Política de Segurança da Informação

Versão 2.00

SUMÁRIO

1 INTRODUÇÃO 4
2 ABRANGÊNCIA 4
3 PRINCÍPIOS GERAIS 4
4 DIRETRIZES..4
4.1 Gestão de Ativos da Informação...4
4.1.1 Classificação da confidencialidade das informações 4
4.1.2 Controles de armazenamento e criptografia de dados 4
4.1.3 Gestão de acesso a dados 5
4.1.4 Utilização de softwares...5
4.1.5 Uso da internet..5
4.1.6 Ambiente de trabalho - mesa e tela limpa..5
4.1.7 Armazenamento e destruição de ativos de informação 6
4.1.8 Descarte de documentos e mídias de armazenamento 6
4.1.9 Comunicação e envio de informações externas 6
4.1.10 Conscientização 6
4.2 Diretrizes para Incidentes de Segurança da Informação e Gestão de Continuidade de Negócios (GCN)...7
4.2.1 Procedimentos de resposta a incidentes..7
4.2.2 Equipe de resposta a incidentes 7
4.2.3 Planos de continuidade de negócios..7
4.2.4 Testes e simulações 7
4.2.5 Revisão e melhoria contínua 7
4.2.6 Gestão de continuidade de negócios (GCN) 7
4.3 Diretrizes para a Gestão de Riscos...7
4.4 Diretrizes para Desenvolvimento Seguro de Sistemas...........................7
5 ATRIBUIÇÕES E RESPONSABILIDADES 7
5.1 Conselho de Administração..8
5.2 Comitê de Riscos 8
5.3 Diretorias, Gerências e Coordenadores de Áreas...................................8
5.4 Área de InfoSec 8
5.5 Área de Governança, Riscos e Compliance..8
5.6 Área de Jurídico Regulatório...8

5.7 Colaboradores, Prestadores de Serviços e Usuários do Sistema CERC 8
6 DISPOSIÇÕES GERAIS 9
7 CONTROLE DOCUMENTAL 9
8 ANEXOS 10
8.1 Definições 10

1 INTRODUÇÃO

Definir diretrizes essenciais para proteger os ativos de informação da CERC, garantindo confidencialidade, integridade e disponibilidade dos dados em toda a operação da empresa. Esta política tem como objetivo defender as informações contra ameaças cibernéticas, garantir a continuidade operacional e melhorar o desempenho em segurança da informação. Isso visa preservar interesses de clientes, fornecedores e parceiros, reforçando a resiliência e confiança no Sistema CERC para contribuir com a estabilidade do mercado financeiro nacional.

2 ABRANGÊNCIA

As diretrizes desta política devem ser observadas e aplicadas por toda a estrutura da CERC nos pilares de pessoas, produtos e tecnologia.

3 PRINCÍPIOS GERAIS

A segurança da informação é aqui caracterizada pelos seguintes princípios:

- **Confidencialidade:** garantir que as informações estão disponíveis apenas a pessoas ou entidades autorizadas;
- **Integridade:** garantir que as informações são precisas, completas e livres de alterações indevidas;
- **Disponibilidade:** garantir que as informações, são acessíveis e utilizáveis por indivíduos ou entidades autorizadas.

Quando algum dos princípios acima é quebrado, a empresa tem riscos materializados que podem gerar impactos financeiros e de negócio, além de comprometer sua imagem perante clientes, parceiros e acionistas.

4 DIRETRIZES

4.1 Gestão de Ativos da Informação

4.1.1 Classificação da confidencialidade das informações

Todas as informações devem ser avaliadas, classificadas e tratadas de acordo com sua confidencialidade, conforme segue:

- **Pública:** seu acesso não precisa ser controlado, registrado e não exige implementação de mecanismos de segurança.
- **Interna:** o acesso a esta informação é somente para uso interno, não devendo ser exposta a pessoas de fora da CERC.
- **Confidencial:** essa informação tem caráter sigiloso e seu acesso deve ser restrito a pessoas autorizadas. Não deve ser divulgada ou redirecionada, mesmo internamente, sem a devida orientação e autorização de quem é responsável pela informação na CERC.

