POLÍTICA DE SEGURANÇA CIBERNÉTICA

Sumário

1. OBJETIVO

Definir os objetivos, processos e controles de segurança cibernética, de acordo com a Resolução CMN nº 4.893/2021. A Usicred busca com este documento estabelecer as diretrizes para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, visando a perenidade e a continuidade dos seus negócios.

2. ABRANGENCIA

Aplicável aos colaboradores, parceiros e fornecedores da Usicred.

3. DIRETRIZES

3.1. Princípios

Para fins de segurança da informação, a Usicred considera os seguintes princípios:

i. Confidencialidade das informações pessoais e sensíveis;
ii. Integridade e transparência das informações perante associados e reguladores;
iii. Disponibilidade dos sistemas.

3.2. Procedimentos e Controles

Os procedimentos de controle utilizados pela Usicred, consistem:

i. Utiliza os drivers da rede cedidos pela empresa mantenedora (São Martinho), segmentadas para garantir a segurança e desempenho das redes, incluindo a sistemas de prevenção de invasão.
ii. Informações administrativas e de Recursos Humanos são armazenadas em sistema de nuvem, por meio de prestador de serviço qualificado;
iii. O prestador de serviços de tecnologia, realiza o gerenciamento sistêmico e o armazenamento de dados (financeiros, cadastrais, contábeis, fiscais, indicadores e operacionais), utilizando as melhores práticas de mercado;
iv. O prestador de serviços de tecnologia realiza Backups diários de todo o banco de dados da Usicred, utilizando ambiente redundante (replicado) e de alta disponibilidade;
v. Backups são testados semanalmente para garantia da integridade;
vi. O prestador de serviços de tecnologia proporciona ferramentas de firewall, antivírus, ambos atualizados e monitorados diariamente, e análises constantes para detecção de possíveis ataques cibernéticos;
vii. A empresa mantenedora (São Martinho) contempla a Usicred em sua rede de informação para rodar o pacote office, e-mail e gerenciamento de rede (arquivos), os quais estão sob as melhores práticas de gerenciamento de riscos cibernéticos;
viii. A Usicred utiliza-se de critérios rígidos de senhas de acesso aos sistemas, bem como rastreamento de acesso dos usuários;
ix. O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos são restritos a pessoas autorizadas e de acordo com a necessidade

para o cumprimento de suas funções. Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função;

x. Periodicamente, os acessos concedidos devem ser revistos e informados à Diretoria Administrativa.

3.2.1. Relatório de Testes de Segurança das Informações

Sempre que solicitado pela Usicred, o prestador de serviços de tecnologia realiza testes dos seus sistemas de segurança de informações, buscando cobrir os seguintes pontos:

i. Identificação e avaliação de potenciais riscos cibernéticos, envolvendo ativos de hardware e software e processos que necessitem de proteção;
ii. Detecção de possíveis anomalias e/ou fragilidades no ambiente tecnológico, incluindo acessos não permitidos, usuários não cadastrados, e dispositivos não autorizados.

Estabelecimento de medidas de prevenção e mitigação de riscos identificados na atividade de identificação de riscos, de forma buscar evitar eventuais ataques cibernéticos aos dados e equipamentos da empresa.

3.2.2. Prevenção

Além das medidas mencionadas acima, são medidas de prevenção, a manutenção do programa de segurança cibernética atualizado, identificando novos e potenciais riscos, ativos e processos, bem como a criação de plano de resposta e recuperação de incidentes que contenha comunicação interna e externa (Plano de Continuidade de Negócio Específico), em linha com a Política de Gerenciamento de Crises e Continuidade de Negócios.

As medidas de prevenção contemplam ainda a implementação de programas de capacitação em segurança.

Os documentos relacionados a segurança da informação, testes e medidas preventivas e corretivas, deverão ser mantidos arquivados.

Senhas e Acessos: com relação às senhas e acessos, o identificador da rede e dos sistemas (login/senha) é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia. Cuidados que devem ser tomados por todos os usuários:

i. Manter a confidencialidade, memorizar e não registrar a senha em lugar algum, ou seja, não informar a ninguém e não a anotar em papel;
ii. Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
iii. Selecionar senhas de qualidade, que sejam de difícil adivinhação;
iv. Impedir o uso do equipamento por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
v. Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del).

3.2.3. Controles adicionais

Além dos controles mencionados acima, a Usicred conta também:

i. Esta Política de segurança cibernética, política de gestão de riscos e continuidade de negócios;
ii. Tratamento confidencial das informações internas;
iii. Uma Diretoria responsável pela execução desta política e sua disseminação;
iv. Comprometimento da alta administração.

4. INCIDENTES RELEVANTES

A condução dos incidentes relevantes ocorridos na Usicred ou empresas prestadoras de serviço ou mantenedora, observará a política de Gestão de Crises e Continuidade de Negócios (PCN específico).

A natureza dos dados e a criticidade dos sistemas e processos afetados serão levados em consideração para a classificação da emergência e providências na gestão da crise.

Haverá o registro e arquivamento das seguintes informações:

i. Possível(is) causa(s) e impactos;
ii. Planos de ação e de resposta;
iii. Acompanhamento da execução do Plano de continuidade de negócio.

4.1. Relatório Anual sobre Incidentes

A Diretoria Administrativa é responsável por esta política e deverá elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro, contendo:

i. Efetividade da implementação das ações;
ii. Resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
iii. Incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
iv. Resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório anual deverá ser apresentado ao conselho de administração ou, na sua inexistência, à diretoria da Usicred até 31 de março do ano seguinte ao da data-base.

4.2. Responsabilidades entre USICRED e Mantenedora (São Martinho)

A Usicred poderá obter dados cadastrais de seus associados, em algumas situações específicas, tal como via importação cadastral (realizada mensalmente através do sistema nuvem proporcionado pelo prestador de serviços de tecnologia e pela Mantenedora), possibilitando atualização de dados cadastrais dos associados.

Os dados fornecidos pelos associados serão mantidos em sigilo e não poderão ter uso diverso.

A Usicred obriga-se a cumprir, com rigor, as disposições legais vigentes no Brasil que tratam da privacidade, sigilo e segurança das informações que receber de seus associados, com a finalidade maior de resguardar os direitos destes.

5. ATRIBUIÇÕES

Diretor(a) Administrativo: execução e divulgação desta política.

Conselho de Administração: aprovação desta política.

6. CONSIDERAÇÕES FINAIS

Esta Política poderá ser revisada periodicamente, em decorrência de alterações na regulamentação e/ou legislação aplicável ou, ainda, para refletir alterações nos procedimentos internos.

A política de segurança cibernética e o plano de ação e de resposta a incidentes devem ser documentados e revisados, no mínimo, anualmente.

Esta Política foi aprovada pelo Conselho de Administração em 07 de outubro de 2021 e revisada em 18 de dezembro de 2023.