

Política de Segurança da Informação para Terceiros

POLÍTICA
DE
SEGURANÇA
DA
INFORMAÇÃO
PARA
TERCEIROS

*Área: Gerência de Segurança da
Informação*

Assunto: Segurança

Abrangência: Terceiros

Versão: 5





SUMÁRIO

01

Objetivo

02

Abrangência

03

Política

04

Deveres das Empresas Prestadoras de Serviço

05

Conscientização

06

Base Regulatória

07

Vigência e Histórico de Aprovação

Este documento é extração da Norma de Governança de Segurança da Informação aprovada em 27/11/2024 pelo Conselho de Administração da SicrediPar



1. Objetivo

Divulgar orientações e procedimentos de Segurança da Informação, estabelecendo deveres e responsabilidades das empresas prestadoras de serviços, visando assegurar a proteção efetiva das informações do Sicredi.



2. Abrangência

Este documento é destinado a todas as empresas prestadoras de serviço, contratadas pelas diversas áreas e entidades do Sicredi, que realizem acesso, coleta, armazenamento ou processamento de dados e informações de propriedade do Sicredi.



3. Política

A **Política de Segurança da Informação e Segurança Cibernética** do Sicredi estabelece diretrizes, regras e controles em todos os níveis e entidades do Sicredi, incluindo o gerenciamento dos riscos de segurança da informação e segurança cibernética. Seu escopo abrange o direcionamento estratégico para assegurar a proteção efetiva das informações do Sicredi.

Para visualizar a Política disponível ao público [clique aqui](#).



4. Deveres das Empresas Prestadoras de Serviço

4.1 Política de Segurança da Informação

Possuir uma Política de Segurança da Informação, formalmente aprovada, de conhecimento de todos os seus funcionários, contemplando critérios e níveis para classificação, tratamento, remoção e descarte seguro de informações.



4.2 Cláusulas Contratuais

Possuir cláusulas de confidencialidade, incluindo disposições de não divulgação de informações e de ciência da Política de Segurança da Informação, nos contratos de trabalho com seus funcionários e prestadores de serviço.

4.3 Licenciamento de Software

Não utilizar ou permitir a utilização de softwares e aplicativos para atividades de trabalho para o Sicredi sem o devido licenciamento, incluindo a utilização de qualquer conteúdo que viole direitos autorais.

4.4 Proteção de Dados de Informações

Utilizar controles para proteger dados e informações do Sicredi armazenados ou processados em seus ambientes, incluindo:

- a) Proteger os dados em softwares desenvolvidos ou utilizados para prestação dos serviços contratados pelo Sicredi;
- b) Proteger os dados contra vazamento e acesso não autorizado em seus equipamentos e ambientes de TI;
- c) Proteger os dados em trânsito;
- d) Segregar logicamente os dados do Sicredi dos dados de outros clientes e dos demais dados da empresa;
- e) Remover e descartar os dados de forma segura de todos os seus equipamentos e ambientes de TI após término do contrato ou por solicitação formal do Sicredi;
- f) Garantir que os dados sejam armazenados ou processados em países e regiões previamente autorizados e acordados contratualmente com o Sicredi.

4.5 Segurança em Softwares

- a) Adotar padrões e boas práticas de desenvolvimento seguro de softwares, como, por exemplo, OWASP Security Code Practices, Microsoft SDL - Security Development Lifecycle, CERT Secure Coding, OWASP - Web Service Security Cheat Sheet, entre outros, para os softwares entregues ao SICREDI;
- b) Desenvolver softwares contemplando controles para prevenir falhas e proteção contra vulnerabilidades, conforme TOP 25 CWE/SANS, Top Ten (OWASP), Top Ten Mobile (OWASP), Top Ten API (OWASP), entre outros, para os softwares entregues ao SICREDI;

- c) Desenvolver softwares, que possuam compatibilidade com versões atualizadas e suportadas pelos fabricantes de sistema operacional, banco de dados, plugins e outros serviços necessários para seu funcionamento para os softwares entregues ao SICREDI.

4.6 Treinamento de Segurança da Informação

- a) Possuir treinamento de segurança da informação, o qual deve ser realizado anualmente, incluindo orientações aos seus funcionários sobre deveres e cuidados no acesso a ambientes e informações do Sicredi, contemplando as orientações que constam no item "5. Conscientização" deste documento;
- b) Possuir ações periódicas para capacitação e disseminação da cultura de segurança da informação, contemplando ações para capacitar e treinar seus funcionários em padrões e boas práticas de desenvolvimento seguro para os softwares entregues ou disponibilizados para uso do Sicredi;
- c) Fornecer ao Sicredi, quando solicitado, a relação de funcionários treinados nas ações de capacitação em segurança da informação e desenvolvimento seguro, incluindo informações que evidenciem os cursos realizados e conteúdos abordados.

