sicres

Cooperativa de Crédito dos Servidores Públicos Municipais da Grande Vitória/ES

Política de Segurança das Informações e de Segurança Cibernética

Sumário

1. INTRODUÇÃO

A Política de Segurança das Informações e de Segurança Cibernética da SICRES é uma declaração formal da cooperativa acerca do seu compromisso com a proteção de Informações Confidenciais e Segurança Cibernética (cybersecurity), conforme definição adiante, devendo ser cumprida por todos os seus Colaboradores, prestadores de serviços terceirizados e membros dos órgãos sociais.

Seu propósito é estabelecer as diretrizes a serem seguidas no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança de Informações Confidenciais, bem como cumprir com as determinações contidas na Resolução nº 4.893, de 26 de fevereiro de 2021.

O Diretor de Segurança Cibernética é o responsável por esta Política de Segurança das Informações e de Segurança Cibernética.

2. OBJETIVO

Esta Política visa proteger as Informações Confidenciais e a propriedade intelectual da SICRES e de seus cooperados, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas, bem como aprimorar a segurança cibernética da cooperativa, nos termos da Resolução nº 4.893, de 26 de fevereiro de 2021.

Via de regra, nenhuma Informação Confidencial deve ser divulgada, dentro ou fora da cooperativa, a quem não necessite ou não deva ter acesso a tais informações para desempenho de suas atividades profissionais. Qualquer informação, independentemente de ser considerada Informação Confidencial, seja sobre a cooperativa, relativa às suas atividades, aos seus cooperados dentre outras, ou obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser revelada ou fornecida ao público, à mídia, ou a terceiros de qualquer natureza da maneira e conforme previstos nos documentos internos da cooperativa.

Os dados e as informações da SICRES são classificados entre: “confidencial”, “público” e “privado”. O Diretor de Segurança Cibernética e o Conselho de Administração são responsáveis por essa classificação. Os dados e as informações devem ser reclassificados sempre que houver mudanças relevantes ou no mínimo anualmente.

Na falta de previsão expressa, a revelação ou fornecimento somente poderá ocorrer com o conhecimento e, dependendo do caso, autorização prévia do Diretor responsável.

3. APLICAÇÃO

A efetividade desta Política depende da conscientização de todos os Colaboradores, prestadores de serviços e membros dos órgãos sociais e do esforço constante para que seja feito bom uso das Informações Confidenciais e dos ativos disponibilizados pela cooperativa ao Colaborador.

Esta Política deve ser conhecida e obedecida por todos os Colaboradores, prestadores de serviços e membros dos órgãos sociais que utilizam os recursos de tecnologia disponibilizados pela cooperativa, sendo de responsabilidade individual e coletiva o seu cumprimento.

4. RESPONSABILIDADE NA GESTÃO DA POLÍTICA

Cabe a todos os Colaboradores, prestadores de serviços e membros dos órgãos sociais:

a) cumprir fielmente esta Política;
b) buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança das Informações Confidenciais;
c) proteger Informações Confidenciais contra acesso, modificação, destruição ou divulgação não autorizados pela cooperativa;
d) assegurar que os recursos de tecnologia à sua disposição sejam utilizados apenas

para as finalidades aprovadas ou não proibidas expressamente pela cooperativa;

e) cumprir as leis e normas que regulamentam os aspectos relacionados ao direito autoral e propriedade intelectual no que se refere às Informações Confidenciais;
f) comunicar imediatamente ao Conselho de Administração sobre qualquer descumprimento ou violação desta Política.

5. CONCEITOS E PRINCIPIOS

Todas as Informações Confidenciais constituem ativos de valor para a SICRES e, por conseguinte, precisam ser adequadamente protegidas contra ameaças e ações que possam causar danos e prejuízos para a Cooperativa, Cooperados, Colaboradores, Prestadores de Serviços e Membros dos Órgãos Sociais.

As Informações Confidenciais podem ser armazenadas e transmitidas de diversas maneiras, como, por exemplo, arquivos eletrônicos, mensagens eletrônicas, sites de Internet, bancos de dados, meio impresso, mídias de áudio e de vídeo, dentre outras. Cada uma dessas maneiras está sujeita a uma ou mais formas de manipulação, alteração, remoção e eliminação do seu conteúdo.

A adoção de políticas e procedimentos que visem a garantir a segurança de Informações Confidenciais deve ser prioridade constante da cooperativa, reduzindo-se os riscos de falhas, os danos e prejuízos que possam comprometer a sua imagem e objetivos. Assim, por princípio, a guarda e segurança das Informações Confidenciais deve abranger três aspectos básicos, destacados a seguir:

a) **acesso**: somente pessoas devidamente autorizadas pela cooperativa devem ter acesso às Informações Confidenciais;
b) **integridade**: somente alterações, supressões e adições autorizadas pela cooperativa devem ser realizadas às Informações Confidenciais;
c) **disponibilidade**: as Informações Confidenciais devem estar disponíveis para os Colaboradores, Prestadores de Serviços e Membros de Órgãos Sociais autorizados sempre que necessário ou for demandado.

