PSIC
2021/09

SULCREDI
Força de quem coopera

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

SULCREDI\CREDILUZ – AV. CASTELO BRANCO, 570 – ABELARDO LUZ - SC

Sumário

1.OBJETIVOS

A Política de Segurança da informação e segurança cibernética (**PSIC)** tem como objetivo estabelecer os princípios, conceitos, valores e práticas que devem ser adotados na utilização dos recursos que tange as informações acessadas pelos administradores, funcionários da Sulcredi – Crediluz na sua atuação interna e com o mercado.

2.ABRANGÊNCIA

Esta Política aplica-se a todos os funcionários, estagiários, prestadores de serviços, consultores, auditores, temporários, fornecedores e parceiros da Sulcredi / Crediluz.

3.CONCEITOS

Para o correto entendimento e cumprimento desta PSIC é necessário o estabelecimento e compreensão dos seguintes conceitos:

- **Confidencialidade:** Garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário;
- **Disponibilidade:** Garante que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessária;
- **Integridade**: Garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.
- **Ambiente cibernético:** é o ambiente eletrônico onde são armazenados dados e ocorre o processamento de informações com ou sem a intervenção humana.
- **Incidentes:** São considerados incidentes todos os fatos ocorridos no ambiente da instituição que coloquem em risco a continuidade do negócio ou facilitam acesso a dados por pessoas não autorizadas;
- **Atividades de monitoramento:** são as atividades que objetivam avaliar e verificar a eficácia dos processos e controles dos riscos cibernéticos, permitindo que as deficiências identificadas sejam comunicadas e mitigadas através de planos de ações específicos;
- **Serviços em nuvem:** são serviços prestados utilizando tecnologias que permitam o acesso a programas, arquivos e serviços por meio da internet, sem a necessidade de instalação de programas ou armazenamento de dados.

Para assegurar a confidencialidade, disponibilidade e integridade todos os dados e informações tratados na Sulcredi – Crediluz devem ser adequadamente gerenciados e protegidos contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

Como a preocupação com a proteção e salvaguarda das informações deve ser um valor compartilhado entre todos na Sulcredi – Crediluz deve-se assumir individualmente e coletivamente atitudes pró ativas e engajadas no que diz respeito à proteção das informações e também realizadas campanhas contínuas de conscientização de Segurança da Informação.

4.ESTRUTURA NORMATIVA

A estrutura normativa da Segurança da Informação da Sulcredi – Crediluz é composta por um conjunto de documentos, relacionados a seguir.

- **Política:** define a estrutura, as diretrizes e os papéis referentes à segurança da informação;
- **Normas:** estabelecem regras, definidas de acordo com as diretrizes da Política, a serem seguidas em diversas situações em que a informação é tratada;
- **Procedimentos:** instrumentam as regras dispostas nas Normas, permitindo a direta aplicação nas atividades da Sulcredi – Crediluz.

5.DIRETRIZES

Para atender seus objetivos a PSIC estabelece um conjunto de diretrizes a serem consideradas para elaboração desta política:

- Proteger o valor e a reputação da instituição;
- Garantir a confidencialidade, integridade e disponibilidade das informações;
- Proteger informações de terceiros por ele custodiadas, contra acessos indevidos;
- Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;
- Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;
- Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a sua atividade;
- Conscientizar, educar e treinar os colaboradores por meio de Política Corporativa de Segurança Cibernética, normas e procedimentos internos aplicáveis às suas atividades diárias;
- Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

6.ASPECTOS GERAIS

Todos os dados e informações independentes de seu formato (físico ou digital) e os ambientes tecnológicos atingidos por essa PSIC são de propriedade exclusiva da Sulcredi – Crediluz, não podendo ser interpretados como de uso pessoal.

As informações da Sulcredi – Crediluz, dos associados e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

Todos os funcionários, estagiários, prestadores de serviços e demais devem ter ciência de que o uso das informações e dos sistemas de informação pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação, podendo estas servir de evidência para a aplicação de medidas disciplinares, processos administrativos e/ou legais;

7.TRATAMENTO DAS INFORMAÇÕES

Para garantir a proteção adequada às informações, deve existir um método de classificação da informação de acordo com o grau de confidencialidade e criticidade para o negócio da Sulcredi – Crediluz, se enquadrando nos seguintes níveis: Restrita, Confidencial, Interna e Pública.