Os dados classificados como confidenciais, como por exemplo dados sensíveis ou críticos e isso inclui informações financeiras e pessoais, devem ter um nível de proteção mais elevado, observando medidas de criptografia, controles de acesso restritos e monitoramento constante.

Esta classificação deve ser respeitada sempre que houver transferência de posse ou comunicação do ativo de informação a outros funcionários, prestadores de serviços, parceiros de negócios e público em geral.

4.1.2 Controles de armazenamento e criptografia de dados

A CERC utilizará, quando apropriado, os seguintes controles para proteger seus dados:

- **Armazenamento Seguro:** os dados devem ser armazenados em ambientes que oferecem controles robustos de segurança. Para dados confidenciais, o armazenamento deve incluir criptografia em repouso e controles de acesso.
- **Criptografia de Dados:** utilizar padrões de criptografia fortes para proteger dados em repouso e em trânsito cujo acesso precisa ser controlado. As chaves de criptografia devem ser geridas de forma segura, evitando a exposição indevida.
- **Transmissão Segura:** assegurar que os dados em trânsito sejam protegidos por meio de protocolos seguros como TLS ou VPNs. Implementar medidas para garantir a integridade e a autenticidade dos dados durante a transmissão. Quando possível, deverá ser usado mTLS.
- **Backup e Recuperação:** o dono da informação deve seguir políticas rigorosas de backup de seus dados considerados críticos para o negócio segundo o BIA, garantindo que cópias de segurança sejam realizadas regularmente e armazenadas em locais seguros. Os procedimentos de recuperação devem ser testados e validados periodicamente.

4.1.3 Gestão de acesso a dados

Os acessos aos sistemas de informação da CERC são pessoais e intransferíveis e convém que sejam baseados no princípio de menor privilégio, garantindo que os funcionários e terceiros acessem apenas os dados necessários para suas funções, não divulgando e utilizando única e exclusivamente para o fim que foi autorizado, seguindo as diretrizes descritas na Norma de Gestão de Identidade e Acessos.

4.1.4 Utilização de softwares

Todos os colaboradores e terceiros devem utilizar

as ferramentas oficiais da CERC e casos de exceções devem ser avaliados pela TI Corporativa (para sua aquisição e distribuição) e pelo time de InfoSec caso não atendam aos requisitos mínimos de segurança descritos na Norma de Gestão de Identidade e Acessos, como por exemplo, mecanismos de autenticação integrada via Single Sign ON (SSO).

Adicionalmente, todos os patches de atualização dos softwares utilizados pela CERC são aplicados assim que disponíveis pelos fornecedores, primeiramente, em ambiente de homologação a fim de evitar problemas no ambiente de produção da CERC.

Vale ressaltar que todos os notebooks e computadores da CERC, além de seus servidores, devem possuir proteções de segurança implementados.

4.1.5 Uso da internet

O acesso à Internet, nas dependências ou utilizando equipamentos da CERC, tem a finalidade única e exclusiva de atender aos interesses do negócio, enriquecimento intelectual ou como ferramenta de busca de informações, ou seja, tudo o que possa contribuir para o desenvolvimento de atividades relacionadas à CERC.

O acesso às páginas e websites é de responsabilidade de cada usuário, ficando vedado o acesso a sites que possam ferir o Código de Conduta da CERC.

O uso da internet para assuntos pessoais deve ser restrito, sem comprometer as atividades dos usuários.

O acesso à internet por visitantes deve ser concedido através de rede WIFI segregada destinada a este fim.

Os acessos à internet serão monitorados através de identificação e autenticação do usuário.

4.1.6 Ambiente de trabalho - mesa e tela limpa

O colaborador deverá sempre bloquear seu computador ao deixar a estação de trabalho, ainda que momentaneamente, e não deverá deixar informações sensíveis ou confidenciais disponíveis ao alcance de outras pessoas (colaboradores ou não).