Para assegurar os 3 (três) aspectos acima, as Informações Confidenciais devem ser adequadamente gerenciadas e protegidas contra furto, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

Em cumprimento à Resolução nº 4.893/21, a cooperativa possui 4 (quatro) pilares principais no seu programa de segurança cibernética

a) identificação e avaliação de riscos (risk assessment);
b) ações de prevenção e proteção;
c) monitoramento e testes; e
d) plano de resposta.

A implantação e monitoramento da capacidade da cooperativa atender a estes pilares deverá ser feito pelo Diretor responsável. Também a fim de atingir os objetivos dispostos acima, cada colaborador da cooperativa, prestador de serviços e membros de órgãos sociais terá suas próprias responsabilidades.

A cooperativa deverá ter uma abordagem holística em relação à segurança cibernética, sendo obrigação do Conselho de Administração promover treinamentos para que os Colaboradores, Prestadores de Serviços e Membros de Órgãos Sociais saibam as suas respectivas funções na proteção de Informações Confidenciais, para que possam agir de maneira apropriada frente as situações que requeiram respostas.

6. MODELO ADOTADO

A SICRES optou por terceirizar os serviços, contratando a empresa Tecnologia da Informação - SRC Soluções em Redes Corporativas Ltda ME especialista em rede, segurança e infraestrutura, dedicado à segurança das informações, segurança cibernética, contingência e outros assuntos relacionados com tecnologia da informação, a realização de tarefas (e.g. instalações, substituições, configurações), verificações e manutenções periódicas.

7. PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA

7.1. Identificação e Avaliação de Riscos (Risk Assessment):

A SICRES deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta, entre os quais se incluem:

a) roubo de dados de cooperados, seguido de solicitação de resgate;
b) facilitação de acesso de terceiros a aplicativos e dados críticos, por um membro interno;
c) ataque ou incidente em um fornecedor que resulta na exposição de dados sensíveis da cooperativa, indisponibilidade ou impossibilidade de acesso às informações dos cooperados;
d) implantação de Malware agressivo dentro do ambiente de computação da cooperativa;
e) sistemático comprometimento do portal da cooperativa até sua total desativação;
f) fraquezas nas aplicações móveis da cooperativa;
g) hackers que capitalizam as vulnerabilidades divulgadas publicamente nos sistemas da cooperativa para roubarem e depois venderem dados de cooperados; e
h) vulnerabilidades de hardware em ativos de tecnologia que possam facilitar a infiltração na rede, possibilitando a criação de pontos de acessos descontrolados, apoiando o entrincheiramento de uma ameaça persistente avançada.

Em seu Código de Segurança Cibernética, 2ª edição, página 5, publicada em 06/12/2017, a ANBIMA – Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais, definiu que os ataques mais comuns de criminosos cibernéticos (cybercriminals) são, dentre outros, os seguintes:

a) Malware (e.g. vírus, cavalo de troia, spyware e ransomware);
b) Engenharia Social;
c) Pharming;

d) Phishing scam;
e) Vishing;
f) Smishing;
g) Acesso pessoal;
h) Ataques de DDoS e botnets; e
i) Invasões (advanced persistente threats), dentre outros.

7.2. Ações de Prevenção e Proteção:

A SICRES adota regras para concessão de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância para acesso. A SICRES trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis, e o acesso remoto a arquivos e sistemas internos ou na nuvem têm controles adequados.

Outro ponto importante é que, ao incluir novos equipamentos e sistemas em produção, a SICRES deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção.

A SICRES conta com recursos de prevenção e detecção, tais como:

- Firewall, para proteção de rede e de intrusos;
- Antivírus, para proteção de estações de trabalhos;
- IPS, para detecção e proteção de intrusos; e
- Proxy, para encapsulamento da rede interna, e outros.

Da mesma maneira monitora o acesso a websites e restringe a execução de softwares e/ou aplicações não autorizadas.

A SICRES realiza, também, backup das informações e dos diversos ativos da

instituição, conforme as disposições do presente documento e do Plano de Continuidade do Negócio.

Todo incidente da informação deve ser registrado e a documentação mantida arquivada pelo prazo de 5 (cinco) anos.

O Diretor de Segurança Cibernética é responsável por responder a incidentes.

7.3. Monitoramento e Testes:

Os sistemas, serviços, dados, informações (incluindo as Informações Confidenciais) disponíveis na SICRES ou por esta disponibilizados para serem usados pelos Colaboradores, Prestadores de Serviços e Membros de Órgãos Sociais não devem ser interpretados como sendo de uso pessoal. Todos os Colaboradores, Prestadores de Serviços e Membros de Órgãos Sociais devem ter ciência de que o uso está sujeito a monitoramento periódico. Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware), por prestador de serviços terceirizado.

