Política Estabelecida em	Revisão/Atualização	Vigência
02/10/2023	02/10/2023	02/10/2024

Título:	Política de Segurança Cibernética	Confidencialidade	Restrita

1 – Introdução

A Cooperativa de Crédito Agrocredi LTDA – Sicoob Agrocredi reconhece a importância de uma Política de Segurança Cibernética com o intuito de proteção de dados, prevenção de ataques, cumprimento de regulamentação, bem como a continuidade da garantia do negócio. Deste modo, esta Política estabelece as diretrizes para proteção dos ativos de informação.

2 – Objetivos

Estabelecer diretrizes para proteção dos ativos de informação contra ameaças, ataques e vulnerabilidades cibernéticas. Assegurar que os cinco pilares de Segurança da Cibernética sejam cumpridos: identificar, proteger, detectar, responder e recuperar.

3 – Responsabilidades

3.1 Diretoria

Responsável pela tomada de decisões estratégicas e pela liderança na proteção dos ativos de informações da Cooperativa contra ameaças e vulnerabilidades cibernéticas. Conforme estrutura organizacional, o Diretor de Segurança Cibernética é cadastrado UNICAD (Sistema de Informações sobre Entidades de Interesse do Banco Central) de acordo com sua área de atuação. Principais responsabilidades:

a) Liderar e supervisionar as ações relacionadas à Segurança Cibernética.

b) Promover cultura sólida e eficaz dentro da Cooperativa através de programas e treinamentos de conscientização para os funcionários.

c) Aprovar orçamentos relacionados e alocar recursos de maneira adequada para implementação eficaz da política de Segurança Cibernética.

d) Definir e aprovar políticas de Segurança Cibernética que estabeleçam diretrizes na proteção dos ativos de informações.

e) Entender e avaliar os riscos cibernéticos enfrentados pela Cooperativa e garantir medidas para mitigar esses riscos.

3.2 Grupo de Segurança Cibernética

Desempenha um papel fundamental na implementação e execução da política de Segurança Cibernética:

a) Responsável em responder a incidentes de segurança, realizando investigação de causa raiz e avaliar o impacto.

b) Responsável em monitorar e avaliar a postura de segurança da Cooperativa.

c) Manter atualizada a Política de Segurança Cibernética.

d) Utilizar ferramentas de varreduras para identificar vulnerabilidades na rede da Cooperativa e nos ativos de informações.

e) Realizar gestão de identidade e acesso, garantindo que os sistemas e seus recursos sejam acessados de maneira adequada de acordo com as funções de seus usuários.

f) Garantir comunicação eficaz com a Cooperativa, promovendo uma análise holística da segurança cibernética.

3.3 Funcionários

Os funcionários são responsáveis por:

a) Seguir as diretrizes de Segurança Cibernética estabelecidas pela Cooperativa.

b) Participar de treinamentos disponibilizados pela Unidade de TI, Central Crediminas ou CCS, melhorando assim sua preparação quanto a Segurança Cibernática na Cooperativa.

c) Usar de forma responsável os sistemas, recursos e ativos de informações.

d) Utilizar senhas fortes e seguras de acordo a Política de Contas de Usuário.

e) Reportar incidentes (ou a possibilidade de sua ocorrência) ao departamento de TI, conforme Política de Gerenciamento de Incidentes de TI.

f) Garantir o bloqueio de dispositivos (computadores, notebooks, smartphones etc.) durante o período em que não estiverem em uso.

g) Manter o local de trabalho limpo, sem exposição de senhas, documentos e/ou dados sensíveis.

h) Salvar arquivos necessários em suas respectivas pastas da rede, para que eles sejam salvos durante as execuções de backup.

4 – Diretrizes

Regras gerais, orientações e princípios que estabelecem uma estrutura para implementar e manter a segurança cibernética na Cooperativa, com o objetivo de criar um ambiente seguro na proteção dos ativos de informação.