Informações confidenciais e de uso restrito não devem ser impressas ou anotadas em papel. Quando isto for necessário, devem ser sempre guardados em local seguro, como armários e gavetas com chave.

Ao final do expediente (no escritório ou home office), todo colaborador deverá guardar os documentos que estiver utilizando em local fechado com chave e desligar sua estação de trabalho, a fim de evitar a exposição de informação (sensível ou não).

4.1.7 Armazenamento e destruição de ativos de informação

Os ativos de informação exclusivamente relacionados à CERC permanecerão armazenados por tempo indeterminado.

Os ativos de informação, inclusive dados pessoais, recebidos de seus participantes, parceiros e fornecedores deverão ser arquivados por, no mínimo, 10 anos em cumprimento de obrigação legal e regulatória, bem como outras bases legais como o exercício regular de direitos, nos termos da Lei de Proteção Geral de Dados.

Após este prazo e após constatação de inexistência de dever legal e regulatório ou quaisquer processos administrativos, criminais ou civis em andamento, os ativos de informação deverão ser anonimizados ou destruídos.

4.1.8 Descarte de documentos e mídias de armazenamento

» **Documentos Confidenciais:** não deixe papéis confidenciais sem supervisão. Eles devem ser destruídos (triturados) ao invés de reciclados.

» **Descarte de Equipamentos:** a equipe de TI Corporativa deve garantir o descarte seguro de equipamentos. Antes de descartar ou doar dispositivos com armazenamento de dados, todos os dados devem ser completamente apagados usando métodos de exclusão seguros.

4.1.9 Comunicação e envio de informações externas

A comunicação e o fornecimento de informações a clientes, fornecedores, parceiros, reguladores e quaisquer outros interessados externos, devem obedecer à sua classificação de confidencialidade e o seu compartilhamento deve ser realizado com extremo cuidado, sempre buscando assegurar que a pessoa que está recebendo a informação seja o destinatário.

É extremamente vedado o upload de arquivos em plataformas públicas (4shared, megaupload, wetransfer, dropbox, box) devendo-se utilizar do Sharepoint, ou plataforma específica desenvolvida ou contratada pelo cliente.

Havendo dúvidas, não forneça a informação e contate a pessoa DPO para a devida orientação.

4.1.10 Conscientização

» **Programa de treinamento contínuo em segurança da informação:** a CERC deverá manter um programa de treinamento em segurança da informação, assegurando que todos os colaboradores estejam cientes das políticas, procedimentos e práticas de segurança.

» **Materiais de treinamento em segurança da informação atualizados:** garantir que os materiais de treinamento reflitam as ameaças e tecnologias mais recentes, e que sejam relevantes para os diferentes papéis dentro da empresa.

» **Campanhas de conscientização regulares:** desenvolver campanhas regulares de conscientização para manter a segurança da informação em destaque, abordando temas como *phishing,* segurança de senhas, segurança em dispositivos móveis, dentre outros.

» **Avaliação e Feedback:** regularmente avaliar a eficácia dos programas de treinamento e conscientização, e ajustá-los com base no feedback dos participantes e nas mudanças nas ameaças à segurança.

» **Integração de Novos Colaboradores:** incluir uma introdução à segurança da informação como parte do processo de integração de novos funcionários, garantindo que eles compreendam as políticas e práticas desde o início.

4.2 Diretrizes para Incidentes de Segurança da Informação e Gestão de Continuidade de Negócios (GCN)

4.2.1 Procedimentos de resposta a incidentes

Deve ser estabelecido um processo claro para responder a incidentes de segurança, incluindo preparação, detecção, análise, contenção, erradicação, recuperação, post-mortem e comunicação interna com as áreas envolvidas para que estas deem início aos processos de comunicação externa com as partes interessadas, como clientes, parceiros e órgãos reguladores competentes, conforme descrito em norma interna.