Os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto nesta Política, e nos demais documentos internos da SICRES e, conforme o caso, servir como evidência em processos administrativos, arbitrais e/ou judiciais.

A SICRES possui roteiro de testes indicando as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. Da mesma maneira deve diligenciar de modo a manter inventários atualizados de hardware e software atualizados, bem como os sistemas operacionais e softwares de uso atualizados.

Periodicamente, a SICRES realiza testes de segurança no seu sistema de segurança da informação e proteção de dados, executando, mas não se limitando, os seguintes procedimentos:

a) análise mensal de vulnerabilidade com reteste caso sejam detectadas

vulnerabilidades;

b) *Pentest* sempre que houver mudanças relevantes no sistema ou a cada dois anos;

c) análise de vulnerabilidades em todos os sistemas pertencentes à SICRES, incluindo programas adquiridos;

d) todos os testes de vulnerabilidades devem ser executados, exceto testes de stress (DoS e DDOS);

É de responsabilidade do Diretor de Segurança Cibernética:

- executar a análise de vulnerabilidades;
- identificar as vulnerabilidades detectadas; e
- executar outros procedimentos inerentes à segurança da informação sempre que as circunstâncias assim o exigirem.

Os prestadores de serviços devem realizar correções de vulnerabilidades detectadas nos serviços prestados. O prestador de serviço de TI – Tecnologia da Informação será responsável por analisar o resultado dos testes de vulnerabilidades realizados pelo prestador de serviços.

De acordo com o art. 8º, da Resolução nº 4.893/21, caberá ao Diretor de Segurança Cibernética a elaboração de relatório anual, com data-base de 31 de dezembro, contendo o resultado das análises de vulnerabilidades e dos *Pentests*, o qual será apresentado ao Conselho de Administração até 31 de março do ano seguinte ao da data-base.

Sem prejuízo dos testes realizados na forma mencionada acima, a SICRES realizará simulações de ataques e respostas da cooperativa que seriam possíveis nestes casos. As simulações deverão prever as ferramentas mais usadas pelos criminosos cibernéticos, revelando as principais vulnerabilidades dos sistemas da SICRES, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real.

O backup de todas as informações armazenadas nos servidores será realizado na

forma descrita no Plano de Contingência e Continuidade de Negócios da cooperativa, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

As rotinas de backup são periodicamente monitoradas.

7.4. Plano de Resposta:

Havendo indícios ou de suspeita fundamentada, a SRC Soluções em Redes Corporativas Ltda ME, deverá ser acionada para realizar os procedimentos necessários de modo a identificar o evento ocorrido.
Os procedimentos a serem aplicados poderão variar de acordo com a natureza e o tipo do evento.

Na hipótese de vazamento de Informações Confidenciais ou outra falha de segurança, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazo possível.

Em caso de necessidade, poderá ser contratada empresa especializada para combater o evento identificado.

Caso o evento tenha sido causado por algum Colaborador, Prestador de Serviços ou Membro de Órgão Social deverá ser avaliada a sua culpabilidade nos termos do Código de Ética e Conduta.

Eventos que envolvam a segurança das Informações Confidenciais ou que sejam decorrentes de quebra de segurança cibernética deverão ser formalizados em relatório para deliberação pelo Conselho de Administração. Tanto o evento, quanto as medidas corretivas adotadas e a deliberação do Conselho de Administração, ainda que sumariamente, deverão constar no Relatório de Controles Internos.

A SRC Soluções em Redes Corporativas Ltda ME será responsável pelo registro e

controle dos efeitos de incidentes.

Os procedimentos de segurança (resposta a incidentes, cenários de incidentes e tecnologias) devem ser testados anualmente.

A política de segurança cibernética e o plano de ação e de resposta a incidentes deverão ser documentados e revisados anualmente, conforme determina o art. 10, da Resolução nº 4.893/2021.

8. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

8.1. Adoção de Comportamento Seguro:

Independentemente do meio e/ou da forma em que se encontrem, as Informações Confidenciais podem ser encontradas na sede da SICRES e fazem parte do ambiente de trabalho de todos os Colaboradores. Portanto, é fundamental para a proteção delas que os Colaboradores adotem comportamento seguro e consistente.

Na SICRES, o processo relacionado à cultura de segurança cibernética compreende os seguintes procedimentos:

a) Programa de conscientização no formato de palestras e cursos, realizados anualmente;
b) O Diretor de Segurança Cibernética é responsável por implementar e manter o programa de conscientização;
c) Após concluir o programa de conscientização, o colaborador, prestador de serviços ou membro de órgão social deverá preencher um questionário;
d) Novos Colaboradores, Prestadores de Serviços e Membros de Órgãos Sociais devem assistir vídeo sobre segurança da informação;
e) A eficiência do programa de conscientização é baseada no número de treinados;
f) Cooperados da SICRES são informados sobre precaução no uso de seus serviços através do site da cooperativa, do facebook, de e-mail marketing e da intranet.
g) O Diretor de Segurança Cibernética e o Conselho de Administração são

responsáveis por compartilhar alterações nos procedimentos de segurança da informação da SICRES através de e-mail para Colaboradores, Prestadores de Serviços e Membros de Órgãos Sociais e através do site da cooperativa para os cooperados.

