CERC Central de Recebíveis S.A.

Política de Segurança da Informação

Versão 1.4
06/12/2021

OBJETIVO

Descrever a abordagem adotada pela CERC para preservar a integridade e confidencialidade das informações internas, de fornecedores, parceiros e dos demais participantes usuários do Sistema CERC, protegendo a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

USUÁRIOS DO NORMATIVO

Todos os envolvidos na operação da CERC, contemplando administradores e colaboradores que definem, executam ou participam dos processos de negócios, de controle e administrativos da CERC, bem como de prestadores de serviços e usuários dos sistemas da CERC.

REFERÊNCIA E DOCUMENTOS RELACIONADOS

Resolução CMN 4.658/2018; Termo de Compromisso – Políticas da CERC.

CONTROLE DO DOCUMENTO

Sempre que necessária, a atualização deste normativo será conduzida pela área de Governança, Riscos e Compliance (GRC) e pela área de Segurança da Informação, submetida para aprovação do Conselho de Administração, podendo ter sua aplicação imediata com a autorização da Diretoria Executiva. Documento mantido por prazo indeterminado na rede, com revisão mínima a cada 3 anos desde a sua última atualização.

Política Segurança da Informação

ÍNDICE

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 dentro do sistema de gestão de segurança da informação.

Comitê Gestor de SGSI: É o órgão colegiado responsável pelo Sistema de Gestão de Segurança da Informação.

Controle: É toda a forma de gerenciar o risco a que está submetido um ativo.

Criptografia: É o processo de codificação de uma mensagem ou informação, de forma que somente as pessoas autorizadas conseguem ter acesso.

Proprietário: É a pessoa responsável perante o SGSI 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.

Informação: A informação é um conjunto organizado de dados sobre um determinado fenômeno, entidade ou evento.

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.

2. REFERÊNCIAS

BIS – *Bank of International Settlements*

- Principles for Financial Market Infrastructures - 2012
- Principles for the Sound Management of Operational Risk – 2011
- Guidance on cyber resilience for financial market infrastructures – 2016

ISO – *International Standards Organization*

- ISO 27.002/2013 - Código de Prática para Controles de Segurança da Informação.

REGULAÇÕES

- Decreto 8.771/2016 – Regulamentação do Marco Civil da Internet.
- Lei Complementar nº 105/2001 - Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.
- Lei 12.737/2012 – Lei que instituiu o crime de invasão de dispositivos informáticos.
- Lei 12.965/2014 – Marco Civil da Internet.
- Lei 13.709/2018 – Lei de Proteção de Dados Pessoais.
- Resolução CMN nº 2.554/1998– Dispõe sobre a implantação e implementação de sistema de controles internos.
- Resolução CMN no 4.557/2017 – Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.
- Res. CMN no 4.893/2020 (vigente a partir de 01/07/2021) - Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

3. PRINCÍPIOS

A segurança da informação é aqui caracterizada pelos seguintes princípios:

- **Confidencialidade:** Garante que as informações tratadas são de conhecimento exclusivo de pessoas autorizadas a acessá-las.

- **Integridade:** Garante que as informações são mantidas íntegras, sem modificações indevidas, sejam acidentais ou propositais.

- **Disponibilidade:** Garante que as informações estão disponíveis a todas as pessoas autorizadas a consultá-las ou tratá-las.

- **Legalidade:** Garante que todas as informações estejam em conformidade com a legislação e normativos advindos de órgãos reguladores, relativos à segurança da informação.

Quando algum dos princípios acima não é respeitado, a empresa está exposta a riscos que podem comprometer a continuidade dos negócios e afetar sua imagem perante seus clientes, parceiros e acionistas.

4. RESPONSABILIDADES

4.1. Diretoria, 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, observando esta Política;
- Revisar, de acordo com os prazos definidos, as liberações de acesso concedidas; e
- Participar junto à Diretoria de Governança, Riscos e Compliance da elaboração de matrizes de risco dos sistemas de informação sob sua gestão.