Todas as informações devem estar adequadamente protegidas em observância às diretrizes de segurança da informação da Sulcredi – Crediluz em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte.

A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

8.GESTÃO DE ACESSO E IDENTIDADE

O acesso às informações e aos ambientes tecnológicos da Sulcredi / Crediluz devem ser controlados de acordo com sua classificação, garantindo que pessoas não autorizadas tenham acesso a informações sem possuírem esse privilégio.

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do trabalhador, evitando que uma pessoa se faça passar por outra. O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 –falsa identidade).

Todos os acessos devem ser liberados pelos responsáveis do departamento de tecnologia mediante solicitação do responsável pelo departamento de recursos humanos ou pelo departamento onde o trabalhador desempenha suas atividades. A exclusão dos acessos de um trabalhador deverá

ser informada tempestivamente pelo departamento de recursos humanos para evitar exposição de dados a pessoas que não possuam mais acessos.

9.GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Qualquer incidente ou indício de incidente deverá ser registrado, classificado e analisado. Os incidentes deverão ser classificados conforme sua severidade e recorrência em “Informação”, “Atenção”, “Média”,“Alta” e “Desastre”.

Incidentes classificados com severidade “Alta” e “Desastre” deverão ser objetos de uma análise de risco que deverá obrigatoriamente incluir: análise de ambiente, análise vulnerabilidades, indicação causa e um plano para mitigar o risco de uma nova ocorrência.

Deverá ser criado uma política e procedimentos específicos para a gestão de incidentes de segurança da informação.

10.RELACIONAMENTO COM PARTES EXTERNAS

Os contratos entre a Sulcredi – Crediluz e empresas prestadoras de serviços com acesso às informações, aos sistemas e/ou ao ambiente tecnológico devem conter cláusulas que garantam a confidencialidade entre as partes e que assegurem minimamente que os profissionais sob sua responsabilidade cumpram a Política e as Normas de Segurança da Informação.

11.RESPONSABILIDADES

Trabalhadores, estagiários e prestadores de serviços:

- Cumprir as Normas e os Procedimentos de Segurança da Informação da Sulcredi - Crediluz, buscando de imediato resolver qualquer dúvida que surgir com seu superior imediato ou com a equipe de tecnologia da informação;
- Salvaguardar todas informações impedindo o acesso, modificação, destruição ou divulgação não autorizados pela Sulcredi – Crediluz;
- Assegurar que todos os recursos tecnológicos se utilizados apenas com a finalidade aprovada pela Sulcredi – Crediluz;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual;
- Não discutir ou comentar assuntos relativos às atividades de trabalho em ambientes públicos ou áreas expostas, incluindo ambientes virtuais como blogs e redes sociais;
- Não compartilhar informações confidenciais de qualquer tipo;
- Comunicar imediatamente a seu superior imediato e ou área de gestão de segurança da informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e

Procedimentos.

Departamento de Tecnologia da Informação:

- Criar controles e políticas para garantir a salvaguarda de todas as informações armazenadas, processadas pela Cooperativa;
- Promover aprimoramentos tecnológicos para melhoria da segurança e estabilidade do ambiente tecnológico;
- Promover respostas a incidentes;
- Criar relatórios.

11.1.ÁREA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

A área de gestão de segurança de informação da Sulcredi – Crediluz será composta pelos trabalhadores da área de tecnologia da informação, podendo solicitar o auxílio de outros trabalhadores ou prestadores de serviços de forma "Ad hoc", isto é, com objetivos específicos para resolver um problema ou desenvolver um projeto.

Cabe à área de Gestão de Segurança da Informação:

- Prover todas as informações de gestão da Segurança da Informação, solicitadas pela Diretoria Executiva;
- Prover divulgação da Política e das Normas de Segurança da Informação para todos os funcionários, estagiários e prestadores de serviços;
- Promover ações de conscientização sobre Segurança da Informação para os funcionários, estagiários e prestadores de serviços;
- Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da Sulcredi – Crediluz;
- Estabelecer normas e procedimentos relacionados à instrumentação da segurança da informação da Sulcredi – Crediluz.

12.TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Os incidentes serão identificados por alertas ou pelo relato dos trabalhadores e serão classificados de acordos com critérios adotados pela Sulcredi – Crediluz que deverão levar em conta critérios como comprometimento de dados de clientes, impacto ao sistema financeiro, impacto a

segurança física e lógica da Sulcredi – Crediluz.