O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela SICRES. Desde que não haja abusos, o eventual uso do e-mail para assuntos particulares é tolerado. É terminantemente proibido o envio de mensagens e arquivos anexos que possam causar constrangimento a terceiros, bem como com conteúdo político ou outro que possa colocar a SICRES em risco.

A SICRES se reserva o direito de monitorar o uso dos dados, informações, serviços, sistemas e demais recursos de tecnologia disponibilizados aos seus Colaboradores, Prestadores de Serviços e Membros dos Órgãos Sociais e que os registros e o conteúdo dos arquivos assim obtidos poderão ser utilizados para detecção de violações aos documentos internos da cooperativa e, conforme o caso, servir como evidência em processos administrativos, arbitrais ou judiciais.

O Diretor responsável indicado no Unicad implantará as medidas necessárias para realizar o monitoramento, bem como para estabelecer as permissões de acesso aos documentos e arquivos da SICRES. Nesse sentido, o monitoramento poderá ser realizado pelo prestador de serviços de TI – Tecnologia da Informação mediante:

a) gravação dos ramais telefônicos internos;
b) gravação em vídeo do ambiente da cooperativa;
c) registro de mensagens de e-mail;
d) registro de acesso à Internet;
e) registro de acesso à rede interna; e
f) registro de acesso a documentos e arquivos.

Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware), pelo prestador de serviços externo.

Apenas pessoas autorizadas pelo Conselho de Administração poderão acessar os arquivos contendo as gravações e registros do monitoramento realizado, bem como, mediante autorização prévia do Diretor responsável indicado no Unicad poderão contratar prestadores de serviços externos para realizar o monitoramento.

O acesso será realizado aleatoriamente, de maneira inopinada e sem periodicidade definida. Os documentos, dados e informações encaminhados pelos prestadores de serviços serão para uso exclusivo do Diretor responsável.

8.2. Gestão de Acesso a Sistemas de Informação e a Outros Ambientes Lógicos:

O uso das Informações Confidenciais e dos recursos de tecnologia disponibilizados pela SICRES são monitorados, e os registros decorrentes do uso poderão ser utilizados para verificação e evidência da adequação das regras desta Política, e demais regras internas da cooperativa, através de monitoramento a ser efetuado pelo prestador de serviço de TI.

Todo acesso às Informações Confidenciais e aos ambientes lógicos da SICRES deve ser controlado, de forma a garantir permissão apenas às pessoas expressamente autorizadas pelo Diretor responsável.

O controle de acesso deve ser documentado e formalizado, contemplando os seguintes itens:

a) pedido formal de concessão e cancelamento de autorização de acesso do usuário aos sistemas;
b) utilização de identificador do Colaborador, Prestador de Serviços ou do Membro dos Órgãos Sociais (ID de cada um), individualizado, de forma a assegurar a responsabilidade de cada Colaborador, Prestador de Serviços ou Membro dos Órgãos Sociais por suas ações e omissões; verificação se o nível de acesso concedido é apropriado ao perfil do Colaborador, Prestador de Serviços ou Membro dos Órgãos Sociais e se é consistente com a Política de Segregação das Atividades;

c) remoção imediata de autorizações dadas aos Colaboradores, Prestadores de Serviços ou Membros dos Órgãos Sociais afastados ou desligados da SICRES, ou que tenham mudado de função, se for o caso; e
d) revisão periódica das autorizações concedidas.

8.3. Utilização da Internet:

O uso da Internet deve restringir-se às atividades relacionadas aos negócios e serviços da SICRES, e para a obtenção de informações e dados necessários ao desempenho dos trabalhos.

8.4. Sites na Internet

O acesso a sites externos na Internet é monitorado. Os arquivos contendo os registros das tentativas de acesso e dos acessos são armazenados nos servidores da SICRES.

Adicionalmente, o Diretor responsável poderá ser informado sobre acessos e tentativas de acesso a determinados sites.

8.5. Telefones Celulares:

Os Colaboradores deverão evitar utilizar telefones celulares durante o horário de expediente enquanto estiverem na sede da SICRES.

8.6. Acesso de Cooperados:

O acesso de cooperado ao site da cooperativa e outros meios digitais, para transações de empréstimos, busca de informações a seu respeito, etc. será feito exclusivamente através do endereço www.ibankdecla.com.br, precedido de termo virtual (ANEXO II) disponível no mesmo local, que deverá ser lido e após marcada a opção “Li e concordo”, mediante senha a ser fornecida pela SICRES para o primeiro acesso, cabendo ao cooperado a responsabilidade pela sua imediata alteração, a qual será pessoal e intransferível. Lembrando que a adequada utilização dos referidos meios

de acesso é um dever e obrigação do cooperado, consistente com as disposições do art. 8º do estatuto social.