4.7 Gestão de Identidades e Acessos

Gerir adequadamente os acessos de seus funcionários e prestadores de serviço, incluindo:

- a) Informar imediatamente ao Sicredi sobre a dispensa e realocação de seus funcionários e sobre a necessidade de revogação de acessos aos ambientes/sistemas do Sicredi;
- b) Utilizar mecanismos e soluções de segurança, incluindo o conceito de privilégio mínimo necessário, para concessão de acesso aos seus ambientes;
- c) Utilizar uma política de senhas fortes, incluindo a troca periódica das senhas;
- d) Utilizar mecanismos para controle de acesso físico aos seus ambientes e dependências onde haja armazenamento ou processamento de dados e informações do Sicredi;
- e) Utilizar autenticação multifator para acesso à rede e ao seu ambiente de TI;
- f) Manter logs de acesso aos seus sistemas e ambientes de TI.

4.8 Segurança em Computadores

- a) Possuir uma solução de proteção contra softwares maliciosos (anti-malware) instalada e atualizada em todos os seus computadores;

- b) Bloquear o uso de dispositivos de armazenamento removíveis (pendrives, cartões de memória, hd's externos, etc.) em seus computadores;
- c) Aplicar criptografia de disco nos computadores;
- d) Não permitir a utilização de computadores particulares para a prestação de serviços ao Sicredi.

4.9 Gestão de Vulnerabilidades

- a) Manter um processo de gestão de vulnerabilidades, incluindo a identificação e correção periódica de vulnerabilidades identificadas nos ativos de seus ambientes de TI;
- b) Manter um processo de atualizações periódicas de segurança (patches) em softwares, sistemas operacionais, banco de dados, etc.

4.10 Acesso Remoto

- a) Utilizar soluções de VPN (Virtual Private Network) para todos os acessos remotos ao seu ambiente de TI, incluindo mecanismos de acesso condicional e/ou múltiplo fator de autenticação.

4.11 Gestão de Incidentes

- a) Possuir um Processo ou Plano de Resposta a Incidentes de Segurança da Informação, documentado e estabelecido, contendo procedimentos para identificação, contenção, resposta e investigação de ataques cibernéticos;
- b) Reportar incidentes de segurança da informação envolvendo dados do SICREDI para o e-mail seguranca_incidentes@sicredi.com.br, imediatamente após a identificação da ocorrência, informando as ações adotadas para contenção, resposta e investigação, incluindo documentação, evidenciando, no mínimo, fator, causa, impacto e ações executadas.

4.12 Comunicação de Subcontratações

- a) Informar e formalizar contratualmente, obtendo anuênciia prévia do Sicredi, quando houver a subcontratação de serviços envolvendo acesso, coleta, armazenamento ou processamento de dados ou informações do Sicredi, garantindo que a empresa cumpra os deveres e responsabilidades estipulados neste documento, sem prejuízo de demais obrigações previstas, de acordo com as cláusulas contratuais estabelecidas entre o Sicredi e a empresa contratada.



5. Conscientização

O conteúdo deste capítulo em sua totalidade deve ser repassado e conscientizado através de treinamentos e ações periódicas de capacitação de segurança da informação, aplicados pelas empresas prestadoras de serviços junto aos seus funcionários, ponderando os deveres que devem ser respeitados, conforme abaixo:

5.1 Acesso aos Ambientes do Sicredi

Ambientes físicos do Sicredi que possuam acesso controlado, somente poderão ser acessados mediante autorização do gestor responsável e acompanhamento por um colaborador do Sicredi.

5.2 Proteção de Equipamentos

Todos devem estar cientes de que são responsáveis pela proteção dos equipamentos de trabalho. Equipamentos e dispositivos disponibilizados pelo Sicredi devem ser devolvidos ao término da atividade ou no ato do encerramento do contrato.

5.3 Equipamentos Particulares

Não é permitida a utilização de equipamentos particulares para atividades de trabalho. Não é permitido gravar áudio, vídeo ou fotografar nos ambientes do Sicredi, incluindo telas de computador e sistemas, documentos impressos e quadros de atividades, sem autorização expressa por parte do gestor responsável no Sicredi.

5.4 Dispositivos de Armazenamento Removíveis

Não é permitida a utilização de dispositivos de armazenamento removíveis (pendrives, hd's externos, cartões de memória, etc.) em atividades de trabalho ou para armazenamento de informações corporativas do Sicredi.

5.5 Bloqueio de Tela

Os computadores devem ser mantidos bloqueados quando não estiverem em uso, sempre efetuando o logout após o uso, inclusive dos sistemas acessados durante as atividades de trabalho.