4.1 Acesso Autorizado

Conceder acesso aos sistemas e dados semente a usuários previamente autorizados e de acordo com suas funções de trabalho, garantindo proteção contra ameaças internas e externas, proteção contra o vazamento de dados e conformidade regulatória e limitação da superfície de ataque.

4.2 Atualização de Softwares

Manter os sistemas e aplicativos atualizados, garantindo que as últimas correções de segurança sejam aplicadas, garantindo proteção contra vulnerabilidades conhecidas, prevenindo contra ataques de Malware. Além da correção de vulnerabilidades, atualizações podem melhorar o desempenho e estabilidade de softwares, garantindo assim a continuidade de negócios.

4.3 Gerenciamento de Ativos

Registrar e atualizar uma relação de todos os ativos de TI, incluindo hardware e software. Aplicar controles de acesso físico a servidores e salas de servidores. Isso permite a identificação de ativos críticos ou suscetíveis a ameaças, que necessitam de prioridade em sua proteção. O gerenciamento de ativos auxilia na economia de recursos, evitando gastos desnecessários em ativos obsoletos, otimizando a alocação de recursos que deve ser realizada pelo diretor de Segurança Cibernética.

4.4 Análise e Monitoramento Contínuo

Utilizar ferramentas de escaneamento de vulnerabilidades assim como de monitoramento em segurança, garantindo dessa forma detecção e prevenção contra possíveis ameaças no ambiente e permitindo a verificação de atividades suspeitas e anomalias em tempo real. Realizar auditorias internas regulares para identificar vulnerabilidades. A análise de vulnerabilidades auxilia na redução do tempo de ameaças na rede, na avaliação de eficácia das ferramentas utilizadas pela Cooperativa e na prevenção de ataques futuros.

4.5 Política de Senhas Fortes

Exigir senhas fortes e seguras de acordo a Política de Contas de Usuário, importante para prevenção contra violação de dados, reduzir o risco de ameaças internas. A Política de Contas de Usuário, através de senhas fortes, torna ataques de força bruta menos eficazes, visto que é necessário um tempo demasiadamente maior para que seja possível adivinhar combinações de senhas complexas.

4.6 Proteção de Dados

Criptografar dados confidenciais em repouso e em trânsito de acordo com as ferramentas disponíveis, garantindo confidencialidade e integridade dos dados, proteção contra sua violação e mitigando o risco de exposição de dados.

4.7 Treinamento e Conscientização

Realizar treinamentos regulares em segurança cibernética para todos os funcionários. Promover uma cultura de segurança cibernética por meio de programas de conscientização. Enfatizar a importância de tais treinamentos e garantir que os funcionários da Cooperativa estejam aptos a responder a ameaças e incidentes.

4.8 Gestão de Incidentes

Seguir as diretrizes estabelecidas na Política de Gerenciamento de Incidentes TI, permitindo o processo de identificação, relato e resposta a incidentes de Segurança Cibernética. A Política de Gerenciamento de Incidentes TI é fundamental para detectar e responder de forma rápida e eficiente os incidentes relacionados a Segurança Cibernética na Cooperativa, reduzindo riscos e permitindo que ações rápidas possam evitar que um incidente se agrave e cause danos significativos a Cooperativa.

7 – Relatórios de Vulnerabilidades

Elaborar relatório de vulnerabilidades que permita uma visão macro do ambiente e riscos relacionados à Segurança Cibernética na Cooperativa, garantindo assim a identificação, avaliação e mitigação dos riscos. Com base nas informações é possível que a liderança tome decisões sobre alocação de recursos e esforços para correções.

8 – Plano de Ação e Resposta a Incidentes

Produzir relatório anual sobre a implementação do plano de ação e de resposta a incidentes apresentando ações implementadas para garantir a efetividade da política de segurança cibernética e adequações das estruturas organizacionais e operacionais aos princípios e às diretrizes da política de segurança cibernética.