Todos os incidentes deverão ser registrados em sistemas ou formulários desenvolvidos com esse objetivo e passar por um processo de análise e comunicação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação, etc, de acordo com os procedimentos operacionais.

A área de Segurança da Informação elaborará um Relatório Anual contendo os incidentes relevantes ocorridos no período, ações realizadas de prevenção e respostas aos incidentes e resultados dos testes de continuidade. Este relatório ao Conselho de Administração, conforme determinações legais e regulamentares.

A Sulcredi/Crediluz poderá criar politicas ou procedimentos adicionais para regulamentar a gestão de incidentes.

13.CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

A área de Segurança da informação com apoio dos demais coordenadores de departamentos é responsável pela divulgação e conscientização dos demais trabalhadores a respeito dos princípios e diretrizes ligados às práticas de segurança da informação.

Essa divulgação dar-se-á pela promoção de programas de conscientização e capacitação internas, bem como divulgação em sites e programas promovidos pela Sulcredi – Crediluz de dicas e informações pertinentes ao quadro social e comunidade em geral objetivando o fortalecimento da cultura de Segurança da informação.

14.GOVERNANÇA COM AS ÁREAS DE NEGÓCIO E TECNOLOGIA

Todas as iniciativas e projetos das áreas de negócios devem estar alinhadas às diretrizes de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações.

15.SEGURANÇA DE ACESSO A AMBIENTES

A Sulcredi – Crediluz deverá estabelecer controles de acesso a ambientes físicos ou lógicos com informações sensíveis a essa PSIC garantindo que somente pessoas autorizadas tenham acesso de acordo com a criticidade das informações disponíveis naquele ambiente.

Os ambientes onde os servidores que armazenam sistemas da Sulcredi – Crediluz estão em área protegida com acesso devidamente controlado e monitorado.

A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmos funcionários, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

16.SEGURANÇA NO DESENVOLVIMENTO DE SISTEMAS DE APLICAÇÃO

Todos os sistemas desenvolvidos ou utilizados pela Sulcredi – Crediluz deverão ser aderentes a está PSIC e demais normas estabelecidas pela instituição bem como às boas práticas de segurança.

17.PROGRAMA DE SEGURANÇA CIBERNÉTICA

O Programa de Segurança Cibernética da Sulcredi – Crediluz é norteado pelos seguintes fatores: regulamentações vigentes; melhores práticas; avaliação de cenários mundiais.

Conforme sua criticidade, o programa divide-se em:

- **Ações críticas –** Consiste de correções emergenciais e imediatas para mitigar riscos iminentes;
- **Ações de Sustentação –** Iniciativas de curto e médio prazo, para mitigação de risco no ambiente, mantendo o ambiente seguro, avaliando o risco futuro para a Instituição e permitindo que ações de longo prazo/estruturantes possam ser realizadas;
- **Ações Estruturantes –** Iniciativas de médio / longo prazo que tratam a causa raiz dos riscos e que preparam a Sulcredi – Crediluz para o futuro.

18.SISTEMAS

Todos os sistemas utilizados nos ambientes da Sulcredi – Crediluz devem possuir controles de acessos que assegurem que apenas pessoas autorizadas tenham acesso às suas informações. As autorizações de acesso devem ser realizadas por perfil do usuário ou de forma excepcional a um usuário. Todas os acessos excepcionais a um usuário devem passar pela autorização de ao menos um membro da diretoria executiva e deve ser registrado em sistema ou formulário desenvolvido com este objetivo em específico.

O sistema ERP para controle da cooperativa, software de aplicações e sistemas operacionais são mantidos com atualizações periódicas liberadas pelos desenvolvedores as quais corrigem falhas e aplicam patch de melhoria e segurança.

O acesso ao terminal do sistema de controle é restrito, a identificação do usuário é feita

utilizando a autenticação Microsoft Actice Directory que garante o gerenciamento de acessos adequado ao perfil do usuário.

Todas as senhas utilizadas para acesso à administração de sistemas ou banco de dados deverão ser compostas por um mínimo de 8 caracteres contendo minimamente um caractere maiúsculo, um carácter minúsculo, um carácter especial e um carácter numérico e deverão ser armazenadas de forma fragmentada em 3 envelopes lacrados contendo as minimamente as assinaturas um responsável pelo departamento de tecnologia e um diretor executivo e deverão cada envelope sendo armazenado em um cofre de propriedade da cooperativa distinto.

As senhas contidas no envelope deverão ser alteradas na ocorrência de um incidente ou fato que comprometam a sua confidencialidade. A geração de senhas deverá ser executada pelo departamento de tecnologia através de um aplicativo ou rotina de geração aleatória.

19.BACKUP

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de Backup (cópia de segurança). Esse procedimento deverá permitir que a Sulcredi – Crediluz restaure os dados na ocorrência de incidentes que venham a ocorrer. Para tanto são estabelecidas algumas regras:

Todo o sistema de informação relevante a operação da Sulcredi – Crediluz deve possuir uma cópia de segurança de seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações;

Os backups são classificados em dois tipos completo ou incremental. No backup completo todos os dados são salvos em dispositivo externo ao servidor de origem e no backup incremental apenas os dados alterados após o último backup é salvo;

Todos os backups devem ser automatizados por sistemas de agendamento, os backups completos devem preferencialmente ser executados fora do horário comercial, períodos de pouco ou nenhum acesso de usuários ou processos aos sistemas de tecnologia;

Todos os backups deverão ser armazenados em storages ou servidores de arquivos sendo que minimamente uma das cópias deve ser armazenada em servidor no próprio datacenter e outra em um servidor localizado a mais de 20 metros do local do datacenter;

Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento;

O departamento de tecnologia da informação deverá preparar anualmente um plano de execução de testes de restauração de dados. Por se tratar de uma simulação a restauração deve ser realizada em um ambiente diferente ao de produção para que os dados não sejam sobrepostos;

Na ocorrência de erro em algum dos processos de backup o departamento de tecnologia da informação deverá avaliar a causa do erro e a viabilidade de realização deste backup fora do horário sempre no primeiro horário de trabalho após a ocorrência do erro. Erros graves nos processos de backup deverão ser reportados no formulário de reporte específico disponível na intranet no menu infraestrutura / Incidentes;

20.MÁQUINAS – ESTAÇÃO DE TRABALHO E TERMINAL

O acesso a todas as estações de trabalho e terminais deverá ser realizado com a utilização de senhas de acesso de conhecimento apenas dos trabalhadores da Sulcredi – Crediluz.

O acesso a estação de trabalho deverá ser encerrado no final do expediente. Sempre que o trabalhador necessitar se ausentar ou distanciar de sua mesa, a estação de trabalho deverá ser bloqueada utilizando a combinação de teclas (Windows + L) em casos de ausência rápida ou totalmente desligada em caso de ausência estendida. Estas ações aplicam-se a todos os trabalhadores com estações de trabalho, incluindo equipamentos portáteis.

O acesso às informações dos sistemas da Sulcredi – Crediluz só deverá ser realizada em equipamentos com controles adequados.

21.BOAS PRÁTICAS DE SEGURANÇA PARA IMPRESSÃO

Toda a impressão realizada deverá ser supervisionada pelo responsável e retirada imediatamente na impressora.

Toda a informação impressa deve ser protegida a contra perda, reprodução e uso não-autorizado. Isto é, documentos esquecidos nas impressoras, ou com demora para retirada, ou até mesmo em cima da mesa, podem ser lidos, copiados ou levados por outro funcionário ou por alguém de fora da instituição.

22.INSTALAÇÃO DE SOFTWARES

Todos os aplicativos instalados nos equipamentos pertencentes a Sulcredi – Crediluz deverão ser homologados pelo departamento de tecnologia da informação. É proibida a instalação de softwares que não possuam licença.

É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários

finais. Este procedimento só poderá ser realizado pela equipe do departamento de tecnologia da informação.

Os trabalhadores não poderão em hipótese alguma utilizar os recursos da Sulcredi – Crediluz para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

A utilização de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego ou qualquer outro aplicativo que possa causar sobrecarga na rede, prejudicar o seu funcionamento ou segurança da rede interna é restrita aos trabalhadores do departamento de segurança da informação ou prestadores de serviços devidamente autorizados e deve ser realizada apenas com o objetivo de aprimorar o funcionamento e a segurança da rede interna e dos aplicativos utilizados nela.

A qualquer momento a equipe do departamento de tecnologia da informação poderá realizar a desinstalação de softwares instalados nos equipamentos pertencentes a Sulcredi – Crediluz e alertar a diretoria sobre instalações não autorizadas através do formulário ou sistema utilizado para controle de incidentes.