5.6 Proteção de Credencias de Acesso

As credenciais (usuário e senha) fornecidas pelo Sicredi são de uso pessoal e intransferível, devem ser mantidas em sigilo, sendo proibido seu compartilhamento. Qualquer utilização indevida é de responsabilidade da empresa contratada e do profissional que assim proceder. O e-mail e a senha fornecidos pelo Sicredi não devem ser utilizados para cadastro em sites/aplicações externas ou de terceiros, e-commerce, redes sociais, entre outros.

5.7 Proteção de Informações

As informações e sistemas devem ser utilizados somente para as finalidades devidamente aprovadas pelo Sicredi, não sendo permitida a utilização, divulgação ou cópia de dados e informações de propriedade do Sicredi sem prévia autorização. Dados e informações de propriedade do Sicredi somente podem ser compartilhados com terceiros autorizados a recebê-los, mediante aprovação do gestor responsável no Sicredi.

5.8 Classificação das Informações

Todos devem observar atentamente a classificação das informações disponibilizadas, considerando os três tipos de classificação adotados pelo Sicredi:

- a) **Confidencial:** São informações cuja revelação não autorizada expõe o Sicredi a prejuízos financeiros, constrangimentos ou comprometimento da segurança e privacidade dos negócios. Seu acesso deve ser controlado e limitado a um usuário ou a um grupo específico de pessoas;
- b) **Uso Interno:** São informações de uso restrito ao ambiente corporativo do Sicredi que não podem ser reveladas ao público externo. Qualquer informação que não possuir uma classificação explícita deverá ser tratada como uma informação exclusivamente de Uso Interno;
- c) **Uso Irrestrito:** Toda informação explicitamente aprovada por seu proprietário, para acesso irrestrito, cuja divulgação ao público externo não expõe o Sicredi a prejuízos financeiros, constrangimentos ou compromete a segurança e privacidade dos negócios.

5.9 Cuidados com Anotações e Lembretes

Deve ser utilizado o computador para realização de anotações e lembretes, evitando-se utilizar papéis e blocos de anotações que podem permanecer expostos.



5.10 Cuidados com E-mails e Contatos Suspeitos

Todos devem manter atenção ao receber e-mails suspeitos ou contendo links para sites externos, na dúvida nunca clicar em links, principalmente de remetentes desconhecidos.

Ao receber um e-mail suspeito e/ou indesejado deve-se reportá-lo através do próprio Outlook no botão 'Relatar' ou 'Relatar Mensagem' localizado na barra de ferramentas, selecionando a opção 'Lixo Eletrônico' ou 'Phishing'.

Além dos cuidados com e-mails, sempre deve-se confirmar a identidade das pessoas que pedirem informações, inclusive por telefone, questionando a real necessidade delas. Na dúvida, nunca fornecer informações.

5.11 Comunicação de Incidentes

Incidentes ou suspeitas de Incidentes de Segurança da Informação devem ser reportados para a área de Segurança da Informação do Sicredi de forma imediata, através do e-mail seguranca_incidentes@sicredi.com.br. Exemplos de incidentes a serem reportados:

- a) Acessos ou tentativas de acesso não autorizado a recursos de TI;
- b) Compartilhamento de credenciais (usuário e senha);
- c) Comprometimento de senha;
- d) Infecção de computador por código malicioso (malware);
- e) Vazamento/comprometimento de dados e informações.

5.12 Monitoramento e Registro dos Acessos

O Sicredi se reserva o direito de monitorar e registrar todo e qualquer acesso à rede, Internet, sistemas e demais ambientes físicos e lógicos de modo que as ações executadas e os usuários possam ser devidamente identificados e responsabilizados.

5.13 Violações e Sanções

A violação ou não observância destas regras poderá acarretar o registro de um incidente de segurança da informação, sem prejuízo de demais sanções previstas, de acordo com as cláusulas contratuais estabelecidas entre o Sicredi e a empresa contratada.



6. Base Regulatória

[Lei nº 9.609/98 \(Proteção de Software\)](#)

[LC nº 105/01 \(Sigilo Bancário\)](#)



[Lei nº 12.965/14 \(Marco Civil da Internet\)](#)

[Lei nº 13.709/18 \(Proteção de Dados Pessoais\)](#)

[Res. CMN 4.893/21 \(Segurança Cibernética\)](#)

[Resolução CVM 35](#)



7. Vigência e Histórico de Aprovação

DATA	DESCRÍÇÃO	APROVADOR
22/11/2023	4ª versão – atualização do documento	Extração da Norma de Governança de Segurança da Informação aprovada em 22/11/2023 pelo Conselho de Administração SicrediPar.
27/11/2024	5ª versão – atualização do documento	Extração da Norma de Governança de Segurança da Informação aprovada em 27/11/2024 pelo Conselho de Administração SicrediPar.

Este documento é extração da Norma de Governança de Segurança da Informação aprovada em 27/11/2024 pelo Conselho de Administração da SicrediPar