Tentativas de violação do site da cooperativa e outros meios digitais e/ou de sua concretização, praticadas pelo cooperado, serão passíveis de sua responsabilização nas esferas legais, incluindo a sua eliminação do quadro de cooperados nos termos do que dispõe o art. 12, do estatuto social.

Eventuais fragilidades identificadas pelo cooperado deverão ser reportadas através do endereço eletrônico ouvidoria@sicres.coop.br ou 0800.283-2909.

8.7. Acesso de Terceiros:

O acesso de terceiros aos arquivos e sistemas da SICRES será possível, mas deve sempre ser precedido da assinatura de um termo de confidencialidade (ANEXO III) que estabeleça penalidade no caso de infração. Ademais, o terceiro deverá garantir à cooperativa, ainda que contratualmente, de que possui os controles necessários à boa guarda e proteção das informações aos quais terá acesso.

9. COMPARTILHAMENTO DE INFORMAÇÕES

Na ocorrência de incidentes que sejam relevantes como, por exemplo, Malware, Ransomware, Phishing, Ataque de Senhas, a SICRES compartilhará com outras instituições financeiras integrantes do SFN - Sistema Financeiro Nacional as informações sobre tais incidentes.

Referido compartilhamento também abrangerá informações sobre incidentes relevantes comunicados à SICRES por empresas prestadoras de serviços a terceiros.

As informações compartilhadas deverão estar disponíveis ao Banco Central do Brasil.

10. ENDEREÇO ELETRÔNICO

Em cumprimento ao art. 4º, da Resolução nº 4.893/21, a presente Política está disponível no endereço eletrônico da SICRES: www.sicres.coop.br.

Eventuais comunicações para o Diretor responsável devem ser enviadas através do seguinte canal: ouuvidoria@sicres.coop.br e 0800-283-2909.

11. REVISÕES E ATUALIZAÇÕES

De acordo com o art. 10, da Resolução nº 4.893/21, esta Política será revisada ao menos uma vez a cada ano. Não obstante as revisões estipuladas, poderá ser alterada sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

O Diretor responsável informará aos Colaboradores, Prestadores de Serviços e Membros de Órgãos Sociais sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da SICRES na Internet, conforme indicado acima.

12. VIGÊNCIA

Esta Política passa a vigorar na data de sua aprovação. Conforme art. 9º, da Resolução nº 4.893/21, compete ao Conselho de Administração aprovar esta Política, devendo este ato ser evidenciado em ata de reunião do referido órgão estatutário.

Vitória/ES, 03 de agosto de 2022.

MARIA JANE PEREIRA DE SOUZA PIMENTA:12542423768 Assinado de forma digital por MARIA JANE PEREIRA DE SOUZA PIMENTA:12542423768 Dados: 2022.08.16 16:33:38 -03'00'

Maria Jane Pereira de Souza Pimenta

Presidente

Assinado Certificado Digital

LINEA FRANCEZ DEPES TALLON:68913800730 Assinado de forma digital por LINEA FRANCEZ DEPES TALLON:68913800730 Dados: 2022.08.16 16:33:10 -03'00'

Linea Francez Depes Tallon

Diretora Administrativa

Assinado Certificado Digital

JOSE ANTONIO PAIVA:52634515715
Assinado de forma digital por JOSE ANTONIO PAIVA:52634515715
Dados: 2022.08.16 16:34:24 -03'00'

José Antônio Paiva

Conselheiro

Assinado Certificado Digital

FERNANDO ANTONIO BARCELLOS DALVI:00974942758
Assinado de forma digital por FERNANDO ANTONIO BARCELLOS DALVI:00974942758
Dados: 2022.08.17 10:39:09 -03'00'

Fernando Antonio Barcelos Dalvi

Diretor Operacional

Assinado Certificado Digital

NILZA HELENA CASTILHO FERNANDES:41689801700
Assinado de forma digital por NILZA HELENA CASTILHO FERNANDES:41689801700
Dados: 2022.08.16 16:35:13 -03'00'

Nilza Helena Castilho Fernandes

Conselheira

Assinado Certificado Digital

ANGELA MARIA BERMUDES:41650000782
Assinado de forma digital por ANGELA MARIA BERMUDES:41650000782
Dados: 2022.08.16 16:35:49 -03'00'

Ângela Maria Bermudes

Conselheira

Assinado Certificado Digital

ELIAS MUGRABI DE OLIVEIRA:17155487104
Assinado de forma digital por ELIAS MUGRABI DE OLIVEIRA:17155487104
Dados: 2022.08.16 16:36:34 -03'00'

Elias Mugrabi de Oliveira

Conselheiro

Assinado Certificado Digital

ANEXO I

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES E DE SEGURANÇA CIBERNÉTICA

Eu, _____, inscrito no CPF/MF sob o nº _____ , declaro que li e estou plenamente de acordo com as disposições da Política de Segurança das Informações e de Segurança Cibernética aprovados pela SICRES em 24 de maio de 2022.

Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações às quais terei acesso.

____, _____, de _____de 2022.

_____

Assinatura

Nome:

ANEXO II

TERMO DE UTILIZAÇÃO DO PORTAL DO ASSOCIADO E DE PRIVACIDADE

O presente termo visa regular a utilização do “Portal do associado SICRES” para contratação de produtos/serviços e acesso às informações, conforme condições abaixo transcritas:

1. O presente termo visa possibilitar somente ao associado SICRES e ao iminente associado o acesso aos seguintes produtos/serviços:

1.1. Solicitação de adesão ao quadro de sócios da SICRES, atualização cadastral, consulta e impressão do informe de rendimentos, consulta e impressão do capital integralizado, consulta de saldo de empréstimos, bem como das parcelas e sua contratação.

2. Para utilização e acesso ao “Portal do Associado SICRES”, o associado deverá informar seu CPF e senha individual intransferível, pois a SICRES não se responsabiliza pelo uso e acesso inadequados e efetuado por terceiros.

2.1. O associado responsabiliza-se pela guarda, sigilo e devida utilização dos dados de acesso ao portal, não sendo responsabilizada a SICRES por qualquer utilização indevida.

2.1.1. O associado é responsável pelas informações prestadas e por sua autenticidade.

2.1.2. É proibida a divulgação ou transferência dos dados de acesso a terceiros, exceto procurador ou curador do associado. No caso de Pessoa Jurídica, somente o administrador destacado no Contrato ou Estatuto Social é a pessoa responsável pelo acesso ao portal e por manter os dados atualizados.

2.1.3. Somente mediante solicitação expressa e formal o associado poderá excluir seu acesso ao portal.

2.1.4. O associado é exclusivamente responsável pelos prejuízos advindos da má utilização ou transferência de login e senha a terceiros.

3. São obrigações do associado:

3.1. Utilizar o portal de acordo com as informações prestadas no próprio site ou por Colaboradores da SICRES.

3.2. Acessar o portal com computador particular, para evitar quaisquer dissabores, sendo as despesas por esse acesso únicas e exclusivas do associado.
3.3. Manter sigilo de seus dados de acesso, solicitando ou providenciando substituição quando necessário.
3.4. Possuir margem consignável, se todos os descontos forem efetuados em holerite, para integralização mensal de capital e descontos das parcelas de empréstimos, inclusive aqueles contratados pelo Portal ou manter saldo na conta corrente indicada (cadastrada na SICRES).
3.5. Informar com atenção valores, datas, tabela de juros e demais dados para efetivação da contratação de produtos/serviços pelo portal, pois a SICRES se exime de quaisquer responsabilidades advindas do preenchimento errado e/ou em desconformidade com o quisto pelo associado.
3.6. Manter seus dados atualizados, guardando-os e protegendo-os para que não sejam indevidamente utilizados por terceiros, ocasião que, desonera a SICRES de quaisquer responsabilidades.
3.7. Informar imediatamente à SICRES qualquer evidência de má utilização com seu acesso, bem como quaisquer divergências.
3.8. Tomar todas as cautelas devidas, sob suas expensas, inclusive relacionadas à detecção de vírus ou qualquer outra.
3.8.1. A SICRES, verificando a existência de programas invasores, fica autorizada a suspender ou cancelar o acesso do associado, para salvaguardar as operações e informações de terceiros.
3.9. Agir com o devido dever moral, bom costume, licitamente e sem violar qualquer ordenamento jurídico, precipuamente quanto à lei de lavagem de dinheiro e anticorrupção e todo o aqui disposto.
4. É defeso ao associado:
4.1. Qualquer tipo de envio de material de cunho erótico, pornográfico, obsceno, difamatório ou calunioso ou que façam apologia ao crime, uso de drogas, consumo de bebidas alcoólicas ou de fumo, violência física ou moral, que promova ou incite qualquer tipo de preconceito, inclusive político, ou qualquer forma de discriminação, bem como o ódio ou atividades ilegais.
4.2. Ameaça, coação, constrangimento físico ou moral aos demais cooperados.

4.3. Violar direitos de terceiros, de sigilo, inclusive de seu próprio, e privacidade alheios.

4.4. Praticar ato que contamine ou prejudique equipamentos de propriedade da SICRES ou que viabilize essa prática ou qualquer outro ato que direta ou indiretamente cause prejuízo à SICRES ou a qualquer outro associado.

4.5. Utilizar qualquer outro nome ou dados advindos de propriedade intelectual de terceiros, inclusive relacionados a órgãos das administrações municipais da área de abrangência da cooperativa, precipuamente quando associados à SICRES.

4.6. Qualquer tipo de utilização da marca, software, slogan, domínio, nome, razão social, título do estabelecimento e todo e qualquer conteúdo do portal, pois a SICRES é a única detentora dessa propriedade.