23.REDE CORPORATIVA

Todos os arquivos devem ser gravados preferencialmente na rede, pois arquivos gravados no computador (local) não possuem cópias de segurança (*backup*) e podem ser perdidos. Os espaços em disco são controlados por departamento de TI, por isso, os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários.

Todo colaborador deve dispor de acesso a uma pasta privada para documentos que não precisam ou não devem ser compartilhados com outros usuários, bem como o compartilhamento controlado das pastas Públicas compartilhadas entre departamentos ou pontos de atendimento com acesso a informações pertinentes para o andamento das atividades diárias.

Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc..) nos *drivers* de rede, pois ocupam espaço comum limitado do departamento.

Documentos digitais de condutas consideradas ilícitas, como por exemplo, apologia ao tráfico de drogas e pedofilia, são proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso pertencente a Sulcredi – Crediluz.

23.1.CRIAÇÃO E GERENCIAMENTO DE VPN

Todas as conexões dos postos de atendimento ao cooperado (PAC) deve ser conectado a rede Sulcredi através do estabelecimento de redes privadas virtuais (VPN) do tipo IPSEC obedecendo os seguintes requisitos mínimos:

- Utilização de um Firewall para realização da interconexão;
- Utilização de algoritmo de criptografia 3DES ou AES (128);
- Função de hash: MD5 ou SHA1;
- Grupo DH: Minimamente de 1024 bits;
- Geração de chave criptográfica complexa tendo minimamente 15 dígitos incluindo números, letras maiúsculas e minúsculas. Essa chave deverá ser gerada por ferramentas de geração de senhas complexas para evitar a criação de senhas fracas.

  As demais conexões realizadas com objetivo de trabalho remoto pelos trabalhadores da Sulcredi devem ser utilizadas VPN através da ferramenta Open CPN essa conexão deverá atender minimamente os seguintes requisitos:
- Utilização de chave TLS de 2048 bit’s;
- Utilização de autenticação de usuários;
- Segregação dos usuários com acesso a VPN utilizando grupos registrados no Active Directory.

  Todas as instalações de novas VPN’s e liberação de acessos a trabalhadores deverá ser realizada com acompanhamento da equipe de tecnologia da informação da Sulcredi/Crediluz e aprovada pelo Comitê de Segurança da Informação (COSI) de forma colegiada ou por decisão expressa de um de seus membros devendo obrigatoriamente seja revisada na primeira reunião deste comitê.

24.MÍDIAS REMOVÍVEIS E DA PORTA USB

A liberação o controle de utilização de mídias removíveis nas estações de trabalho deverá ser realizada via software de antivírus.

O uso de mídias removíveis na empresa não é estimulado, devendo ser tratado como exceção à regra e sua solicitação deverá ser feita com a utilização de formulário ou sistema de solicitação especial de acesso e passar pela aprovação de minimamente um integrante da diretoria executiva.

O compartilhamento de arquivos na instituição deverá ser feito preferencialmente via diretórios de rede.

Os usuários que por algum motivo utilizarem mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia é um grande vetor de disseminação de vírus e softwares maliciosos podendo danificar e corromper dados.

25.INTERNET

A internet deve ser utilizada para fins corporativos, enriquecimento intelectual ou como ferramenta de busca de informações, tudo que possa vir a contribuir para o desenvolvimento de atividades relacionadas à empresa.

A navegação em *web sites* deverá ser feito via servidores de proxy o acesso direto deverá ser exclusivo em servidores e nas estações de trabalho do departamento de tecnologia da informação caso necessário para desempenho adequado de suas funções.

O servidor de proxy deverá possuir uma lista de sites de conteúdo relevantes ao desempenho das funções diárias dos trabalhadores que poderão ser acessados por qualquer pessoa na rede, os demais acessos são liberados apenas com senha sendo exclusivo aos coordenadores de departamento e integrantes da diretoria.

Qualquer liberação de um novo acesso a sites de conteúdo relevante deve ser utilização de formulário ou sistema de solicitação especial de acesso e passar pela aprovação de minimamente um integrante da diretoria executiva.

O acesso às páginas e *web sites* é de responsabilidade de cada usuário ficando vedado o acesso a *sites* com conteúdo impróprio e de relacionamentos.

É vedado qualquer tipo de *download*. Como também o upload de qualquer *software* licenciado à empresa ou de dados de propriedade da empresa ou de seus associados, sem expressa autorização do gerente responsável pelo *software* ou pelos dados.