4.2.2 Equipe de resposta a incidentes

Convém que seja definido uma equipe especializada em resposta a incidentes, com papéis e responsabilidades claros, incluindo a comunicação com partes interessadas internas e externas, conforme descrito na Norma de Resposta a Incidentes Cibernéticos.

4.2.3 Planos de continuidade de negócios

Deve estar integrado a resposta a incidentes com os planos de continuidade de negócios, assegurando a rápida recuperação das operações críticas após um incidente de segurança cibernética.

4.2.4 Testes e simulações

Convém que sejam realizados testes regulares e simulações de incidentes para avaliar a prontidão da equipe e a eficácia dos planos de resposta e recuperação.

4.2.5 Revisão e melhoria contínua

Após um incidente, realizar uma análise de post-mortem para identificar lições aprendidas e oportunidades de melhoria nos processos e controles de segurança.

4.2.6 Gestão de continuidade de negócios (GCN)

A CERC deve estabelecer princípios, definições, diretrizes e responsabilidades que assegurem que todas as medidas preventivas e mecanismos de recuperação de desastre estão implantados e submetidos a testes regulares, garantindo a sustentabilidade dos negócios da CERC, mesmo em situações adversas, conforme descrito na Política de Continuidade de Negócios.

4.3 Diretrizes para a Gestão de Riscos

A Gestão de Riscos adotada pela CERC visa estabelecer princípios, diretrizes e responsabilidades a serem observadas na gestão dos riscos, suficientes para propiciar à CERC capacidade de maneira proativa, manter os níveis de exposição dentro do aceitável descrito na RAS (*Risk Appetite Statement*) conforme Política de Gestão de Riscos.

4.4 Diretrizes para Desenvolvimento Seguro de Sistemas

As práticas de segurança da informação devem ser rigorosamente aplicadas durante o desenvolvimento de sistemas internos e na aquisição de sistemas externos. Isso garante a aderência aos requisitos descritos na Norma de Desenvolvimento Seguro, assegurando uma governança efetiva em todo o ciclo de vida do software.

5 ATRIBUIÇÕES E RESPONSABILIDADES

Deverão ser observados conforme atribuição de cada membro abaixo listado, as diretrizes contidas nos seguintes documentos: Estatuto, Regimentos e demais Normativos Internos da CERC.

5.1 Conselho de Administração

- Revisar e aprovar periodicamente a Política;

5.2 Comitê de Riscos

- Apresentar parecer ao Conselho de Administração sobre a Política, os riscos tecnológicos e os mecanismos para proteção de dados informacionais.

5.3 Diretorias, Gerências e Coordenadores de Áreas

- Cumprir as determinações da presente política, informando à área responsável pelo sistema de gestão de Segurança da Informação, toda e qualquer ação não condizente às práticas estabelecidas nesta;
- Participar, se necessário, da investigação de incidentes relacionados à informação sob sua responsabilidade;
- Autorizar a liberação de acesso à informação sob sua responsabilidade;
- Revisar, de acordo com os prazos definidos, as liberações de acesso concedidas; e
- Participar junto à Diretoria de Riscos da elaboração de matrizes de riscos dos sistemas de informação sob sua gestão.

5.4 Área de InfoSec

- Atualizar e revisar esta Política periodicamente;
- Estabelecer e gerir continuamente a estratégia de segurança da informação, desenhada de acordo com as necessidades e objetivos da CERC;
- Elaborar e revisar as políticas e normas relacionadas à Segurança da Informação;
- Estabelecer controles, e processos que visam proteger as informações contra eventuais ataques cibernéticos ou modificações, divulgação e destruição não autorizada;
- Apoiar os responsáveis pelos ativos na redução do risco de acesso indevido; e
- Orientar os colaboradores e fornecedores quanto aos quesitos de Segurança da Informação e fornecer treinamentos relacionados ao tema, quando necessário.

5.5 Área de Governança, Riscos e Compliance

- Supervisionar o modelo de gestão de riscos, apoiando a área de InfoSec no monitoramento de seus riscos e certificação dos controles internos;
- Realizar o controle de apontamentos de auditorias internas e externas para garantir o cumprimento de prazos na implantação de plano de ação relativos à Segurança da Informação;
- Elaborar e revisar as matrizes de riscos dos sistemas de informação; e
- Avaliar a conformidade das diretrizes presentes na Política.

5.6 Área de Jurídico Regulatório

- Manter as áreas informadas sobre eventuais alterações legais e/ou regulatórias que impliquem em responsabilidade e/ou ações envolvendo a governança da segurança da informação.

5.7 Colaboradores, Prestadores de Serviços e Usuários do Sistema CERC

- Cumprir fielmente as orientações desta Política;

- Avaliar e classificar as informações de acordo com a sua confidencialidade: pública, interna e confidencial;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela CERC;
- Notificar a área de InfoSec em caso de suspeita de anormalidades, descumprimentos ou qualquer violação identificada no seu ambiente de trabalho relacionada a segurança cibernética;
- Disseminar a cultura de proteção e segurança da informação; e
- Participar dos treinamentos de segurança da informação sempre que for convocada(o) e implementar os aprendizados em seu dia a dia.

6 DISPOSIÇÕES GERAIS

- A segurança da informação é responsabilidade de todos os membros da organização. Cada indivíduo é responsável por proteger os ativos de informação aos quais tem acesso.

7 CONTROLE DOCUMENTAL

CRIAÇÃO | REVISÃO | REVOGAÇÃO			
Versão Anterior	**Versão Atual**	**Data da Aprovação**	**Ref. De ATA/Aprovação**
1.5	**2.0**	**05/03/2024**	**Conselho de Administração**
Diretoria Responsável		**Área Responsável**	
CoEs		**InfoSec**	
PRINCIPAIS MODIFICAÇÕES			
Alterações: » Reestruturação completa do documento para atender aos requisitos da Resolução BCB n° 304 de 20/3/2023.			

LEGISLAÇÕES OU DOCUMENTOS RELACIONADOS
» Resolução 304/2023 BCB; e » Lei n° 13.709/2018 (Lei Geral de Proteção de Dados).

8 ANEXOS

8.1 Definições

- **Ativo:** é tudo o que tem valor para a CERC.
- **Ativos de Informação:** são todos os ativos, tangíveis e intangíveis, que estão relacionados à informação.
- **Ciclo de Vida da Informação:** todas as fases pelas quais a informação passa dentro dos processos de negócio da CERC (produção, distribuição, armazenamento, processamento, transporte, consulta e destruição).
- **Classificação do Ativo:** é a indicação da importância do ativo.
- **Controle:** é toda forma de gerenciar o risco a que está submetido um ativo.
- **Criptografia:** é o processo de codificação de uma mensagem ou informação.
- **Proprietário:** é a pessoa responsável pelo ativo de informação. Ao proprietário cabe classificar o ativo e autorizar o acesso a ele.
- **Incidente de Segurança da Informação:** todo evento que constitua uma violação da Política de Segurança da Informação.
- **Risco:** é o potencial de uma ameaça trazer prejuízos para a CERC. É estimado com base na probabilidade da ameaça se concretizar e no impacto que poderá causar.
- **Segregação de Funções:** é o princípio de que, onde houver necessidade para o controle mais apurado dos riscos, cada pessoa seja encarregada e possa executar apenas parte do processo.
- **Segurança da Informação:** é a proteção da informação de forma que apenas as pessoas autorizadas tenham acesso a ela (Confidencialidade), que esteja disponível quando necessário (Disponibilidade) e com seu conteúdo correto (Integridade).
- **Sistema de Gestão de Segurança da Informação (SGSI):** é o conjunto de processos de trabalho e ferramentas que garantem que a CERC tenha uma efetiva e funcional segurança da informação.