4.2. Área de Segurança da Informação

- Estabelecer e gerir continuamente o sistema de gestão de segurança da informação, desenhado de acordo com as necessidades e objetivos da CERC;
- Elaborar e revisar as políticas e normas relacionadas à Segurança da Informação;
- Manter as atividades de segurança da informação alinhadas ao plano diretor de SI;

- Estabelecer controles, e processos que visam proteger as informações contra modificações, divulgação e destruição não autorizada, oriunda de erros, fraudes, vandalismo, espionagem ou sabotagem, independente do meio onde as informações trafegam ou são armazenadas;
- Apoiar os responsáveis pelos ativos na redução do risco de acesso indevido ou comprometimento das informações por pessoas não autorizadas;
- Garantir o funcionamento da organização no que tange à proteção da informação frente às ameaças a que está sujeita;
- Orientar os colaboradores e fornecedores quanto aos quesitos de Segurança da Informação e fornecer treinamentos relacionados ao tema, quando necessário;
- Suportar o processo de revisão dos perfis de acesso, junto aos gestores de sistemas;
- Identificar e avaliar os potenciais riscos de segurança da informação, bem como suas causas e consequências, apoiando na definição e implantação de medidas corretivas para redução de seu nível de exposição.

4.3. Área de Governança, Riscos e Compliance

- Acompanhar projetos implementados pelas áreas da instituição, discutindo sobre riscos e propondo medidas de controle no que tange à Segurança da Informação;
- 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;
- Supervisionar o modelo de gestão de riscos, apoiando a área de Segurança da Informação 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; e
- Supervisionar colaboradores e prestadores de serviços com relação ao cumprimento das determinações da Política.

4.4. Colaboradores, Fornecedores 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;
- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
- Notificar à Diretoria Executiva e a área de Gestão da Segurança da Informação em caso de anormalidade, descumprimento ou violação identificada no seu ambiente de trabalho;
- Disseminar a cultura de proteção e segurança da informação; e
- Participar dos treinamentos de segurança da informação sempre que for convocado.

5. DIRETRIZES PARA A GESTÃO DE ATIVOS DA INFORMAÇÃO

5.1. Propriedade do Ativo

A informação é o principal ativo da CERC e a base de todos os processos do negócio CERC. As informações acessadas, geradas ou desenvolvidas nas dependências internas ou externas por colaboradores, prestadores de serviços ou parceiros de negócios devem ser devidamente manuseadas, protegidas e utilizadas unicamente para a finalidade previamente autorizada, independente da forma como foi armazenada ou compartilhada.

Todos os recursos tecnológicos utilizados pela CERC, como sistemas, computadores, e-mail, telefones, redes, equipamentos de comunicação e de acesso à Internet, bem como documentos impressos, devem ser manuseados corretamente, de forma a zelar, proteger e preservar a continuidade do negócio.

5.2. 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 a originou.

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.

Todos os ativos de informação devem ser devidamente guardados e protegidos de acordo com sua classificação de confidencialidade. Importante lembrar que nenhum documento ou mídia (papéis, pen drives, entre outros) deve ser abandonado após sua utilização, cópia ou impressão.

5.3. Concessão de Acesso Físico

O acesso às dependências da CERC é controlado e disponibilizado apenas a pessoas autorizadas. Somente a equipe de infraestrutura possui acesso ao CPD e somente pessoas autorizadas possuem acesso às áreas restritas.

As regras relacionadas a este assunto estão descritas em normativo específico.

5.4. Concessão de Acesso Lógico

Os acessos aos sistemas de informação da CERC são pessoais e intransferíveis e todos os colaboradores usuários têm o dever e a responsabilidade de proteger, não divulgar e utilizar única e exclusivamente para o fim que foi autorizado.

São gerados logs de acesso para fins de auditoria e rastreabilidade.