26.CORREIO ELETRÔNICO (E-MAIL)

Cada trabalhador deve possuir uma caixa de e-mail corporativa com login e senha de acesso exclusivo a ele. É vedado o uso de sistemas *webmail* externo para envio de documentos com informações da Sulcredi – Crediluz. O recebimento de informações de interesse da cooperativa deverá ser feita exclusivamente pelo e-mail corporativo excetuando-se e-mails criados

anteriormente a criação do serviço de e-mail corporativo e utilizados para cadastros em fornecedores e órgãos governamentais.

É proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem da empresa perante seus associados e a comunidade em geral e que possam causar prejuízo moral e financeiro.

Evitar utilização do *e-mail* corporativo para assuntos pessoais.

Assegurar a propriedade de todas as mensagens geradas internamente e/ou por meio de recursos de comunicação e definir o uso desses recursos como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado por ser propriedade da empresa e até mesmo vistoriado por direitos de verificação e auditoria.

Não executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Exemplo de extensões que não devem ser abertas: .bat, .exe, .src, .lnk e .com, ou de quaisquer outros formatos alertados pela área de TI.

Utilizar o *e-mail* para comunicações oficiais internas, as quais não necessitam obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

27.ANTIVÍRUS E FIREWALL

Todas as estações de trabalho utilizadas pelos usuários deverão possuir antivírus instalados e atualizado periodicamente. A versão de antivírus instalada nas estações de trabalho deverá ser o “Panda Endpoint Protection” é vedada a instalação de qualquer outro antivírus nestes equipamentos.

A instalação de antivírus e Firewall´s nos servidores deverá ser feita após uma análise de impacto e caso seja avaliado que é relevante deverá ser indicada qual o produto é mais eficiente para os serviços que são hospedados no servidor.

Os Switch´s instalados na Sulcredi – Crediluz deverão ser preferencialmente gerenciáveis pois esse tipo de equipamento permite a segregação da rede e identificação e controle de tráfego.

28.CONTROLE DE ACESSO LÓGICO

Todos os trabalhadores deverão ter um login único de acesso aos recursos de rede que permite ele acessar os sistemas fornecidos pela cooperativa para o desempenho de suas atividades.

O login deve ser composto pela primeira letra do nome seguido do sobrenome do usuário na

existência de homônimos previamente cadastrados os responsáveis pelo departamento de tecnologia deverão criar um login utilizando um elemento que o distingua.

O acesso a redes sem fio deverá ser segregado, garantindo o isolamento da rede interna da cooperativa, com o objetivo de fornecer acesso a sistemas e dados internos apenas para os colaboradores desempenharem suas tarefas; poderão existir outras redes com acesso apenas à Internet a serem disponibilizadas a visitantes e usuários que não precisam/podem ter acesso aos dados internos. A definição de qual rede o usuário deverá ingressar ficará a cargo do departamento de tecnologia da informação após análise dos requisitos de acesso

Todas as redes sem fio com acesso à rede interna da cooperativa deverão permitir controle centralizado dos acessos através de uma console única que permita aos responsáveis pelo departamento de tecnologia verificar as estações conectadas de forma on-line e permita revogar o acesso de uma estação com facilidade. A chave das redes sem fio com acesso à rede interna deverá ser de conhecimento restrito aos trabalhadores do departamento de tecnologia da informação não devendo ser divulgada entre os demais trabalhadores e deverá ser alterada sempre que ocorrer indícios de utilização indevida.

Os acessos externos a rede da cooperativa, aos sistemas, deverão ser preferencialmente realizados por conexões VPN´s seguras criptografadas e deverão ser disponibilizadas apenas a trabalhadores ou prestadores de serviços expressamente autorizados através da utilização de formulário ou sistema de solicitação especial de acesso e passar pela aprovação de minimamente um integrante da diretoria executiva.

A Sulcredi – Crediluz reserva-se o direito de monitorar e registrar o acesso à Internet e a seus sistemas como forma de inibir a proliferação de programas maliciosos, garantindo a integridade da rede, sistemas e dados internos.

29.RASTREABILIDADE DAS INFORMAÇÕES

A Sulcredi – Crediluz deverá priorizar a utilização de softwares que permitam a realização de trilhas de auditorias identificando os usuários responsáveis por transação e o seu local de execução.

Sempre que possível deverá ser utilizado um software de armazenamento e análise de arquivos de log´s para facilitar sua interpretação e backup.

A Sulcredi – Crediluz deverá realizar periodicamente testes de segurança para garantir a segurança e estabilidade de seus ambientes.

30.SERVIÇOS EM NUVEM

Todos os serviços de armazenamento e processamento em nuvem utilizados pela Sulcredi – Crediluz devem ser realizados por empresas que adotem de práticas de governança corporativa e de gestão, proporcionais ao risco e complexidade do serviço prestado.

Todos os dados e processamento em nuvem deverão ser realizados preferencialmente em servidores alocados no território nacional, caso isso não seja possível poderão ser utilizados servidores alocados em territórios que possuam convênio para troca de informações entre o Banco Central do Brasil e às autoridades supervisoras dos países onde os serviços serão prestados.

Todos os contratos de armazenamento e processamento em nuvem celebrados após a vigência deste contrato deverão garantir o cumprimento da legislação e da regulamentação em vigor.

Todos os contratos de prestação de serviços de processamento e armazenamento em nuvem devem possuir cláusulas que preveem:

- A indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
- Medidas de segurança para a transmissão e armazenamento dos dados;
- Segregação dos dados e dos controles de acesso para proteção das informações;
- Continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços e transferência de dados a novo prestador;
- Exclusão total dos dados armazenados na extinção do contrato;
- Acesso a informações relativas às certificações e aos relatórios de auditoria especializada;
- Informações e recursos de gestão adequados ao monitoramento dos serviços prestados;
- Notificação sobre a subcontratação de serviços relevantes para a instituição;
- Permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços;
- Especificação de políticas de controle de acesso e backup de dados;
- Informação sobre limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;
- Acesso irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processos, dados e contratos em caso de determinação de

regime e resolução da instituição contratante pelo Banco Central do Brasil;

- Obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços seja qualquer for a motivação desta intenção, com, pelo menos, trinta dias de antecedência da data prevista para a interrupção;
- Atendimento total às exigências da resolução Nº 4.658 e outras resoluções que venham a ser emitidas pelo Banco Central do Brasil (Bacen) ou pelo Conselho Monetário Nacional (CMN).

31.SANÇÕES POR NÃO CONFORMIDADE

No caso de não cumprimento das normas estabelecidas nesta PSIC o trabalhador poderá sofrer as seguintes penalidades a critério da Diretoria Executiva poderá adotar com o apoio das Assessoria Jurídica e de Recursos Humanos, sanções administrativas e/ou legais como:

- **Advertência verbal:** O trabalhador será comunicado verbalmente que está infringindo as normas da política de segurança cibernética e será recomendado à leitura desta Norma;
- **Advertência formal:** A primeira notificação será enviada ao colaborador informando o descumprimento da norma, com a indicação precisa da violação cometida. A segunda notificação será encaminhada para a chefia imediata do infrator.

Essas ações poderão culminar com o desligamento e eventuais processos criminais, se aplicáveis.

32.RELATÓRIO ANUAL

Deverá ser elaborado um relatório anual com data-base de 31 de dezembro sobre a implementação da política de segurança da instituição e encaminhado ao conselho de administração contendo minimamente os seguintes itens:

- Ações desenvolvidas para adequação da estrutura organizacional e operacional a PSIC;
- Lista de rotinas, procedimentos, controles e tecnologias utilizados na prevenção e respostas a incidentes;
- Responsáveis pelo controle de incidentes;
- Resultados obtidos com a implementação da PSIC;
- Incidentes ocorridos no período;
- Plano de manutenção e atualização do parque tecnológico;

33.REVISÃO

Para garantir a melhoria contínua da PSIC de forma que a resposta aos incidentes ocorridos seja assertiva e tempestiva e o atendimento às determinações do Banco central do Brasil (BACEN) essa política deverá ser revisada anualmente sempre após a avaliação do relatório anual pelo conselho de administração.

Denílson Luiz Rodighero Diretor Presidente	Rodrigo Schweikar Diretor Responsável pela Política

Versão	Data	Alterações	Editor	Aprovação
2020/05	26/05/2020	Criação	Evandro Bonetti	Conselho de administração
2021/09	27/09/2021	Gestão de Incidentes, Controles Criptográficos	Evandro Bonetti	Conselho de Administração