5. O associado é responsável exclusivamente por:

5.1. Todos e quaisquer atos ou omissões decorrentes de seu acesso ao portal.

5.2. Todo e qualquer *upload* ou conteúdo carregado, enviado e/ou transmitido.

5.3. Qualquer tipo de indenização, moral ou material, decorrente de quaisquer danos ocasionados por sua culpa ou dolo a outros cooperados, terceiros ou à SICRES, inclusive em virtude do descumprimento do disposto neste Termo.

5.3.1. A SICRES exime-se de qualquer responsabilidade:

a) advinda de ação ou omissão de seu associado, inclusive que ocasione dano, independente se for por uso indevido do Site ou se ocasionado por terceiros autorizados pelo associado;

b) por falhas, impossibilidade técnica ou indisponibilidade sistêmica, mesmo que por conta disso não haja conclusão de qualquer tipo de negócio do associado;

c) por qualquer tipo de instalação de programas adicionais, anti vírus, etc. ou qualquer ônus dela advinda;

d) de todos atos decorrentes de falhas no computador do associado ou mau funcionamento de programas/softwares/equipamento;

e) informações/documentações erradas ou incompletas fornecidas pelo associado;

f) erros ou atos bancários e g) de eventuais consequências decorrentes de divulgação a terceiros de quaisquer dados/informações fornecidos pelo associado.

6. A SICRES é responsável por prestar necessárias informações sobre acesso e utilização do portal, além de ter prévia autorização do associado para processar e contabilizar todas as transações por ele efetuadas no portal.

7. As partes, SICRES e associado, deverão manter sob o sigilo qualquer tipo de informação obtidas no portal, preservando sempre pela privacidade e proteção de dados, conforme legislação vigente, sendo autorizada a guarda, coleta e utilização dos dados pela SICRES, somente para os fins que se destinam.

8. A vigência do presente termo é por prazo indeterminado, iniciando-se a partir da ciência e concordância do associado. A rescisão automática ocorrerá quando:

a) o associado for demitido da SICRES ou se perder sua elegibilidade;

b) descumprimento de qualquer cláusula aqui disposta;

c) ato fraudulento, viciado consubstanciando obtenção de vantagens;

d) discordância de qualquer cláusula aqui disposta ou colocada/retirada/alteração em momento posterior.

8.1. A infração de quaisquer cláusulas gera o dever da parte infratora ao pagamento das perdas e danos ocasionados, bem como honorários advocatícios, momento em que a SICRES poderá, por sua liberalidade e sem aviso prévio, tomar as medidas legais cabíveis e/ou suspender e/ou limitar o acesso ao portal e/ou tomar outras providências que entender necessárias, a qualquer tempo.

9. Disposições gerais:

9.1. Qualquer tolerância por parte da SICRES não poderá ser tratada como renúncia, novação, nem perdão, nem alteração de qualquer dispositivo presente nesse termo.

9.2. A SICRES poderá, sem aviso prévio, cancelar, suspender, remover, interromper, alterar ou atualizar, no todo ou em parte o “Portal do associado SICRES”, bem como efetuar, bloqueio de senha, suspenção ou cancelamento do acesso do cooperado para efetuar quaisquer averiguações ou quando houver evidência de descumprimento desse termo ou de legislação.

9.3. Presumir-se-á tácita a concordância do associado às alterações do presente ou do portal ou de qualquer informação nele contida, quando houver acesso ao portal, pelo associado, posterior à efetivação da alteração. Quanto à alteração da forma de acesso, essa poderá ser efetuada em qualquer momento e independentemente de aviso prévio.

O presente termo tem natureza cível e a responsabilidade das partes fica adstrita aos danos comprovados, sendo excluídos os danos indiretos, negócios frustrados e lucros cessantes.

9.5. Para maior segurança, poderá ser adotado critério de tempo de conexão.

9.6. A SICRES possui demais canais de atendimento, portanto não poderá ser responsabilizada por qualquer compromisso assumido pelo associado com terceiros.
9.7. Qualquer cancelamento de operações efetuadas no portal deverá ser solicitado à SICRES a qual poderá negar, conforme seus padrões operacionais.

As partes elegem o foro da Comarca de Vitória, Estado do Espírito Santo, para dirimir eventuais litígios e/ou controvérsias oriundas do presente instrumento.

☐ Declaro que li e concordo com os procedimentos acima descritos, comprometendo-me a respeitá-los e cumpri-los plena e integralmente.

ANEXO III

TERMO DE RESPONSABILIDADE E SIGILO

Eu, XXXXXXX, pelo presente instrumento, na qualidade de recurso disponível na prestação de atendimento ao cliente SICRES, comprometo-me a cumprir todas as orientações e determinações a seguir especificadas e outras editadas, bem como com as informações pertencentes à organização, ou por ela custodiadas, em razão da permissão de acesso aos recursos necessários para a execução de minhas atividades profissionais, estando ciente, de acordo, aderente e responsável que:

1) Devo obedecer, cumprir e respeitar, as diretrizes, políticas, normas e procedimentos de Segurança da Informação da SICRES publicadas e armazenadas nos meios de comunicação internos que regem o uso dos recursos a mim disponibilizados, sejam estes digitais ou impressos; bem como o manuseio das informações a que tenho acesso, ou possa vir a ter, em decorrência da execução de minhas atividades como prestador de serviços.