O compartilhamento de senhas constitui falta grave, podendo sujeitar os colaboradores às sanções dispostas no Código de Conduta da CERC.

As regras relacionadas a este assunto estão descritas em normativo específico.

5.5. Concessão de Acesso Remoto

O acesso remoto aos recursos de sistemas e rede deve ser liberado somente após solicitação formal à Segurança da Informação que deve avaliar a solicitação e justificativa do acesso, antes de formalizar a respectiva autorização.

O acesso remoto realizado por empresas parceiras deverá estar em conformidade com esta política, e estará sujeito à análise prévia dos requisitos de segurança da CERC, bem como definição de responsabilidade em cláusula específica do contrato de parceria.

As regras relacionadas a este assunto estão descritas em normativo específico.

5.6. Utilização de Softwares

Todos os funcionários devem utilizar apenas os softwares instalados pela equipe de Tecnologia, que se encontram devidamente registrados e licenciados pela CERC, não é permitido o uso ou instalação de programas que não foram adquiridos, homologados e licenciados.

Havendo necessidade de aquisição ou desenvolvimento de um software ou aplicativo, a área usuária deverá encaminhar solicitação à área de Tecnologia, que procederá às análises de viabilidade e autorizações necessárias.

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 (fornecedores e próprios), possuem antivírus e anti-*malwares* instalados e atualizados.

5.7. Uso de Dispositivos Móveis e de Gravação

A utilização de dispositivos removíveis e de gravação (pen drives, modems 3G ou celulares para acesso à Internet, leitores/gravadores de CDs, entre outros) nas dependências da CERC não é permitida.

Dispositivos removíveis e de gravação estão desativados em todos os notebooks da CERC.

Em casos excepcionais, em que seja necessário o uso de dispositivos em decorrência de atividade ou situação específica, o colaborador deverá enviar solicitação à área de Gestão da Segurança da Informação, contendo aprovação de seu gestor imediato.

Apenas os equipamentos e softwares disponibilizados e homologados pela CERC serão permitidos em suas dependências.

Equipamentos móveis que não são de propriedade da CERC, devem ser avaliados quanto ao seu risco, autorizados e controlados pela área de Gestão da Segurança da Informação para

que a conexão de rede seja permitida. A solicitação de acesso deve ser realizada formalmente, através de formulário específico.

5.8. Uso do E-mail Corporativo

O e-mail corporativo é uma ferramenta disponibilizada para o desenvolvimento das funções do colaborador da CERC, sendo as mensagens neste trafegadas, monitoradas pela área de Gestão da Segurança de Informação.

Sendo assim, deve-se evitar a utilização do e-mail para troca de mensagens confidenciais ou estratégicas para os negócios da instituição.

É proibido o uso do e-mail para envio de mensagens que possam comprometer a imagem da CERC, ou qualquer outro material que possa trazer má publicidade ou constrangimento aos seus clientes e prestadores de serviços.

É recomendado não executar ou abrir arquivos anexados, enviados por remetentes desconhecidos, suspeitos ou em formatos alertados pela área de TI.

5.9. Uso da Internet

O acesso à Internet, tem a finalidade única e exclusiva para 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 com conteúdo considerados impróprios pela 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 com usuário e senhas temporárias. Após utilização os acessos devem ser revogados.

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

5.10. Uso da Rede Interna

O acesso à rede é para uso exclusivo das atividades da CERC.

Não é permitida a gravação de arquivos particulares nos drives da rede.

Todos os arquivos devem ser gravados na rede, pois arquivos gravados no computador (local) não possuem cópias de segurança (backup) e podem ser perdidos. Os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários.

Todos os dispositivos de acesso à rede interna da CERC deverão estar protegidos contra malwares através de softwares de proteção que devem ser atualizados automaticamente sempre que houver novas atualizações disponíveis.

Não é responsabilidade da área de TI a recuperação de arquivos que não respeitem a regra acima citada.

5.11. Impressão de Documentos

Todos os colaboradores devem utilizar senha de acesso para a impressão de documentos e recolher o material impresso de imediato.

Todo o funcionário que constatar irregularidades na utilização da impressora deve comunicar o fato ao seu gestor, à área de Gestão da Segurança da Informação ou à área de Governança e Riscos da Segurança da Informação, que tem autonomia para destruir o que foi encontrado e não retirado da impressora, além de informar o superior hierárquico do infrator.

5.12. 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 outros colaboradores e quaisquer terceiros que possuam acesso físico às dependências da CERC.

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, todo colaborador deverá guardar os documentos que estiver utilizando em local fechado com chave e desligar sua estação de trabalho, a fim de deixar a sua mesa limpa e sem nenhum tipo de informação disponível.

Deve-se, ainda, manter os armários e gaveteiros devidamente trancados, evitando assim o acesso indevido a informações da instituição e de seus clientes.

5.13. Controles Criptográficos

A CERC utilizará, quando apropriado, controles criptográficos para proteger as informações cujo acesso não é autorizado, de modo a garantir sua confidencialidade das informações. Isso é válido para informações críticas que precisam transitar para fora da rede da CERC.

Sendo assim, esses arquivos são criptografados e as chaves de segurança ficam armazenadas pela equipe de TI da CERC, sendo disponibilizadas apenas para o destinatário final do arquivo.

5.14. Backup de Informações

A equipe de TI será responsável pelo backup das informações da CERC.

As regras relacionadas a este assunto estão descritas em normativo específico.

5.15. 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 comuns e sensíveis, recebidos de seus Participantes, parceiros e fornecedores deverão ser arquivados por, no mínimo, 10 anos em cumprimento de obrigação legal e exercício regular de direitos, nos termos da Lei de Proteção Geral de Dados.

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

5.16. Descarte de Papéis e Mídias de Armazenamento

Papéis com informações confidenciais não devem ser deixados sem supervisão. Também não devem ser reciclados, devendo ser triturados para descarte.

A equipe de tecnologia é responsável pelo descarte seguro dos equipamentos utilizados pela CERC.

Todos os dispositivos descartados, mesmo como doação, que contenham unidades de armazenamento de informações, deverão ter seus dados previamente apagados. Deverão ser utilizados aplicativos que fazem uma deleção segura dos arquivos.

As regras relacionadas a este assunto estão descritas em normativo específico.

5.17. Comunicação

A comunicação e o fornecimento de informações a clientes, fornecedores, parceiros, colaboradores e quaisquer outros interessados, devem obedecer à sua classificação de confidencialidade.

O fornecimento de informações da CERC a terceiros, quando necessário, deve ser realizado com extremo cuidado, sempre buscando assegurar que a pessoa que está recebendo a informação seja o destinatário correto e que esta informação não traga prejuízos à CERC.

Havendo dúvidas, não forneça a informação e contate as áreas de Compliance e Jurídico para a devida orientação.

5.18. Conscientização

No processo de contratação, os colaboradores recebem acesso a uma pasta específica da rede denominada Kit Boas-Vindas, através desta pasta, a Política Interna de Segurança da Informação deve ser acessada e lida. Posteriormente o colaborador deve assinar o respectivo Termo de Compromisso com o objetivo de atribuir responsabilidade em observar fielmente as disposições contidas na Política e a adotar as práticas indicadas na execução de suas atividades.

Periodicamente são realizadas ações de aculturamento e conscientização para colaboradores e prestadores de serviços.

6. DIRETRIZES PARA A GESTÃO DE RISCOS E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

6.1. Gestão de Riscos

A Gestão de Riscos adotada pela CERC visa identificar, avaliar e atuar sobre riscos ao negócio, de forma a proativamente mantê-los dentro de parâmetros adequados à continuidade da operação. Visa garantir também que os processos e procedimentos relacionados à gestão de riscos da CERC atendam aos requerimentos regulatórios vigentes, bem como às melhores práticas.

As ameaças e os riscos decorrentes dos ativos de informação são avaliados e, se necessário, encaminhados para a Comissão de Segurança da Informação que irá decidir sobre a execução de medidas sugeridas para o controle de riscos. As medidas aprovadas serão implementadas nas condições e prazos estabelecidos por esta Comissão.

6.2. Aquisição, Desenvolvimento e Manutenção dos Sistemas

Os requisitos de segurança da informação devem ser considerados e incluídos no desenvolvimento dos sistemas e nos sistemas adquiridos externamente.

Os sistemas em operação devem ser mantidos e atualizados nas versões estáveis mais recentes e suportadas pelos fornecedores. Todas as modificações e atualizações de hardware e software devem ser analisadas de acordo com as necessidades do negócio, controladas e documentadas adequadamente.

Os sistemas deverão funcionar com os direitos necessários e suficientes para sua execução.

Todas as versões de sistemas e funcionalidades devem ser testadas e aprovadas nos ambientes de “Teste” e “Homologação” antes de entrarem em “Produção”.

As regras relacionadas a este assunto estão descritas em normativo específico.

O controle de versões de sistemas deve garantir que todas as mudanças sejam feitas de modo ordenado e que sempre esteja disponível a versão anterior para recuperação em caso de problemas.

O procedimento deve ser seguido de acordo com o normativo específico destinado ao assunto.

6.3. Gestão de Incidentes de Segurança da Informação

A área de infraestrutura de TI deve fornecer suporte tecnológico (hardware e software) para a proteção das informações, de modo a eliminar ou diminuir as vulnerabilidades (antigas ou que vierem aparecer) e sugerindo e implantando os controles tecnológicos adequados às necessidades do negócio, sempre procurando reduzir os riscos à segurança da informação.

Deverão ser implantados controles tecnológicos para detectar, prevenir e alertar possíveis incidentes de vazamento de informações e crimes cibernéticos.

Periodicamente devem ser realizados testes de vulnerabilidades técnicas dos equipamentos críticos de infraestrutura. As vulnerabilidades identificadas nestes testes, devem ser tratadas de acordo com seus níveis de criticidade e prazos definidos. Os resultados das varreduras devem ser comparados com os resultados anteriores para identificar o correto tratamento realizado ao longo do tempo.

As aplicações de patches de segurança disponibilizadas pelos fornecedores de softwares, a atualização das versões utilizadas e a manutenção dos programas de proteção contra malwares, é realizada pela equipe de infraestrutura da CERC.

A aplicação é realizada inicialmente no ambiente de testes, e após aplicada em homologação. Somente após os testes em homologação, é realizada a aplicação em produção.

A utilização da capacidade dos sistemas de informação deve ser monitorada e as projeções de capacidade devem ser feitas para assegurar que o processamento adequado e capacidade de armazenagem estejam disponíveis quando necessário.

As medidas de segurança devem ser verificadas periodicamente: autenticação, controle de acesso, estatísticas, controle de rede entre outras.

O procedimento deve ser seguido de acordo com o normativo específico destinado ao assunto.

6.4. Gestão de Continuidade de Negócios (GCN)

A CERC possui estratégia de GCN, que foi projetado como um guia para o GAC - Grupo de Ação em Contingência, grupo designado pela Diretoria Executiva para tal função, e para demais colaboradores da CERC no trato de crises (emergência) internas ou externas que ameacem ou realmente impactem a condução dos negócios.

O procedimento deve ser seguido de acordo com o normativo específico destinado ao assunto.

7. HISTÓRICO DE ATUALIZAÇÃO

Data	Versão	Descrição	Área
31/03/2017	1.0	Criação	Operações / TI
17/12/2018	1.1	Atualização	Controles Internos / TI
18/10/2019	1.2	Atualização	Controles Internos / TI-SI
01/04//2021	1.3	Atualização	TI-SI GRC
06/12/2021	1.4	Atualização	TI-SI / GRC