Apresentar no plano as rotinas, procedimentos, controles e tecnologias utilizadas na prevenção e respostas a incidentes, tais como:

a) Procedimentos de Hardening.

b) Monitoramento de ativos.

c) Classificação de dados quanto a relevância.

d) Tecnologias, soluções e ferramentas utilizados para prevenção, análise e solução de incidentes cibernéticos.

9 – Revisão e Atualização

Revisar e atualizar a política de segurança cibernética periodicamente devido a evolução de ameaças, vulnerabilidades emergentes e as constantes mudanças e atualizações tecnológicas.

9 páginas - Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinaturas gerado em 10 de October de 2023, 16:52:30

Política de Segurança Cibernética Revisado pdf

Código do documento 0d76dbce-9cbf-4164-95bd-d4eb8428c319

Assinaturas

Geraldo Souza Ribeiro Filho
geraldo.filho@sicoobagrocredi.com.br
Assinou como parte

Luiz Alberto Andrade
luiz.andrade@sicoobagrocredi.com.br
Assinou como parte

Amarildo Freitas Pelozo
amarildo.pelozo@sicoobagrocredi.com.br
Assinou como parte

Antônio Lourival Junqueira
antonio.junqueira@sicoobagrocredi.com.br
Assinou como parte

Irson Ribeiro de Oliveira
irson.oliveira@sicoobagrocredi.com.br
Assinou como parte

Paulo Mariotti Flora
paulo.flora@sicoobagrocredi.com.br
Assinou como parte

Roberto Gomes Castejon
roberto.castejon@sicoobagrocredi.com.br
Assinou como parte

Virgolino Adriano Muniz
virgolino.muniz@sicoobagrocredi.com.br
Assinou como parte

Luiz Antônio de Almeida Basilli
luiz.basilli@sicoobagrocredi.com.br
Assinou como parte

Eventos do documento

06 Oct 2023, 12:30:10
Documento 0d76dbce-9cbf-4164-95bd-d4eb8428c319 **criado** por COOPERATIVA DE CREDITO AGROCREDI LTDA. - SICOOB AGROCREDI - CONTA SISTEMA (49258c6e-bbe6-4b57-b0d5-03d8844907f9). Email:juridico@sicoobagrocredi.com.br. - DATE_ATOM: 2023-10-06T12:30:10-03:00

06 Oct 2023, 12:31:32

Assinaturas **iniciadas** por COOPERATIVA DE CREDITO AGROCREDI LTDA. - SICOOB AGROCREDI - CONTA SISTEMA (49258c6e-bbe6-4b57-b0d5-03d8844907f9). Email: juridico@sicoobagrocredi.com.br. - DATE_ATOM: 2023-10-06T12:31:32-03:00

06 Oct 2023, 13:50:23
GERALDO SOUZA RIBEIRO FILHO **Assinou como parte** (908e7ab3-a2b6-494e-b2ac-066aa343a2f5) - Email: geraldo.filho@sicoobagrocredi.com.br - IP: 177.41.164.72 (177.41.164.72.static.host.gvt.net.br porta: 52138) - Geolocalização: -21.2983337 -46.6924689 - Documento de identificação informado: 952.686.778-53 - DATE_ATOM: 2023-10-06T13:50:23-03:00

06 Oct 2023, 15:26:59
PAULO MARIOTTI FLORA **Assinou como parte** (b848f489-0b46-49dd-8e0d-e8285014c981) - Email: paulo.flora@sicoobagrocredi.com.br - IP: 177.191.103.40 (177-191-103-40.xd-dynamic.algarnetsuper.com.br porta: 20738) - Geolocalização: -21.7914529 -46.5886681 - Documento de identificação informado: 583.299.276-87 - DATE_ATOM: 2023-10-06T15:26:59-03:00