2) Qualquer meio de acesso a informações ou instalações, como Identificador de Usuário <LOGIN>, Senhas de acesso a Sistemas <PASSWORD>, Aplicativos, Internet, Intranet, Conta para acesso a Correio Eletrônico, crachás, cartões, chaves, tokens ou afins, que a SICRES me forneceu ou vier a me fornecer são individuais, intransferíveis, estarão sob minha custódia e serão utilizados exclusivamente no cumprimento de minhas responsabilidades funcionais perante a Instituição, devendo ser por mim devolvidos ou disponibilizados para a SICRES em caso de rescisão contratual.

3) Meus acessos à Internet (conforme nível de acesso permitido, devem ser utilizados para a realização de atividades vinculadas a prestação de atendimento ao cliente SICRES.

4) Todos os meus acessos efetuados e informações por mim manipuladas (sistemas de informação, correspondências, cartas, e-mails etc.), serão passíveis de verificação pelos representantes da SICRES, que recebam atribuição para tal, a qualquer momento, independente de aviso prévio. Em decorrência disto, estou ciente que a SICRES é o legítimo proprietário e custodiante de todos os

equipamentos, infraestrutura e sistemas de informação que serão por mim utilizados.

5) As informações por mim geradas ou recebidas durante minha estadia neste local no cliente SICRES e/ou em função desta, deverão tratar apenas de assuntos profissionais e ligados exclusivamente a prestação de serviços.

6) Não devo adquirir, reproduzir, instalar, utilizar e/ou distribuir cópias não autorizadas de softwares ou programas aplicativos, produtos, mesmo aqueles desenvolvidos internamente pelos departamentos técnicos pertencentes à SICRES.

7) Não é permitida a entrada ou saída de informações da SICRES, quer estas sejam em meios magnéticos (CDs, fitas, disquetes, pen drives, dentre outros) ou em meios físicos (papel etc.) sem o conhecimento e autorização de seu responsável.

8) Todos os recursos de tecnologia da informação a mim disponibilizados são para fins relacionados única e exclusivamente a prestação de serviços.

9) Em caso de utilização de acesso remoto, devidamente autorizado, aos recursos da SICRES para a execução de minhas atividades profissionais, devo manusear as informações obedecendo aos mesmos critérios de segurança exigidos nas instalações internas para o desempenho de minha atividade como prestador de serviços.

10) Devo zelar pela segurança, pelo uso correto e pela manutenção adequada dos equipamentos existentes no âmbito corporativo, compreendendo entre outros aspectos:

a. Nunca deixar equipamento de minha utilização ativo sem antes bloquear seu acesso ou desativar a senha;
b. Jamais emprestar minha senha ou utilizar a senha de outros;
c. Solicitar eliminação ou bloqueio de minha senha ao ausentar-me por período superior a 30(trinta) dias.
d. Nunca utilizar senhas triviais que possam ser facilmente descobertas;
e. Não divulgar informações da SICRES a quem quer que seja.
f. Não deixar relatórios, disquetes, CDs, ou quaisquer mídias com informações confidenciais em cima das mesas ou em local de fácil acesso;
g. Não utilizar/instalar software que não tenha sido devidamente homologado pelo departamento de T.I.;
h. Respeitar as leis de direitos autorais e propriedade intelectual;

i. Zelar pelos equipamentos pertencentes à SICRES, a mim confiados, para a execução de minhas atividades como prestador de serviços;
j. Ao término do expediente, ou no caso de ausência prolongada, me comprometo a deixar o local de utilização limpo e organizado;
k. Devo efetuar o descarte das informações de forma a impedir o seu resgate, independentemente do meio de armazenamento no qual a informação se encontra.
l. Informar imediatamente à área competente de Tecnologia da Informação acerca de qualquer violação das regras de sigilo.

11) Reconheço que as recomendações acima são meramente exemplificativas e ilustrativas e que outras hipóteses de confidencialidade que já existam ou que venham a surgir no futuro devem ser consideradas e mantidas em segredo, e que em caso de dúvida acerca da confidencialidade de determinada informação devo tratar a mesma sob sigilo até que venha a ser autorizado a tratá-la diferentemente pelo órgão responsável. Em hipótese alguma irei interpretar o silêncio da SICRES como liberação de qualquer dos compromissos ora assumidos.

12) Descumprindo os compromissos por mim assumidos neste Termo estarei sujeito às penalidades e sanções aplicáveis.

____ , _____ de _____ de _____.

_____

Terceiro

Nome.:

Matrícula: xxxxxxx

Departamento.: .....

Login de acesso.: xxxxxxxx

RG.: xxxxxxxxxxxxxx

Gestor:

Empresa: