratam da privacidade, sigilo e segurança das informações que receber de seus cooperados, com a finalidade maior de resguardar os direitos.

5.3.13. CONSIDERAÇÕES FINAIS

Essa política deve ser cumprida e aplicada em todas as áreas da CECREB e deve ser revista e/ou alterada por proposta do conselho de administração ou diretor e ser levada ao conhecimento de todos os colaboradores.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da CECREB. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

Os SLA's estão inseridos nos contratos dos prestadores de serviços.