06 Oct 2023, 15:33:09
AMARILDO FREITAS PELOZO **Assinou como parte** (197759cd-9575-4752-83ab-0e4fd0e0e643) - Email: amarildo.pelozo@sicoobagrocredi.com.br - IP: 186.193.110.4 (186-193-110-4.as28220.net porta: 4580) - Geolocalização: -21.4147531 -45.9418631 - Documento de identificação informado: 440.289.706-87 - DATE_ATOM: 2023-10-06T15:33:09-03:00

06 Oct 2023, 18:25:53
IRSON RIBEIRO DE OLIVEIRA **Assinou como parte** (7e5569ab-2a38-4554-95e6-88d229760bd8) - Email: irson.oliveira@sicoobagrocredi.com.br - IP: 200.58.250.126 (200.58.250.126 porta: 31224) - Geolocalização: -21.100955 -46.5811365 - Documento de identificação informado: 184.227.216-00 - DATE_ATOM: 2023-10-06T18:25:53-03:00

06 Oct 2023, 21:29:51
ANTÔNIO LOURIVAL JUNQUEIRA **Assinou como parte** (ed60f232-27aa-4782-884f-b6c0ed2d150e) - Email: antonio.junqueira@sicoobagrocredi.com.br - IP: 152.255.97.47 (152-255-97-47.user.vivozap.com.br porta: 56574) - Documento de identificação informado: 866.467.458-20 - DATE_ATOM: 2023-10-06T21:29:51-03:00

07 Oct 2023, 18:54:45
LUIZ ALBERTO ANDRADE **Assinou como parte** (d1bb73cc-711c-4842-9215-bc65162d923a) - Email: luiz.andrade@sicoobagrocredi.com.br - IP: 177.41.164.25 (177.41.164.25.static.host.gvt.net.br porta: 45858) - Geolocalização: -21.2998435 -46.6947426 - Documento de identificação informado: 353.587.426-20 - DATE_ATOM: 2023-10-07T18:54:45-03:00

09 Oct 2023, 17:46:17
LUIZ ANTÔNIO DE ALMEIDA BASILLI **Assinou como parte** (1c7e3e0b-038a-4683-becf-1f37e3169e95) - Email: luiz.basilli@sicoobagrocredi.com.br - IP: 177.77.253.157 (ip-177-77-253-157.user.vivozap.com.br porta: 44380) - Geolocalização: -21.5279605 -46.6473583 - Documento de identificação informado: 130.617.968-86 - **Assinado com EMBED** - Token validado por **email** - DATE_ATOM: 2023-10-09T17:46:17-03:00

09 Oct 2023, 18:10:48

ROBERTO GOMES CASTEJON **Assinou como parte** (728cd733-6733-457f-9328-5cd6ce18ef4a) - Email: roberto.castejon@sicoobagrocredi.com.br - IP: 152.255.119.84 (152-255-119-84.user.vivozap.com.br porta: 4656) - Documento de identificação informado: 872.707.148-00 - DATE_ATOM: 2023-10-09T18:10:48-03:00

09 Oct 2023, 18:56:28
VIRGOLINO ADRIANO MUNIZ **Assinou como parte** (8eb0f6e8-d65b-4ce5-b8d6-27fc1ac9dd3f) - Email: virgolino.muniz@sicoobagrocredi.com.br - IP: 191.14.170.98 (191-14-170-98.user.vivozap.com.br porta: 50822) - Geolocalização: -21.4746539 -46.3946554 - Documento de identificação informado: 214.308.456-00 - DATE_ATOM: 2023-10-09T18:56:28-03:00

Hash do documento original
(SHA256):85900fe3cac97f13af1e8ded975fb07aa5a8bb929aeaf63e7d299bd0660d2592
(SHA512):4b11641da00b2dedf673d33036561673787df1faa2eeb64d44004c24f3c65b07ded5fb5d877b05e5c8fd2c2ddd8aecfca042aa70f28812f28ea99dc6705d8be3

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign